CHAPTER 34

match regex through message-length Commands

match regex

To identify a regular expression in a regular expression class map, use the **match regex** command in class-map type regex configuration mode. To remove the regular expression from the class map, use the **no** form of this command.

match regex *name*

no match regex *name*

Syntax Description

name	The name of the regular expression you added with the **regex** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map type regex configuration	•	•	•	—	•

Command History

Release	Modification
7.0(2)	We introduced this command.

Usage Guidelines

The **regex** command can be used for various features that require text matching. You can group regular expressions in a regular expression class map using the **class-map type regex** command and then multiple **match regex** commands.

For example, you can configure special actions for application inspection using an inspection policy map (see the **policy map type inspect** command). In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets.

Examples

The following is an example of an HTTP inspection policy map and the related class maps. This policy map is activated by the Layer 3/4 policy map, which is enabled by the service policy.

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log
hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test [a Layer 3/4 class map not shown]
hostname(config-pmap-c)# inspect http http-map1
hostname(config-pmap-c)# service-policy test interface outside
```

Related Commands

Command	Description
class-map type regex	Creates a regular expression class map.
regex	Adds a regular expression.
test regex	Tests a regular expression.

match req-resp

To configure a match condition for both HTTP requests and responses, use the **match req-resp** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **req-resp content-type mismatch**

no match [**not**] **req-resp content-type mismatch**

Syntax Description

content-type	Specifies to match the content type in the response to the accept types in the request.
mismatch	Specifies that the content type field in the response must match one of the mime types in the accept field of the request.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command enables the following checks:

- Verifies that the value of the header content-type is in the internal list of supported content types,
- Verifies that the header content-type matches the actual content in the data or entity body portion of the message.
- Verifies the content type field in the HTTP response matches the **accept** field in the corresponding HTTP request message.

If the message fails any of the above checks, the ASA takes the configured action.

The following is the list of supported content types.

<table>
<tr><td>audio/* |</td><td>audio/basic |</td><td>video/x-msvideo</td></tr>
<tr><td>audio/mpeg |</td><td>audio/x-adpcm |</td><td>audio/midi</td></tr>
<tr><td>audio/x-ogg |</td><td>audio/x-wav |</td><td>audio/x-aiff |</td></tr>
<tr><td>application/octet-stream</td><td>application/pdf</td><td>application/msword</td></tr>
<tr><td>application/vnd.ms-excel</td><td>application/vnd.ms-powerpoint</td><td>application/postscript</td></tr>
<tr><td>application/x-java-arching</td><td>application/x-msn-messenger</td><td>application/x-gzip</td></tr>
<tr><td>image |</td><td>application/x-java-xm</td><td>application/zip</td></tr>
<tr><td>image/jpeg |</td><td>image/cgf |</td><td>image/gif |</td></tr>
<tr><td>image/x-3ds |</td><td>image/png |</td><td>image/tiff |</td></tr>
<tr><td>image/x-portable-bitmap |</td><td>image/x-bitmap |</td><td>image/x-niff |</td></tr>
<tr><td>text/* |</td><td>image/x-portable-greymap |</td><td>image/x-xpm |</td></tr>
<tr><td>text/plain |</td><td>text/css</td><td>text/html |</td></tr>
<tr><td>text/xmcd</td><td>text/richtext |</td><td>text/sgml</td></tr>
<tr><td>video/-flc</td><td>text/xml</td><td>video/*</td></tr>
<tr><td>video/sgi</td><td>video/mpeg</td><td>video/quicktime</td></tr>
<tr><td>video/x-mng</td><td>video/x-avi</td><td>video/x-fli</td></tr>
</table>

Some content-types in this list may not have a corresponding regular expression (magic number) so they cannot be verified in the body portion of the message. When this case occurs, the HTTP message will be allowed.

Examples

The following example shows how to restrict HTTP traffic based on the content type of the HTTP message in an HTTP policy map:

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# match req-resp content-type mismatch
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match request-command

To restrict specific FTP commands, use the **match request-command** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **request-command** *ftp_command* [*ftp_command...*]

no match [**not**] **request-command** *ftp_command* [*ftp_command...*]

Syntax Description

ftp_command	Specifies one or more FTP commands to restrict.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for a specific FTP command in an FTP inspection policy map:

```
hostname(config)# policy-map type inspect ftp ftp_map1
hostname(config-pmap)# match request-command stou
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match request-method

To configure a match condition for the SIP method type, use the **match request-method** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **request-method** *method_type*

no match [**not**] **request-method** *method_type*

Syntax Description

method_type	Specifies a method type according to RFC 3261 and supported extensions. Supported method types include: ack, bye, cancel, info, invite, message, notify, options, prack, refer, register, subscribe, unknown, update.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the path taken by a SIP message in a SIP inspection class map:

```
hostname(config-cmap)# match request-method ack
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match request method

To configure a match condition for HTTP requests, use the **match request method** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

no match [**not**] **request** {*built-in-regex* | **regex** {*regex_name* | **class** *class_map_name*}}

Syntax Description

built-in-regex	Specifies the built-in regex for content type, method, or transfer encoding.
class *class_map name*	Specifies the name of the class map of regex type.
regex *regex_name*	Specifies the name of the regular expression configured using the **regex** command.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Table 34-1 Built-in Regex Values

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify
options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

Examples

The following example shows how to define an HTTP inspection policy map that will allow and log any HTTP connection that attempts to access "www\.example.com/.*\.asp" or "www\example[0-9][0-9]\.com" with methods "GET" or "PUT." All other URL/Method combinations will be silently allowed:

```
hostname(config)# regex url1 "www\.example.com/.*\.asp
hostname(config)# regex url2 "www\.example[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"
hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit
hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit
hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit
hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
show running-config class-map	Displays the information about the class map configuration.

match route-type

To redistribute routes of the specified type, use the **match route-type** command in route-map configuration mode. To remove the route type entry, use the **no** form of this command.

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

Syntax Description

external	OSPF external routes or EIGRP external routes.
internal	OSPF intra-area and interarea routes or EIGRP internal routes.
local	Locally generated BGP routes.
nssa-external	Specifies the external NSSA.
type-1	(Optional) Specifies the route type 1.
type-2	(Optional) Specifies the route type 2.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Route-map configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **route-map** global configuration command and the **match** and **set** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match** route-map configuration command has multiple formats. You can enter the **match** commands in any order. All **match** commands must “pass” to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

A route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored. To modify only some data, you must configure a second route map section and specify an explicit match.

For OSPF, the **external type-1** keywords match only type 1 external routes and the **external type-2** keywords match only type 2 external routes.

Examples

The following example shows how to redistribute internal routes:

```
hostname(config)# route-map name
hostname(config-route-map)# match route-type internal
```

Related Commands

Command	Description
match interface	Distributes distribute any routes that have their next hop out one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
match metric	Redistributes routes with the metric specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

match rtp

To specify a UDP port range of even-number ports in a class map, use the **match rtp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match rtp *starting_port range*

no match rtp *starting_port range*

Syntax Description

starting_port	Specifies lower bound of even-number UDP destination port. Range is 2000-65535
range	Specifies range of RTP ports. Range is 0-16383.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

Use the **match rtp** command to match RTP ports (even UDP port numbers between the *starting_port* and the *starting_port* plus the *range*).

Examples

The following example shows how to define a traffic class using a class map and the **match rtp** command:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match rtp 20000 100
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match sender-address

To configure a match condition on the ESMTP sender e-mail address, use the **match sender-address** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **sender-address [length gt** *bytes* | **regex** *regex*]

no match [**not**] **sender-address [length gt** *bytes* | **regex** *regex*]

Syntax Description

length gt *bytes*	Specifies to match on the sender e-mail address length.
regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the sender email address of length greater than 320 characters in an ESMTP inspection policy map:

```
hostname(config-pmap)# match sender-address length gt 320
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match server

To configure a match condition for an FTP server, use the **match server** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

The ASA matches the server name based using the initial 220 server message that is displayed above the login prompt when connecting to an FTP server. The 220 server message might contain multiple lines. The server match is not based on the FQDN of the server name resolved through DNS.

Examples

The following example shows how to configure a match condition for an FTP server in an FTP inspection policy map:

```
hostname(config-pmap)# match server class regex ftp-server
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match service

To configure a match condition for a specific instant messaging service, use the **match service** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

no match [**not**] **service** {**chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference**}

Syntax Description

chat	Specifies to match the instant messaging chat service.
file-transfer	Specifies to match the instant messaging file transfer service.
games	Specifies to match the instant messaging games service.
voice-chat	Specifies to match the instant messaging voice chat service.
webcam	Specifies to match the instant messaging webcam service.
conference	Specifies to match the instant messaging conference service.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an IM class map or policy map. Only one entry can be entered in a IM class map.

Examples

The following example shows how to configure a match condition for the chat service in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match service chat
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
show running-config class-map	Displays the information about the class map configuration.

match third-party-registration

To configure a match condition for the requester of a third-party registration, use the **match third-party-registration** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

The third-party registration match command is used to identify the user who can register others with a SIP registar or SIP proxy. It is identified by the From header field in the REGISTER message in the case of mismatching From and To values.

Examples

The following example shows how to configure a match condition for third-party registration in a SIP inspection class map:

```
hostname(config-cmap)# match third-party-registration regex class sip_regist
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match tunnel-group

To match traffic in a class map that belongs to a previously defined tunnel-group, use the **match tunnel-group** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match tunnel-group *name*

no match tunnel-group *name*

Syntax Description

name	Text for the tunnel group name.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **match** commands are used to identify the traffic included in the traffic class for a class map. They include different criteria to define the traffic included in a class-map. Define a traffic class using the **class-map** global configuration command as part of configuring a security feature using Modular Policy Framework. From class-map configuration mode, you can define the traffic to include in the class using the **match** command.

After a traffic class is applied to an interface, packets received on that interface are compared to the criteria defined by the **match** statements in the class map. If the packet matches the specified criteria, it is included in the traffic class and is subjected to any actions associated with that traffic class. Packets that do not match any of the criteria in any traffic class are assigned to the default traffic class.

To enable flow-based policy actions, use the **match flow ip destination-address** and **match tunnel-group** commands with the **class-map**, **policy-map**, and **service-policy** commands. The criteria to define flow is the destination IP address. All traffic going to a unique IP destination address is considered a flow. Policy action is applied to each flow instead of the entire class of traffic. QoS action police is applied using the **police** command. Use **match tunnel-group** along with **match flow ip destination-address** to police every tunnel within a tunnel group to a specified rate.

Examples

The following example shows how to enable flow-based policing within a tunnel group and limit each tunnel to a specified rate:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
show running-config class-map	Displays the information about the class map configuration.
tunnel-group	Creates and manages the database of connection-specific records for IPsec and L2TP,

match uri

To configure a match condition for the URI in the SIP headers, use the **match uri** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

no match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

Syntax Description

sip	Specifies a SIP URI.
tel	Specifies a TEL URI.
length gt *gt_bytes*	Specifies the maximum length of the URI. Value is between 0 and 65536.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a SIP class map or policy map. Only one entry can be entered in a SIP class map.

Examples

The following example shows how to configure a match condition for the URI in the SIP message:

```
hostname(config-cmap)# match uri sip length gt
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match url-filter

To configure a match condition for URL filtering in an RTSP message, use the **match url-filter** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

This command can be configured in an RTSP class map or policy map.

Examples

The following example shows how to configure a match condition for URL filtering in an RTSP inspection policy map:

```
hostname(config)# regex badurl www.example.com/rtsp.avi
hostname(config)# policy-map type inspect rtsp rtsp-map
hostname(config-pmap)# match url-filter regex badurl
hostname(config-pmap-p)# drop-connection
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match user group

To specifie a user or group to whitelist for Cloud Web Security, use the **match user group** command in parameters configuration mode. You can access the parameters onfiguration mode by first entering the **class-map type inspect scansafe** command. To remove the match, use the **no** form of this command.

match [**not**] {[**user** *username*] [**group** *groupname*]}

no match [**not**] {[**user** *username*] [**group** *groupname*]}

Syntax Description

not	(Optional) Specifies that the user and/or group should be filtered using Web Cloud Security. For example, if you whitelist the group "cisco," but you want to scan traffic from users "johncrichton" and "aerynsun," you can specify **match not** for those users.
user *username*	Specifies a user to whitelist.
group *groupname*	Specifies a group to whitelist.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

If you use AAA rules or IDFW, you can configure the ASA so that web traffic from specific users or groups that otherwise match the service policy rule is not redirected to the Cloud Web Security proxy server for scanning. When you bypass Cloud Web Security scanning, the ASA retrieves the content directly from the originally requested web server without contacting the proxy server. When it receives the response from the web server, it sends the data to the client. This process is called "whitelisting" traffic.

Although you can achieve the same results of exempting traffic based on user or group when you configure the class of traffic using ACLs to send to Cloud Web Security, you might find it more straightforward to use a whitelist instead. Note that the whitelist feature is only based on user and group, not on IP address.

After creating the whitelist as part of the inspection policy map (**policy-map type inspect scansafe**), you can use this map when you specify the Cloud Web Security action using the **inspect scansafe** command.

Examples

The following example whitelists the same users and groups for the HTTP and HTTPS inspection policy maps:

```
hostname(config)# class-map type inspect scansafe match-any whitelist1
hostname(config-cmap)# match user user1 group cisco
hostname(config-cmap)# match user user2
hostname(config-cmap)# match group group1
hostname(config-cmap)# match user user3 group group3

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap1
hostname(config-pmap)# parameters
hostname(config-pmap-p)# http
hostname(config-pmap-p)# default group default_group
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist

hostname(config)# policy-map type inspect scansafe cws_inspect_pmap2
hostname(config-pmap)# parameters
hostname(config-pmap-p)# https
hostname(config-pmap-p)# default group2 default_group2
hostname(config-pmap-p)# class whitelist1
hostname(config-pmap-c)# whitelist
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.

Command	Description
whitelist	Performs the whitelist action on the class of traffic.

match username

To configure a match condition for an FTP username, use the **match username** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

regex_name	Specifies a regular expression.
class *regex_class_name*	Specifies a regular expression class map.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in an FTP class map or policy map. Only one entry can be entered in a FTP class map.

Examples

The following example shows how to configure a match condition for an FTP username in an FTP inspection class map:

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# match username regex class ftp_regex_user
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match any	Includes all traffic in the class map.

Command	Description
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

match version

To configure a match condition for a GTP message ID, use the **match message length** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

Syntax Description

vresion_id	Specifies a version between 0 and 255.
range *lower_range upper_range*	Specifies a lower and upper range of versions.

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP class map or policy map. Only one entry can be entered in a GTP class map.

Examples

The following example shows how to configure a match condition for a message version in a GTP inspection class map:

```
hostname(config-cmap)# match version 1
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.

Command	Description
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.
show running-config class-map	Displays the information about the class map configuration.

max-failed-attempts

To specify the number of failed attempts allowed for any given server in the server group before that server is deactivated, use the **max-failed-attempts** command in aaa-server group configuration mode. To remove this specification and revert to the default value, use the **no** form of this command.

max-failed-attempts *number*

no max-failed-attempts

Syntax Description

number	An integer in the range of 1-5, specifying the number of failed connection attempts allowed for any given server in the server group specified in a previous **aaa-server** command.

Defaults

The default value of *number* is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
aaa-server group configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have configured the AAA server or group before issuing this command.

Examples

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 4
hostname(config-aaa-server-group)#
```

Related Commands

Command	Description
aaa-server *server-tag* **protocol** *protocol*	Enters aaa-server group configuration mode so that you can configure AAA server parameters that are group-specific and common to all hosts in the group.

clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

max-forwards-validation

To enable check on Max-forwards header field of 0, use the **max-forwards-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

no max-forwards-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection of a violation occurs.
log	Specifies standalone or additional log in case of violation. It can be associated to any of the actions.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command counts the number of hops to destination, which cannot be 0 before reaching the destination.

Examples

The following example shows how to enable max forwards validation in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# max-forwards-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

max-header-length

To restrict HTTP traffic based on the HTTP header length, use the **max-header-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
request	Request message.
reset	Send a TCP reset message to client and server.
response	(Optional) Response message.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **max-header-length** command, the ASA only allows messages having an HTTP header within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and optionally create a syslog entry.

Examples

The following example restricts HTTP requests to those with HTTP headers that do not exceed 100 bytes. If a header is too large, the ASA resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

max-object-size

To set a maximum size for objects that the ASA can cache for WebVPN sessions, use the max-object-size command in cache mode. To change the size, use the command again.

max-object-size *integer range*

Syntax Description

integer range	0 - 10000 KB

Defaults

1000 KB

Command Modes

The following table shows the modes in which you enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Cache mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The Maximum object size must be larger than the minimum object size. The ASA calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 4000 KB:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# max-object-size 4000
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
min-object-size	Defines the minimum sizze of an object to cache.

max-retry-attempts

To configure the number of times the ASA retries a failed SSO authentication attempt before letting the request time out, use the **max-retry-attempts** command in the webvpn configuration mode for the specific SSO server type.

To return to the default value, use the **no** form of this command.

max-retry-attempts *retries*

no max-retry-attempts

Syntax Description

retries	The number of times the ASA retries a failed SSO authentication attempt. The range is 1 to 5 retries.

Defaults

The default value for this command is 3.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
config-webvpn-sso-saml	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

Once you have configured the ASA to support SSO authentication, optionally you can adjust two timeout parameters:

- The number of times the ASA retries a failed SSO authentication attempt using the **max-retry-attempts** command.
- The number of seconds before a failed SSO authentication attempt times out (see the **request-timeout** command).

Examples

The following example, entered in webvpn-sso-siteminder configuration mode, configures four authentication retries for the SiteMinder SSO server named my-sso-server:

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

max-uri-length

To restrict HTTP traffic based on the length of the URI in the HTTP request message, use the **max-uri-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allow the message.
drop	Closes the connection.
bytes	Number of bytes, range is 1 to 65535.
log	(Optional) Generate a syslog.
reset	Send a TCP reset message to client and server.

Defaults

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
HTTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

After enabling the **max-uri-length** command, the ASA only allows messages having a URI within the configured limit and otherwise takes the specified action. Use the **action** keyword to cause the ASA to reset the TCP connection and create a syslog entry.

URIs with a length less than or equal to the configured value will be allowed. Otherwise, the specified action will be taken.

Examples

The following example restricts HTTP requests to those with URIs that do not exceed 100 bytes. If a URI is too large, the ASA resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

mcc

To identify the mobile country code and the mobile network code for IMSI prefix filtering, use the **mcc** command in GTP map configuration mode. To remove the configuration, use the **no** form of this command.

mcc *country_code* **mnc** *network_code*

no mcc *country_code* **mnc** *network_code*

Syntax Description

country_code	A non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prepended by 0 to create a three-digit value.
network_code	A two or three-digit value identifying the network code.

Defaults

By default, the ASA does not check for valid MCC/MNC combinations.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command is used for IMSI Prefix filtering. The MCC and MNC in the IMSI of the received packet is compared with the MCC/MNC configured with this command and is dropped if it does not match.

This command must be used to enable IMSI Prefix filtering. You can configure multiple instances to specify permitted MCC and MNC combinations. By default, the ASA does not check the validity of MNC and MCC combinations, so you must verify the validity of the combinations configured. To find more information about MCC and MNC codes, see the ITU E.212 recommendation, *Identification Plan for Land Mobile Stations*.

Examples

The following example identifies traffic for IMSI Prefix filtering with an MCC of 111 and an MNC of 222:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
hostname(config-gtpmap)#
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

media-termination

To specify the media termination instance to use for media connections to the Phone Proxy feature, use the **media-termination** command in global configuration mode.

To remove the media-termination address from the Phone Proxy configuration, use the **no** form of this command.

media-termination *instance_name*

no media-termination *instance_name*

Syntax Description

instance_name	Specifies the name of the interface for which the media termination address is used. Only one media-termination address can be configured per interface.

Defaults

There are no default settings for this command.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.
8.2(1)	This command was updated to allow for using NAT with the media-termination address. The **rtp-min-port** and **rtp-max-ports** keywords were removed from the command syntax and included as a separate command

Usage Guidelines

The ASA must have IP addresses for media termination that meet the following criteria:

For the media termination instance, you can configure a global media-termination address for all interfaces or configure a media-termination address for different interfaces. However, you cannot use a global media-termination address and media-termination addresses configured for each interface at the same time.

If you configure a media termination address for multiple interfaces, you must configure an address on each interface that the ASA uses when communicating with IP phones.

The IP addresses are publicly routable addresses that are unused IP addresses within the address range on that interface.

See CLI configuration guide for the complete list of prerequisites that you must follow when creating the media termination instance and configuring the media termination addresses.

Examples

The following example shows the use of the media-termination address command to specify the IP address to use for media connections:

```
hostname(config-phone-proxy)# media-termination mta_instance1
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

media-type

To set the media type to copper or fiber Gigabit Ethernet, use the **media-type** command in interface configuration mode. The fiber SFP connector is available on the 4GE SSM for the ASA 5500 series adaptive security appliance. To restore the media type setting to the default, use the **no** form of this command.

media-type {**rj45** | **sfp**}

no media-type [**rj45** | **sfp**]

Syntax Description

rj45	(Default) Sets the media type to the copper RJ-45 connector.
sfp	Sets the media type to the fiber SFP connector.

Defaults

The default is **rj45**.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

The **sfp** setting uses a fixed speed (1000 Mbps), so the **speed** command allows you to set whether the interface negotiates link parameters or not. The **duplex** command is not supported for **sfp**.

Examples

The following example sets the media type to SFP:

```
hostname(config)# interface gigabitethernet1/1
hostname(config-if)# media-type sfp
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

member

To assign a context to a resource class, use the **member** command in context configuration mode. To remove the context from the class, use the **no** form of this command.

member *class_name*

no member *class_name*

Syntax Description

class_name	Specifies the class name you created with the **class** command.

Defaults

By default, the context is assigned to the default class.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Context configuration	•	•	—	—	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the ASA, except where maximum limits per context are enforced. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, for example, then you can configure resource management to limit the use of resources per context. The ASA manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

Examples

The following example assigns the context test to the gold class:

```
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
```

Related Commands

Command	Description
class	Creates a resource class.
context	Configures a security context.
limit-resource	Sets the limit for a resource.
show resource allocation	Shows how you allocated resources across classes.
show resource types	Shows the resource types for which you can set limits.

member-interface

To assign a physical interface to a redundant interface, use the **member-interface** command in interface configuration mode. This command is available only for the redundant interface type. You can assign two member interfaces to a redundant interface. To remove a member interface, use the **no** form of this command. You cannot remove both member interfaces from the redundant interface; the redundant interface requires at least one member interface.

member-interface *physical_interface*

no member-interface *physical_interface*

Syntax Description

physical_interface	Identifies the interface ID, such as **gigabitethernet 0/1**. See the **interface** command for accepted values. Both member interfaces must be the same physical type.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Interface configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Both member interfaces must be of the same physical type. For example, both must be Ethernet.

You cannot add a physical interface to the redundant interface if you configured a name for it. You must first remove the name using the **no nameif** command.

Caution If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

The only configuration available to physical interfaces that are part of a redundant interface pair are physical parameters such as **speed** and **duplex** commands, the **description** command, and the **shutdown** command. You can also enter run-time commands like **default** and **help**.

If you shut down the active interface, then the standby interface becomes active.

To change the active interface, enter the **redundant-interface** command.

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the **mac-address** command or the **mac-address auto** command). When the active interface fails over to the standby, the same MAC address is maintained so traffic is not disrupted.

Examples

The following example creates two redundant interfaces:

```
hostname(config)# interface redundant 1
hostname(config-if)# member-interface gigabitethernet 0/0
hostname(config-if)# member-interface gigabitethernet 0/1
hostname(config-if)# interface redundant 2
hostname(config-if)# member-interface gigabitethernet 0/2
hostname(config-if)# member-interface gigabitethernet 0/3
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
debug redundant-interface	Displays debug messages related to redundant interface events or errors.
interface redundant	Creates a redundant interface.
redundant-interface	Changes the active member interface.
show interface	Displays the runtime status and statistics of interfaces.

memberof

To specify a list of group-names that this user is a member of, use the **memberof** command in username attributes configuration mode. To remove this attribute from the configuration, use the **no** form of this command.

memberof *group_1*[,*group_2,...group_n*]

no memberof *group_1*[,*group_2,...group_n*]

Syntax Description

group_1 through group_n	Specifies the groups to which this user belongs.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Username attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Enter a comma-separated list of group names to which this user belongs.

Examples

The following example entered in global configuration mode, creates a username called newuser, then specifies that newuser is a member of the DevTest and management groups:

```
hostname(config)# username newuser nopassword
hostname(config)# username newuser attributes
hostname(config-username)# memberof DevTest,management
hostname(config-username)#
```

Related Commands

Command	Description
clear configure username	Clears the entire username database or just the specified username.
show running-config username	Displays the currently running username configuration for a specified user or for all users.
username	Creates and manages the database of user names.

memory delayed-free-poisoner enable

To enable the delayed free-memory poisoner tool, use the **memory delayed-free-poisoner enable** command in privileged EXEC mode. To disable the delayed free-memory poisoner tool, use the **no** form of this command. The delayed free-memory poisoner tool lets you monitor freed memory for changes after it has been released by an application.

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

Syntax Description

This command has no arguments or keywords.

Defaults

The **memory delayed-free-poisoner enable** command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enabling the delayed free-memory poisoner tool has a significant impact on memory usage and system performance. The command should only be used under the supervision of the Cisco TAC. It should not be run in a production environment during heavy system usage.

When you enable this tool, requests to free memory by the applications running on the ASA are written to a FIFO queue. As each request is written to the queue, each associated byte of memory that is not required by lower-level memory management is “poisoned” by being written with the value 0xcc.

The freed memory requests remain in the queue until more memory is required by an application than is in the free memory pool. When memory is needed, the first freed memory request is pulled from the queue and the poisoned memory is validated.

If the memory is unmodified, it is returned to the lower-level memory pool and the tool reissues the memory request from the application that made the initial request. The process continues until enough memory for the requesting application is freed.

If the poisoned memory has been modified, then the system forces a crash and produces diagnostic output to determine the cause of the crash.

The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically. Validation can also be started manually using the **memory delayed-free-poisoner validate** command.

The **no** form of the command causes all of the memory referenced by the requests in the queue to be returned to the free memory pool without validation and any statistical counters to be cleared.

Examples

The following example enables the delayed free-memory poisoner tool:

```
hostname# memory delayed-free-poisoner enable
```

The following is sample output when the delayed free-memory poisoner tool detects illegal memory reuse:

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                          |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

Table 34-2 describes the significant portion of the output.

Table 34-2 Illegal Memory Usage Output Description

Field	Description
heap region	The address region and size of the region of memory available for use by the requesting application. This is not the same as the requested size, which may be smaller given the manner in which the system may parcel out memory at the time the memory request was made.
memory address	The location in memory where the fault was detected.
byte offset	The byte offset is relative to the beginning of the heap region and can be used to find the field that was modified if the result was used to hold a data structure starting at this address. A value of 0 or that is larger than the heap region byte count may indicate that the problem is an unexpected value in the lower level heap package.

Table 34-2 Illegal Memory Usage Output Description

Field	Description
allocated by/freed by	Instruction addresses where the last malloc/calloc/realloc and free calls where made involving this particular region of memory.
Dumping...	A dump of one or two regions of memory, depending upon how close the detected fault was to the beginning of the region of heap memory. The next eight bytes after any system heap header is the memory used by this tool to hold a hash of various system header values plus the queue linkage. All other bytes in the region until any system heap trailer is encountered should be set to 0xcc.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory delayed-free-poisoner validate

To force validation of all elements in the **memory delayed-free-poisoner** queue, use the **memory delayed-free-poisoner validate** command in privileged EXEC mode.

memory delayed-free-poisoner validate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must enable the delayed free-memory poisoner tool using the **memory delayed-free-poisoner enable** command before issuing the **memory delayed-free-poisoner validate** command.

The **memory delayed-free-poisoner validate** command causes each element of the **memory delayed-free-poisoner** queue to be validated. If an element contains unexpected values, then the system forces a crash and produces diagnostic output to determine the cause of the crash. If no unexpected values are encountered, the elements remain in the queue and are processed normally by the tool; the **memory delayed-free-poisoner validate** command does not cause the memory in the queue to be returned to the system memory pool.

Note The delayed free-memory poisoner tool periodically performs validation on all of the elements of the queue automatically.

Examples

The following example causes all elements in the **memory delayed-free-poisoner** queue to be validated:

```
hostname# memory delayed-free-poisoner validate
```

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
show memory delayed-free-poisoner	Displays a summary of the delayed free-memory poisoner tool queue usage.

memory caller-address

To configure a specific range of program memory for the call tracing, or caller PC, to help isolate memory problems, use the **memory caller-address** command in privileged EXEC mode. The caller PC is the address of the program that called a memory allocation primitive. To remove an address range, use the **no** form of this command.

memory caller-address *startPC endPC*

no memory caller-address

Syntax Description

endPC	Specifies the end address range of the memory block.
startPC	Specifies the start address range of the memory block.

Defaults

The actual caller PC is recorded for memory tracing.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Use the **memory caller-address** command to isolate memory problems to a specific block of memory.

In certain cases the actual caller PC of the memory allocation primitive is a known library function that is used at many places in the program. To isolate individual places in the program, configure the start and end program address of the library function, thereby recording the program address of the caller of the library function.

Note The ASA might experience a temporary reduction in performance when caller-address tracing is enabled.

Examples

The following examples show the address ranges configured with the **memory caller-address** commands, and the resulting display of the **show memory-caller address** command:

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464
```

```
hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a text range of memory to profile.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory-caller address	Displays the address ranges configured on the ASA.

memory profile enable

To enable the monitoring of memory usage (memory profiling), use the **memory profile enable** command in privileged EXEC mode. To disable memory profiling, use the **no** form of this command.

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

Syntax Description

peak_value	Specifies the memory usage threshold at which a snapshot of the memory usage is saved to the peak usage buffer. The contents of this buffer could be analyzed at a later time to determine the peak memory needs of the system.

Defaults

Memory profiling is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

Before enabling memory profiling, you must first configure a memory text range to profile with the **memory profile text** command.

Some memory is held by the profiling system until you enter the **clear memory profile** command. See the output of the **show memory status** command.

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

The following example enables memory profiling:

```
hostname# memory profile enable
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.
show memory profile	Displays information about the memory usage (profiling) of the ASA.

memory profile text

To configure a program text range of memory to profile, use the **memory profile text** command in privileged EXEC mode. To disable, use the **no** form of this command.

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

Syntax Description

all	Specifies the entire text range of the memory block.
endPC	Specifies the end text range of the memory block.
resolution	Specifies the resolution of tracing for the source text region.
startPC	Specifies the start text range of the memory block.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

For a small text range, a resolution of “4” normally traces the call to an instruction. For a larger text range, a coarse resolution is probably enough for the first pass and the range could be narrowed down to a set of smaller regions in the next pass.

After entering the text range with the **memory profile text** command, you must then enter the **memory profile enable** command to begin memory profiling. Memory profiling is disabled by default.

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following example shows how to configure a text range of memory to profile, with a resolution of 4:

```
hostname# memory profile text 0x004018b4 0x004169d0 4
```

The following example displays the configuration of the text range and the status of memory profiling (OFF):

```
hostname# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

Note To begin memory profiling, you must enter the **memory profile enable** command. Memory profiling is disabled by default.

Related Commands

Command	Description
clear memory profile	Clears the buffers held by the memory profiling function.
memory profile enable	Enables the monitoring of memory usage (memory profiling).
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory-caller address	Displays the address ranges configured on the ASA.

memory-size

To configure the amount of memory on the ASA which the various components of WebVPN can access, use the **memory-size** command in webvpn mode. You can configure the amount of memory either as a as a set amount of memory in KB or as a percentage of total memory. To remove a configured memory size, use the **no** form of this command.

Note A reboot is required for the new memory size setting to take effect.

memory-size {percent | kb} *size*

no memory-size [{percent | kb} *size***]**

Syntax Description

kb	Specifies the amount of memory in Kilobytes.
percent	Specifies the amount of memory as a percentage of total memory on the ASA.
size	Specifies the amount of memory, either in KB or as a percentage of total memory.

Defaults

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The configured amount of memory will be allocated immediately. Before configuring this command, check the amount of available memory by using show memory. If a percentage of total memory is used for configuration, ensure that the configured value is below the available percentage. If a Kilobyte value is used for configuration, ensure that the configured value is below the available amount of memory in Kilobytes.

Examples

The following example shows how to configure a WebVPN memory size of 30 per cent:

```
hostname(config)# webvpn
hostname(config-webvpn)# memory-size percent 30
hostname(config-webvpn)#
hostname(config-webvpn)# reload
```

Related Commands

Command	Description
show memory webvpn	Displays WebVPN memory usage statistics.

memory tracking enable

To enable the tracking of heap memory request, use the **memory tracking enable** command in privileged EXEC mode. To disable memory tracking, use the **no** form of this command.

memory tracking enable

no memory tracking enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

Use the **memory tracking enable** command to track heap memory requests. To disable memory tracking, use the **no** form of this command.

Examples

The following example enables tracking heap memory requests:

```
hostname# memory tracking enable
```

Related Commands

Command	Description
clear memory tracking	Clears all currently gathered information.
show memory tracking	Shows currently allocated memory.
show memory tracking address	Lists the size, location, and topmost caller function of each currently allocated piece memory tracked by the tool.
show memory tracking dump	This command shows the size, location, partial callstack, and a memory dump of the given memory address.
show memory tracking detail	Shows various internal details to be used in gaining insight into the tool's internal behavior.

merge-dacl

To merge a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet, use the **merge-dacl** command in aaa-server group configuration mode. To disable the merging of a downloadable ACL with the ACL received in the Cisco AV pair from a RADIUS packet, use the **no** form of this command.

merge dacl {**before_avpair** | **after_avpair**}

no merge dacl

Syntax Description

after_avpair	Specifies that the downloadable ACL entries should be placed after the Cisco AV pair entries. This option applies only to VPN connections. For VPN users, ACLs can be in the form of Cisco AV pair ACLs, downloadable ACLs, and an ACL that is configured on the ASA. This option determines whether or not the downloadable ACL and the AV pair ACL are merged, and does not apply to any ACLs configured on the ASA.
before_avpair	Specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries.

Defaults

The default setting is **no merge dacl**, which specifies that downloadable ACLs will not be merged with Cisco AV pair ACLs.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
AAA-server group configuration	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If both an AV pair and a downloadable ACL are received, the AV pair has priority and is used.

Examples

The following example specifies that the downloadable ACL entries should be placed before the Cisco AV pair entries:

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

Related Commands

Command	Description
aaa-server host	Identifies the server and the AAA server group to which it belongs.
aaa-server protocol	Identifies the server group name and the protocol.
max-failed-attempts	Specifies the maximum number of requests sent to a AAA server in the group before trying the next server..

message-length

To filter GTP packets that do not meet the configured maximum and minimum length, use the **message-length** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form to remove the command.

message-length min *min_bytes* **max** *max_bytes*

no message-length min *min_bytes* **max** *max_bytes*

Syntax Description

max	Specifies the maximum number of bytes allowed in the UDP payload.
max_bytes	The maximum number of bytes in the UDP payload. The range is from 1 to 65536
min	Specifies the minimum number of bytes allowed in the UDP payload
min_bytes	The minimum number of bytes in the UDP payload. The range is from 1 to 65536

Defaults

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
GTP map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The length specified by this command is the sum of the GTP header and the rest of the message, which is the payload of the UDP packet.

Examples

The following example allows messages between 20 bytes and 300 bytes in length:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
hostname(config-gtpmap)#
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.