match r – me

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:

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

Command History

Release	Modification
7.0(2)	This command was added.

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.

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
```

```
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
 [a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(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 mismatch	Matches traffic with a content-type field in the HTTP response that does not match the accept field in the corresponding HTTP request message.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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.

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword

application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

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:

```
ciscoasa
(config)#
 policy-map type inspect http http_map
ciscoasa
(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(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.
match port	Identifies a specific port number in a class map.

Command	Description
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 condition, 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(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.
match any	Includes all traffic in the class map.
match port	Identifies a specific port number in a class map.

Command	Description
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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Table 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:

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

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

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:

```
ciscoasa(config)# route-map name
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
```

```
 rtp 20000 100
ciscoasa(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 selection-mode

To configure a match for the Selection Mode information element in the Create PDP Context request, use the **match selection-mode** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **selection-mode** *mode_value*
no match [**not**] **selection-mode** *mode_value*

Syntax Description

mode_value The Selection Mode information element in the Create PDP Context request. The selection mode specifies the origin of the Access Point Name (APN) in the message, and can be one of the following.

- 0—Verified. The APN was provided by the mobile station or network, and the subscription is verified.
- 1—Mobile Station. The APN was provided by the mobile station, and the subscription is not verified.
- 2—Network. The APN was provided by the network, and the subscription is not verified.
- 3—Reserved, not used.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

This command can be configured in a GTP policy map.

You can filter on the Selection Mode information element in the Create PDP Context request. The selection mode specifies the origin of the Access Point Name (APN) in the message. You can drop and optionally log messages based on these modes. Selection Mode filtering is supported for GTPv1 and GTPv2 only.

Examples

The following example shows how to match selection mode 1 and 2 and drop and log the Create PDP Context messages that have those modes.

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match selection-mode 1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap)# match selection-mode 2
ciscoasa(config-pmap-c)# drop log
```

Related Commands

Command	Description
drop	Drop packets that match the criteria.
log	Log packets that match the criteria.
inspect gtp	Enables GTP application inspection.
policy-map type inspect gtp	Creates or edits a GTP inspection policy map.

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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(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.

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 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(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 service-indicator

To configure a match condition for the service indicator of M3UA messages, use the **match service-indicator** command in policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **service-indicator** *number*
no match [**not**] **service-indicator** *number*

Syntax Description

number The service indicator number, 0-15. See the usage section for a list of supported service indicators.

Command Default

M3UA inspection allows all service indicators.

Command Modes

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

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

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

You can configure this command in an M3UA inspection policy map. You can drop packets based on the service indicator. Following are the available service indicators. Consult M3UA RFCs and documentation for detailed information about these service indicators.

- 0—Signaling Network Management Messages
- 1—Signaling Network Testing and Maintenance Messages
- 2—Signaling Network Testing and Maintenance Special Messages
- 3—SCCP
- 4—Telephone User Part
- 5—ISDN User Part
- 6—Data User Part (call and circuit-related messages)
- 7—Data User Part (facility registration and cancellation messages)
- 8—Reserved for MTP Testing User Part
- 9—Broadband ISDN User Part
- 10—Satellite ISDN User Part

- 11—Reserved
- 12—AAL type 2 Signaling
- 13—Bearer Independent Call Control
- 14—Gateway Control Protocol
- 15—Reserved

Examples

The following example shows how to configure a match condition for M3UA service indicators.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

Related Commands

Command	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.

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 condition, 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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 register 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:

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

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.

Command	Description
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.

matchtunnel-group*name*
nomatchtunnel-group*name*

Syntax Description

name	Text for the tunnel group name.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa(config)# class-map cmap
```

```
ciscoasa(config-cmap)# match
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(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 condition, 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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(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 specify a user or group to whitelist for Cloud Web Security, use the **match user group** command in class-map configuration mode. 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:

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

Command History

Release	Modification
9.0(1)	This command was added.

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:

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
match user group	Matches a user or group for a whitelist.
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.
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.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(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 uuid

To configure a match condition for the universally unique identifier (UUID) of DCERPC messages, use the **match uuid** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

match [**not**] **uuid** *type*
no match [**not**] **uuid** *type*

Syntax Description

type The UUID type to match. One of the following:

- **ms-rpc-epm**—Matches Microsoft RPC EPM messages.
- **ms-rpc-isystemactivator**—Matches ISystemMapper messages.
- **ms-rpc-oxidresolver**—Matches OxidResolver messages.

Command Default

DCERPC inspection allows all message types.

Command Modes

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

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

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This command can be configured in a DCERPC inspection class map or policy map. Use it to filter traffic based on DCERPC UUID. You can then reset or log matching traffic.

Examples

The following example shows how to configure a match condition for the ms-rpc-isyustemactivator UUID in the DCERPC message:

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap

ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```

Related Commands

Command	Description
class-map type inspect	Creates an inspection class map.
policy-map type inspect	Creates an inspection policy map.

match version

To configure a match condition for the GTP version in GTP inspection, use the **match version** command in 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

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command can be configured in a GTP policy map.

Examples

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

```
ciscoasa(config-pmap)# match version 1
```

Related Commands

Command	Description
inspect gtp	Configures inspection of GTP traffic.

max-area-addresses

To configure additional manual addresses for an IS-IS area, use the **max-area-addresses** command in router isis configuration mode. To disable the manual addresses, use the **no** form of this command.

max-area-addresses *number*
no max-area-addresses *number*

Syntax Description

number	The number of manual addresses to add. The range is 3 to 234.

Command Default

No manual addresses are configured for an IS-IS area.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command lets you maximize the size of an IS-IS area by configuring additional manual addresses. You specify the number of addresses you want to add and assign a NET address to create each manual address.

Examples

The following example configures three addresses:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addreses 3
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.

Command	Description
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.

Command	Description
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.

Command	Description
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

max-failed-attempts

To specify the number of failed AAA transactions 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*
nomax-failed-attempts

Syntax Description

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

Command Default

The default value of *number* is 3.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

Examples

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

Command	Description
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.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

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

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

Command	Description
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.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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.

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

To set the maximum time that LSPs can remain in an ASA's database without being refreshed, use the **max-lsp-lifetime** command in router configuration mode. To restore the default lifetime, use the **no** form of this command.

max-lsp-lifetime *seconds*
nomax-lsp-lifetime

Syntax Description

seconds	The lifetime of the LSP in seconds. The range is 1 to 65535.

Command Default

The default is 1200 seconds (20 minutes).

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If the lifetime is exceeded before a refresh LSP arrives, the LSP is dropped from the database.

You might need to adjust the maximum LSP lifetime if you change the LSP refresh interval with the **lsp-refresh-interval** command. LSPs must be periodically refreshed before their lifetimes expire. The value set for the **lsp-refresh-interval** command should be less than the value set for the **max-lsp-lifetime** command; otherwise, LSPs will time out before they are refreshed. If you misconfigure the LSP lifetime to be too low compared to the LSP refresh interval, the software reduces the LSP refresh interval to prevent the LSPs from timing out.

You might prefer higher values for each command to reduce control traffic at the expense of holding stale LSPs from a crashed or unreachable router in the database longer (thus wasting memory) or increasing the risk of undetected bad LSPs staying active (very rare).

Examples

The following example configures an LSP lifetime of 40 minutes:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

maximum-paths (BGP)

To control the maximum number of parallel BGP routes that can be installed in a routing table, use the maximum-paths command in address-family configuration mode. To restore the default value, use the no form of this command.

maximum-paths [**ibgp**] *number-of-paths*
no maximum-paths [**ibgp**] *number-of-paths*

Syntax Description

ibgp	(Optional) This will enable you to control the maximum number of internal BGP routes that can be installed to the routing table.
number-of-paths	Number of routes to install to the routing table.

Command Default

By default, BGP installs only one best path in the routing table.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The maximum-paths command is used to configure equal-cost or unequal-cost multipath load sharing for BGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to BGP peers when BGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path.

To configure BGP equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.

Examples

The following example configuration installs two parallel iBGP paths:

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

Related Commands

Commands	Description
show bgp	Displays entries in the BGP routing table.

maximum-paths (IS-IS)

To configure multipath load sharing for IS-IS protocol, use the **maximum-paths** command in router isis configuration mode. To disable multipath load sharing for ISIS routes, use the **no** form of this command.

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

Syntax Description

number-of-paths	The number of routes to install to the routing table. The range is 1 to 8.

Command Default

By default, IS-IS only installs one best path in the routing table.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

The **maximum-paths** command is used to configure ISIS multipath load sharing when ECMP is configured in the ASA.

Examples

The following example configures the maximum paths in the routing table at eight:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.

Command	Description
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.

Command	Description
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.

Command	Description
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

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*integerrange*

Syntax Description

integer	0 - 10000
range	KB

Command Default

1000 KB

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

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:

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

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.

Command	Description
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 size of an object to cache.

max-retry-attempts (Deprecated)

Note The last supported release for this command was Version 9.5(1).

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*
nomax-retry-attempts

Syntax Description

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

Command Default

The default value for this command is 3.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class-map type regex configuration	• Yes	—	• Yes	—	—
config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

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:

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

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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.

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

mcast-group

To specify the multicast group for a VXLAN VNI interface, use the **mcast-group** command in interface configuration mode. To remove the group, use the **no** form of this command.

mcast-group *mcast_ip*
nomcast-group

Syntax Description

mcast_ip	Sets the multicast group IP address, IPv4 or IPv6.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.
9.20(1)	This command now supports IPv6.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface with the **mcast-group** command (or on the VTEP as a whole).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

If you do not set the multicast group for the VNI interface, the default group from the VTEP source interface configuration is used, if available (**default-mcast-group** command). If you manually set a VTEP peer IP for the VTEP source interface using the **peer ip** command, you cannot specify a multicast group for the VNI interface. Multicast is not supported in multiple context mode.

Examples

The following example configures the VNI 1 interface and specifies a multicast group of 236.0.0.100:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Command	Description
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

mcc

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

[**drop**] **mcc** *country_code* **mnc** *network_code*
no [**drop**] **mcc** *country_code* **mnc** *network_code*

Syntax Description

drop	Specifies that connections that match the prefix combination should be dropped. Thus, your combinations indicate the unwanted prefixes. Without this keyword, connections must match the prefix combinations to be allowed. All prefix filtering within a given map must be consistent, either all drop or all allow.
country_code	A non-zero, three-digit value identifying the mobile country code. One or two-digit entries will be prefixed by 0 to create a three-digit value.
network_code	A two or three-digit value identifying the network code.

Command Default

By default, GTP inspection does not check for valid MCC/MNC combinations.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
9.16(1)	The **drop** keyword was added.

Usage Guidelines

You can enter the command as many times as necessary to specify all targeted MCC/MNC pairs, but all commands within the policy map must be either **mcc** or **drop mcc**. You cannot combine these commands.

By default, GTP inspection does not check for valid Mobile Country Code (MCC)/Mobile Network Code (MNC) combinations. If you configure IMSI prefix filtering, the MCC and MNC in the IMSI of the received packet is compared with the configured MCC/MNC combinations. The system then takes one of the following actions based on the command:

- **mcc** command—The packet is dropped if it does not match.

- **drop mcc** command—The packet is dropped if it does match.

The Mobile Country Code is a non-zero, three-digit value; add zeros as a prefix for one- or two-digit values. The Mobile Network Code is a two- or three-digit value.

Add all MCC and MNC combinations you want to either permit or to drop. 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:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

media-termination (Deprecated)

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

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

media-terminationinstance_name
nomedia-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.

Command Default

There are no default settings for this command.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.
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.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

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:

```
ciscoasa(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.

Command Default

The default is **rj45**.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was added.

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:

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(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.

Command	Description
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*
nomember*class_name*

Syntax Description

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

Command Default

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:

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

Command History

Release	Modification
7.2(1)	This command was added.

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:

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

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(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.

Command Default

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(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 appcache-threshold enable

To enable the memory application cache threshold, use the **memory appcache-threshold enable** command in the configuration mode. To disable the **memory appcache-threshold,** use the **no** form of this command.

memoryappcache-thresholdenable
nomemoryappcache-thresholdenable

Syntax Description

This command has no arguments or keywords.

Command Default

This **memory appcache-threshold enable** command is enabled on ASA 5585-X FirePOWER SSP-60 (5585-60) by default.

Command Modes

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

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

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

Enabling memory appcache-threshold restricts application cache allocations after reaching certain memory threshold so that there is a reservation of memory to maintain stability and manageability of the device.

In ASA 9.10.1 release, the memory appcache-threshold feature was implemented on 5585-60 to restrict the application cache allocations for through-the-box connections only.

This command configures the application cache allocation threshold to 85%of the system memory. When the memory usage reaches the threshold level, the new through-the-box connections to the device are dropped.

The **no** form of the command causes all of the memory allocation restriction to be freed for usage without validation. The current statistical counters are retained to maintain the troubleshooting history until the **clear memory appcache-threshold** command is executed.

For 9.10.1 release, only SNP Conn Core 00 application cache type is managed. This name is aligned with the output of “show mem app-cache”.

Examples

The following example enables the appcache-memory threshold:

```
ciscoasa(config)# memory appcache-threshold enable
```

Related Commands

Command	Description
show memory appcache-threshold	Show the status and hit count of memory appcache-threshold
clear memory appcache-threshold	Clear the hit count of memory appcache-threshold

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.

memorydelayed-free-poisonerenable
nomemorydelayed-free-poisonerenable

Syntax Description

This command has no arguments or keywords.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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
```

<xref> describes the significant portion of the output.

Table 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.
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.

memorydelayed-free-poisonervalidate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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:

```
ciscoasa# 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.

memorycaller-address*startPCendPC*
nomemorycaller-address

Syntax Description

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

Command Default

The actual caller PC is recorded for memory tracing.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was added.

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:

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08

ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
```

```
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# 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 logging

To enable memory logging, use the **memory logging** command in global configuration mode. To disable memory logging, use the **no** form of this command.

memory logging [**1024-4194304**] [**wrap**] [**size** [**1-2147483647**]] [**process** *process-name*] [**context** *context-name*]
nomemorylogging

Syntax Description

1024-4194304	Specifies the number of logging entries in the memory logging buffer. This is the only required argument to specify.
context *context-name*	Specifies the virtual context and context name to monitor.
process *process-name*	Specifies the process and process name to monitor. **Note** The Checkheaps process is completely ignored as a process because it uses the memory allocator in a non-standard way.
size 1-2147483647	Specifies the size and number of entries to monitor.
wrap	Save the buffer when it wraps. It can only be saved once. If it wraps multiple times, it can be overwritten. When the buffer wraps, a trigger is sent to the event manager to enable saving of the data.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

To change memory logging parameters, you must disable it, then reenable it.

Examples

The following example enables memory logging:

```
ciscoasa
```

```
(config)#
memory logging 202980
```

Related Commands

Command	Description
event memory-logging-wrap	Enables response to memory logging wrap events.
show memory logging	Displays memory logging results.

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.

memoryprofileenablepeak*peak_value*
nomemoryprofileenablepeak*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.

Command Default

Memory profiling is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was added.

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:

```
ciscoasa# memory profile enable
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.

Command	Description
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.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was added.

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:

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

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

```
ciscoasa# 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.

Command Default

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was added.

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:

```
ciscoasa
(config)#
 webvpn
ciscoasa
```

```
(config-webvpn)#
 memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(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.

memorytrackingenable
nomemorytrackingenable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(8)	This command was added.

Usage Guidelines

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

Before you enable memory tracking, ensure to change the default interval and count value in the app-agent heartbeat command to the ones below:

app-agent heartbeat interval 6000 retry-count 6

Examples

The following example enables tracking heap memory requests:

```
ciscoasa# 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.

Command	Description
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.

memory-utilization

Use the memory utilization command to configure ASA to automatically reboot or crash once the system memory is used up at a pre-defined level. Once the memory usage reaches the configured threshold limit, the system automatically reloads.Threshold value could be in the range of 90-99%.

memory-utilization reload-threshold < **%** >
memory-utilization reload-threshold < **%** > [**crashinfo**]

Syntax Description

reload-threshold	Specifies the system memory threshold limit.
crashinfo	(Optional) Specifies that if used, the crash information is saved before a system reload.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

It is recommended that you DO NOT configure this feature on those systems that are known to experience environments, where very high memory utilization is commonly observed. Use the optional crashinfo argument to generate a crash information file before a system reload.

Examples

The following example displays how to configure memory utilization feature on ASA:

```
ciscoasa# memory-utilization reload-threshold 95
```

Related Commands

Command	Description
memory profile text	Configures a text range of memory to profile.
memory profile enable	Enables the monitoring of memory usage (memory profiling).
clear memory profile	Clears the buffers held by the memory profiling function.

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.

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** }
nomergedacl

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.

Command Default

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:

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

Command History

Release	Modification
8.0(2)	This command was added.

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:

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(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 DNS packets that do not meet the configured maximum length, use the message-length command in parameters configuration mode. Use the **no** form to remove the command.

message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }
no message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }

Syntax Description

length	The maximum number of bytes allowed in a DNS message, from 512 to 65535.
client {*length* | **auto**}	The maximum number of bytes allowed in a client DNS message, from 512 to 65535, or **auto** to set the maximum length to the value in the Resource Record.
server {*length* | **auto**}	The maximum number of bytes allowed in a server DNS message, from 512 to 65535, or **auto** to set the maximum length to the value in the Resource Record.

Command Default

The default inspection sets DNS maximum message length to 512, and client length to **auto**.

Command Modes

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

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

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

You can configure the maximum DNS message length as parameter in a DNS inspection map.

Examples

The following example shows how to configure the maximum DNS message length in a DNS inspection policy map:

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

Related Commands

Commands	Description
parameter	Enters parameter configuration mode while in policy map configuration mode.

Commands	Description
policy-map type inspect dns	Creates a DNS inspection policy map.

message-tag-validation

To validate the content of certain fields in M3UA messages, use the **message-tag-validation** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect m3ua** command. Use the **no** form of this command to remove the setting.

message-tag-validation { **dupu** | **error** | **notify** }
no message-tag-validation { **dupu** | **error** | **notify** }

Syntax Description

dupu	Enable validation for the Destination User Part Unavailable (DUPU) message. The User/Cause field must be present, and it must contain only valid cause and user codes.
error	Enable validation for the Error message. All mandatory fields must be present and contain only allowed values. Each error message must contain the required fields for that error code.
notify	Enable validation for the Notify message. The status type and status information fields must contain allowed values only.

Command Default

The default setting for this command is disabled.

Command Modes

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

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

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use this command to ensure that the content of certain fields are checked and validated for the specified M3UA message type. Messages that fail validation are dropped.

Examples

The following example enables message validation for DUPU, Error, and Notify messages in M3UA inspection.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
policy-map type inspect	Creates an inspection policy map.
show service-policy inspect m3ua	Displays M3UA statistics.

metric

To globally change the metric value for all IS-IS interfaces, use the **metric** command in router isis configuration mode. To disable the metric value and reinstate the default metric value of 10, use the **no** form of this command.

metric *default-value* [**level-1** | **level-2**]
no metric *default-value* [**level-1** | **level-2**]

Syntax Description

default-value	The metric value to be assigned to the link and used to calculate the path cost via the links to destinations. The range is 1 to 63.
level-1	(Optional) Sets IS-IS Level 1 IPv4 or IPv6 metric.
level-2	(Optional) Sets IS-IS Level 2 IPv4 or IPv6 metric.

Command Default

The default is 10.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

When you need to change the default metric value for all IS-IS interfaces, we recommend that you use the **metric** command in to configure all interfaces globally. Globally configuring the metric values prevents user errors, such as unintentionally removing a set metric from an interface without configuring a new value and unintentionally allowing the interface to revert to the default metric of 10, thereby becoming a highly preferred interface in the network.

Once you enter the **metric** command to change the default IS-IS interface metric value, an enabled interface uses the new value instead of the default value of 10. Passive interfaces continue to use the metric value of 0.

Examples

The following example configures the IS-IS interfaces with a global metric of 111:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

metric-style

To configure a router running IS-IS so that it generates and accepts only new-style type, length, value objects (TLVs), use the **metric-style** command in router isis configuration mode. To disable this function, use the **no** form of this command.

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
no metric [**level-1** | **level-2** | **level-1-2**]

Syntax Description

narrow	Instructs the ASA to use the old style of TLVs with the narrow metric.
transition	(Optional) Instructs the ASA to accept both old- and new-style TLVs during transition.
wide	Instructs the ASA to use the new style of TLVs to carry the wider metric.
level-1	(Optional) Enables this command on routing Level 1.
level-2	(Optional) Enables this command on routing Level 2.
level-1-2	(Optional) Instructs the router to accept both old- and new-style TLVs.

Command Default

The default is 10.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

If you enter the metric-style wide command, an ASA generates and accepts only new-style TLVs. Therefore, the ASA uses less memory and other resources than it would if it generated both old-style and new-style TLVs.

This style is appropriate for enabling MPLS traffic engineering across an entire network.

Examples

The following example configures the ASA to generate and accept new-style TLVs on Level 1:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.