CHAPTER 20

mac-address-table aging-time through multicast-routing Commands

mac-address-table aging-time

To set the timeout for MAC address table entries, use the **mac-address-table aging-time** command in global configuration mode. To restore the default value of 5 minutes, use the **no** form of this command.

mac-address-table aging-time *timeout_value*

no mac-address-table aging-time

Syntax Description

timeout_value	The time a MAC address entry stays in the MAC address table before timing out, between 5 and 720 minutes (12 hours). 5 minutes is the default.

Defaults

The default timeout is 5 minutes.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples

The following example sets the MAC address timeout to 10 minutes:

```
hostname(config)# mac-address-timeout aging time 10
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

mac-address-table static

To add a static entry to the MAC address table, use the **mac-address-table static** command in global configuration mode. To remove a static entry, use the **no** form of this command.

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

Syntax Description

interface_name	Sets the source interface.
mac_address	Sets the MAC address you want to add to the table.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

Normally, MAC addresses are added to the MAC address table dynamically as traffic from a particular MAC address enters an interface. You can add static MAC addresses to the MAC address table if desired. One benefit to adding static entries is to guard against MAC spoofing. If a client with the same MAC address as a static entry attempts to send traffic to an interface that does not match the static entry, then the FWSM drops the traffic and generates a system message.

Examples

The following example adds a static MAC address entry to the MAC address table:

```
hostname(config)# mac-address-table static inside 0010.7cbe.6101
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.

Command	Description
mac-learn	Disables MAC address learning.
show mac-address-table	Shows MAC address table entries.

mac-learn

To disable MAC address learning for an interface, use the **mac-learn** command in global configuration mode. To reenable MAC address learning, use the **no** form of this command.

mac-learn *interface_name* **disable**

no mac-learn *interface_name* **disable**

Syntax Description

disable	Disables MAC learning.
interface_name	Sets the interface on which you want to disable MAC learning.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, each interface automatically learns the MAC addresses of entering traffic, and the FWSM adds corresponding entries to the MAC address table. You can disable MAC address learning if desired.

Examples

The following example disables MAC learning on the outside interface:

```
hostname(config)# mac-learn outside disable
```

Related Commands

Command	Description
clear configure mac-learn	Sets the **mac-learn** configuration to the default.
firewall transparent	Sets the firewall mode to transparent.
mac-address-table static	Adds static MAC address entries to the MAC address table.

Command	Description
show mac-address-table	Shows the MAC address table, including dynamic and static entries.
show running-config mac-learn	Shows the **mac-learn** configuration.

mac-list

To specify a list of MAC addresses to be used to exempt MAC addresses from authentication and/or authorization, use the **mac-list** command in global configuration mode. To remove a MAC list entry, use the **no** form of this command.

mac-list *id* {**deny** | **permit**} *mac macmask*

no mac-list *id* {**deny** | **permit**} *mac macmask*

Syntax Description

deny	Indicates that traffic matching this MAC address does not match the MAC list and is subject to both authentication and authorization when specified in the **aaa mac-exempt** command. You might need to add a deny entry to the MAC list if you permit a range of MAC addresses using a MAC address mask such as ffff.ffff.0000, and you want to force a MAC address in that range to be authenticated and authorized.
id	Specifies a hexadecimal MAC access list number. To group a set of MAC addresses, enter the **mac-list** command as many times as needed with the same ID value. The order of entries matters, because the packet uses the first entry it matches, as opposed to a best match scenario. If you have a permit entry, and you want to deny an address that is allowed by the permit entry, be sure to enter the deny entry before the permit entry.
mac	Specifies the source MAC address in 12-digit hexadecimal form; that is, nnnn.nnnn.nnnn
macmask	Specifies the portion of the MAC address that should be used for matching. For example, ffff.ffff.ffff matches the MAC address exactly. ffff.ffff.0000 matches only the first 8 digits.
permit	Indicates that traffic matching this MAC address matches the MAC list and is exempt from both authentication and authorization when specified in the **aaa mac-exempt** command.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To enable MAC address exemption from authentication and authorization, use the **aaa mac-exempt** command. You can only add one instance of the **aaa mac-exempt** command, so be sure that your MAC list includes all the MAC addresses you want to exempt. You can create multiple MAC lists, but you can only use one at a time.

Examples

The following example bypasses authentication for a single MAC address:

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

The following entry bypasses authentication for all Cisco IP Phones, which have the hardware ID 0003.E3:

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

The following example bypasses authentication for a a group of MAC addresses except for 00a0.c95d.02b2. Enter the deny statement before the permit statement, because 00a0.c95d.02b2 matches the permit statement as well, and if it is first, the deny statement will never be matched.

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

Related Commands

Command	Description
aaa authentication	Enables user authentication.
aaa authorization	Enables user authorization services.
aaa mac-exempt	Exempts a list of MAC addresses from authentication and authorization.
clear configure mac-list	Removes a list of MAC addresses previously specified by the **mac-list** command.
show running-config mac-list	Displays a list of MAC addresses previously specified in the **mac-list** command.

management-access

To allow management access to an interface other than the one you entered the FWSM from, use the **management-access** command in global configuration mode. To disable this access, use the **no** form of this command.

management-access *mgmt_if*

no management-access *mgmt_if*

Syntax Description

mgmt_if	Specifies the name of the management interface you want to access when entering the FWSM from another interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command allows you to connect to an interface other than the one you entered the FWSM from. For example, if you enter the FWSM from the outside interface, this command lets you connect to the inside interface using Telnet; or you can ping the inside interface when entering from the outside interface.

You can define only one management interface.

The **management-access** command is supported for the following through an IPSec VPN tunnel only:

- SNMP polls to the management interface
- HTTPS requests to the management interface
- ASDM access to the management interface
- Telnet access to the management interface
- SSH access to the management interface
- Ping to the management interface
- Syslog polls to the management interface
- NTP requests the management interface

Examples

The following example shows how to configure a firewall interface named "inside" as the management access interface:

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an interface for management access of the FWSM.
show management-access	Displays the name of the interface configured for management access.

management-only

To set an interface to accept management traffic only, use the **management-only** command in interface configuration mode. To allow through traffic, use the **no** form of this command.

management-only

no management-only

Syntax Description

This command has no arguments or keywords.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enables management-only mode on a subinterface:

```
hostname(config)# interface gigabitethernet2.1
hostname(config-subif)# management-only
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

mask

To mask out part of the packet that matches a **match** command or class map when using Modular Policy Framework, use the **mask** command in match or class configuration mode. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. To disable this action, use the **no** form of this command.

mask [**log**]

no mask [**log**]

Syntax Description

log	(Optional) Logs the match. The system log message number depends on the application.

Defaults

No default behaviors or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This mask action is available in an inspection policy map for application traffic; however, not all applications allow this action. For example, you can you use **mask** command for the HTTP application inspection to mask text in a message header before allowing the traffic through the FWSM.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **mask** command to mask part of the packet that matches the **match** command or **class** command.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http** *http_policy_map* command where *http_policy_map* is the name of the inspection policy map.

Examples

The following example masks the HTTP response if the content-type field does not match the accept field in the corresponding HTTP request message before allowing the traffic through the FWSM:

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# mask log
```

Related Commands

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

mask-syst-reply

To hide the FTP server response from clients, use the **mask-syst-reply** command in ftp map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the **no** form of this command.

mask-syst-reply

no mask-syst-reply

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the mask-syst-reply command with strict FTP inspection to protect the FTP server system from clients. After enabling this command, the servers replies to the **syst** command are replaced by a series of Xs.

Examples

The following example causes the FWSM to replace the FTP server replies to the syst command with Xs:

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-map)# exit
```

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables ftp map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.
request-command deny	Specifies FTP commands to disallow.

match access-list

When using the Modular Policy Framework, use an access list to identify traffic to which you want to apply actions by using the **match access-list** command in class-map configuration mode. To remove the **match access-list** command, use the **no** form of this command.

match access-list *access_list_name*

no match access-list *access_list_name*

Syntax Description

access_list_name	Specifies the name of an access list to be used as match criteria.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

   After you enter the **class-map** command, you can enter the **match access-list** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You can only include one **match access-list** command in the class map, and you cannot combine it with other types of **match** commands. The exception is if you define the **match default-inspection-traffic** command which matches the default TCP and UDP ports used by all applications that the FWSM can inspect, then you can narrow the traffic to match using a **match access-list** command. Because the **match default-inspection-traffic** command specifies the ports and protocols to match, any ports or protocols in the access list are ignored.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

The following example creates three Layer 3/4 class maps that match three access lists:

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

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 any

When using the Modular Policy Framework, match all traffic to which you want to apply actions by using the **match any** command in class-map configuration mode. To remove the **match any** command, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

   After you enter the **class-map** command, you can enter the **match any** command to identify all traffic. Alternatively, you can enter a different type of **match** command, such as the **match port** command. You cannot combine the **match any** command with other types of **match** commands.
2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match any
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
clear configure class-map	Removes all class maps.
match access-list	Matches traffic according to an access list.
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 body

To configure a match condition on the length or length of a line of an ESMTP body message, use the **match body** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **body [length | line length] gt** *bytes*

no match [**not**] **body [length | line length] gt** *bytes*

Syntax Description

length	Specifies the length of an ESMTP body message.
line length	Specifies the length of a line of an ESMTP body message.
bytes	Specifies the number to match in bytes.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for a body line length in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match body line length gt 1000
```

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 called-party

To configure a match condition on the H.323 called party, use the **match called-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **called-party** [**regex** *regex*]

no match [**not**] **match** [**not**] **called-party** [**regex** *regex*]

Syntax Description

regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the called party in an H.323 inspection class map:

```
hostname(config-cmap)# match called-party regex caller1
```

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 calling-party

To configure a match condition on the H.323 calling party, use the **match calling-party** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **calling-party** [**regex** *regex*]

no match [**not**] **match** [**not**] **calling-party** [**regex** *regex*]

Syntax Description

regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the calling party in an H.323 inspection class map:

```
hostname(config-cmap)# match calling-party regex caller1
```

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 cmd

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

match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

no match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

Syntax Description

verb *verb*	Specifies the ESMTP command verb.
line length gt *bytes*	Specifies the length of a line.
RCPT count gt *recipients_number*	Specifies the number of recipient email addresses.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition in an ESMTP inspection policy map for the verb (method) NOOP exchanged in the ESMTP transaction:

```
hostname(config-pmap)# match cmd verb NOOP
```

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 content

To configure a match condition on the SIP content header, use the **match content** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **content [regex** *regex*]

no match [**not**] **match** [**not**] **content [regex** *regex*]

Syntax Description

regex *regex*	Specifies to match on the regular expression.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for the content in a SIP inspection class map:

```
hostname(config-cmap)# match content regex sample
```

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 default-inspection-traffic

To specify default traffic for the inspect commands in a class map, use the **match default-inspection-traffic** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match default-inspection-traffic

no match default-inspection-traffic

Syntax Description

This command has no arguments or keywords.

Defaults

See the "Usage Guidelines" section for the default traffic of each inspection.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

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

Using the **match default-inspection-traffic** command, you can match default traffic for the individual **inspect** commands. The **match default-inspection-traffic** command can be used in conjunction with one other match command, which is typically an access-list in the form of **permit ip** *src-ip dst-ip*.

The rule for combining a second **match** command with the **match default-inspection-traffic** command is to specify the protocol and port information using the **match default-inspection-traffic** command and specify all other information (such as IP addresses) using the second **match** command. Any protocol or port information specified in the second **match** command is ignored with respect to the **inspect** commands.

For instance, port 65535 specified in the example below is ignored:

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# match port 65535
```

Default traffic for inspections are as follows:

Inspection Type	Protocol Type	Source Port	Destination Port
ctiqbe	tcp	N/A	1748
dns	udp	53	53
ftp	tcp	N/A	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	N/A	1720
h323 ras	udp	N/A	1718-1719
http	tcp	N/A	80
icmp	icmp	N/A	N/A
ils	tcp	N/A	389
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	N/A
rpc	udp	111	111
rsh	tcp	N/A	514
rtsp	tcp	N/A	554
sip	tcp,udp	N/A	5060
skinny	tcp	N/A	2000
smtp	tcp	N/A	25
sqlnet	tcp	N/A	1521
tftp	udp	N/A	69
xdmcp	udp	177	177

Examples

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
```

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 ehlo-reply-parameter

To configure a match condition on the ESMTP ehlo reply parameter, use the **match ehlo-reply-parameter** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **ehlo-reply-parameter** *parameter*

no match [**not**] **ehlo-reply-parameter** *parameter*

Syntax Description

parameter	Specifies the ehlo reply parameter.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for an ehlo reply parameter in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match ehlo-reply-parameter auth
```

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 header

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

match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

no match [**not**] **header [[length | line length] gt** *bytes* | **to-fields count gt** *to_fields_number*]

Syntax Description

length gt *bytes*	Specifies to match on the length of the ESMTP header message.
line length gt bytes	Specifies to match on the length of a line of an ESMTP header message.
to-fields count gt *to_fields_number*	Specifies to match on the number of To: fields.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

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

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match header length gt 512
```

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 im-subscriber

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

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for a SIP IM subscriber in a SIP inspection class map:

```
hostname(config-cmap)# match im-subscriber regex class im_sender
```

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 interface

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in route-map configuration mode. To remove the match interface entry, use the **no** form of this command.

match interface *interface-name...*

no match interface *interface-name...*

Syntax Description

interface-name	Name of the interface as specified by the **nameif** command. You can specify multiple interface names.

Defaults

No match interfaces are defined.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the interface-type interface-number arguments.

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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 give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions that are given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria. If there is more than one interface specified in the **match** command. then the **no match interface** *interface-name* can be used to remove a single interface.

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. If you want to modify only some data, you must configure a second route map section and specify an explicit match.

Examples

The following example shows that the routes with their next hop outside is distributed:

```
hostname(config)# route-map name
hostname(config-route-map)# match interface outside
```

Related Commands

Command	Description
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 ip route-source	Redistributes routes that have been advertised by routers and access servers at the address that is specified by the access lists.
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 invalid-recipients

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

match [**not**] **invalid-recipients count gt** *number*

no match [**not**] **invalid-recipients count gt** *number*

Syntax Description

count gt *number*	Specifies to match on the invalid recipient number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for invalid recipients count in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match invalid-recipients count gt 1000
```

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 ip address

To redistribute any routes that have a route address or match packet that is passed by one of the access lists specified, use the **match ip address** command in route-map configuration mode. To restore the default settings, use the **no** form of this command.

match ip address {*acl...*}

no match ip address {*acl...*}

Syntax Description

acl	Specifies an ACL by name. You can specify multiple ACLs.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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.

Examples

The following example shows how to redistribute internal routes:

```
hostname(config)# route-map name
hostname(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

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 ip next-hop

To redistribute any routes that have a next-hop router address that is passed by one of the access lists specified, use the **match ip next-hop** command in route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip next-hop {*acl...* | **prefix-list** *prefix_list*}

no match ip next-hop {*acl...* | **prefix-list** *prefix_list*}

Syntax Description

acl	Name of an ACL. You can specify multiple ACLs.
prefix-list prefix_list	Name of prefix list.

Defaults

Routes are distributed freely, without being required to match a next-hop address.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-name argument.

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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.

When you are passing routes through a route map, 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.

Examples

The following example shows how to distribute routes that have a next-hop router address passed by access list acl_dmz1 or acl_dmz2:

```
hostname# route-map name
hostname(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

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 ip route-source

To redistribute routes that have been advertised by routers and access servers at the address that is specified by the access lists, use the **match ip route-source** command in the route-map configuration mode. To remove the next-hop entry, use the **no** form of this command.

match ip route-source {*acl...* | **prefix-list** *prefix_list*}

no match ip route-source {*acl...* | **prefix-list** *prefix_list*}

Syntax Description

acl	Name of an ACL. You can specify multiple ACLs.
prefix_list	Name of prefix list.

Defaults

No filtering on a route source.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-name argument.

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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. The next-hop and source-router address of the route are not the same in some situations.

Examples

The following example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by access lists acl_dmz1 and acl_dmz2:

```
hostname(config)# route-map name
hostname(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

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 message-path

To configure a match condition for the path taken by a SIP message as specified in the Via header field, use the **match message-path** command in class-map or policy-map configuration mode. To remove the match condtion, use the **no** form of this command.

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config-cmap)# match message-path regex class sip_message
```

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 metric

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

match metric *number*

no match metric *number*

Syntax Description

number	Route metric; valid values are from 0 to 4294967295.

Defaults

No filtering on a metric value.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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. The **match** commands can be given in any order, and 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.

Examples

The following example shows how to redistribute routes with the metric 5:

```
hostname(config)# route-map name
hostname(config-route-map)# match metric 5
```

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.
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 mime

To configure a match condition on the ESMTP mime encoding type, mime filename length, or mime file type, use the **match mime** command in policy-map configuration mode. To disable this feature, use the **no** form of this command.

match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex*]

no match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex*]

Syntax Description

encoding *type*	Specifies to match on the encoding type.
filename length gt *bytes*	Specifies to match on the filename length.
filetype *regex*	Specifies to match on the file type.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for a mime filename length in an ESMTP inspection policy map:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match mime filename length gt 255
```

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 port

When using the Modular Policy Framework, match the TCP or UDP ports to which you want to apply actions by using the **match port** command in class-map configuration mode. To remove the **match port** command, use the **no** form of this command.

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

Syntax Description

eq *port*	Specifies a single port name or number.
range *beg_port end_port*	Specifies beginning and ending port range values between 1 and 65535.
tcp	Specifies a TCP port.
udp	Specifies a UDP port.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Configuring Modular Policy Framework consists of four tasks:

1. Identify the Layer 3 and 4 traffic to which you want to apply actions using the **class-map** command.

   After you enter the **class-map** command, you can enter the **match port** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** command. You can only include one **match port** command in the class map, and you cannot combine it with other types of **match** commands.

2. (Application inspection only) Define special actions for application inspection traffic using the **policy-map type inspect** command.
3. Apply actions to the Layer 3 and 4 traffic using the **policy-map** command.
4. Activate the actions on an interface using the **service-policy** command.

Examples

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 8080
```

Related Commands

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

match request-method

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

match request, response

To perform matches on HTTP headers for HTTP inspection, use the **match request, response** command in policy-map configuration mode. To not match on HTTP headers, use the **no** form of this command.

match [**not**] { **request** | **response** } **header** { *header_name* | **content-type** | **transfer-encoding** | **length gt** *bytes* | **count** *number* } { *built_in_regex* | **regex class** *class_map_name* | **regex** *regex_name* | **length gt** *bytes* | **count** *number* }

no match [**not**] { **request** | **response** } **header** { *header_name* | **content-type** | **transfer-encoding** | **length gt** *bytes* | **count** *number* } { *built_in_regex* | **regex class** *class_map_name* | **regex** *regex_name* | **length gt** *bytes* | **count** *number* }

Syntax Description

header	Specifies the of the HTTP message.
header_name	Specifies the name of the HTTP header to match.
content-type	Specifies to match the content type in the response to the accept types in the request.
transfer-encoding	
length gt *bytes*	Specifies to match on the length of the HTTP header message.
count *number*	
built_in_regex	Specifies the built-in regex for content type, method, or transfer encoding.
regex class *class_map_name*	Specifies the name of the class map of regex type.
regex regex_name	Specifies the name of the regular expression configured using the regex command.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Total Header Length Check

The following command performs a check to determine if the entire header portion of the HTTP message is greater than *bytes*:

[no] match [not] { request | response } header length gt <bytes>

Count of All Header Fields Check

The following command performs a check to determine if the number of header fields in the HTTP message is greater than *number*:

```
hostname(config-pmap)# [no] match [not] { request | response } header count number
```

Total Header Regex Check

The following command performs a regex scan of the entire header of the HTTP message. This can be useful for checking for non-ASCII characters.

```
hostname(config-pmap)# [no] match [not] { request | response }  header regex  { class
class_map_name | regex_name }
```

Specified Header Field Length Check

The following command performs a length check of an individual header field to ensure that it is less than *bytes* characters long:

```
hostname(config-pmap)# [no] match [not] { request | response }  header { header_name |
content-type | transfer-encoding } length gt bytes
```

Note Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

```
hostname(config)# regex foo [Ff][Oo][Oo]
hostname(config)# policy-map
hostname(config-pmap)# match request header foo length gt 99
```

Specified Header Field Count Check

The following command will count the instances of the specified field and perform a check to ensure that it occurs less than <number> of times.

```
hostname(config-pmap)# [no] match [not] { request | response }  header { header_name |
content-type | transfer-encoding } count number
```

Note Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

```
hostname(config)# regex foo [Ff][Oo][Oo]
hostname(config)# policy-map
hostname(config-pmap)# match request header foo count 3
```

Specified Header Field Regex Value Check

The following command will attempt to match the specified regex or regex class against value of the specified field:

```
hostname(config-pmap)# [no] match [not] { request | response }  header { header_name |
content-type | transfer-encoding } regex { class class_map_name | regex_name }
```

Note Unless the user specifies the **content-type** or **transfer-encoding** keywords, the *header_name* argument must be predefined using the **regex** command. For example:

hostname(config)# **regex foo** [**Ff**][**Oo**][**Oo**]

```
hostname(config)# regex  bar [Bb][Aa][Rr]
hostname(config)# policy-map
hostname(config-pmap)# match request header foo regex bar
```

Content-type Header Check

In addition to the length, count and regex checks described above, the user can perform various special checks on the content type field:

- The user can match the mime-type in the header's value against a set of built-in keywords for the known mime-types.
- The user can also specify that the mime-type must one of the built-ins by using the "unknown" keyword.
- The user can also cause content-type verification to be done by specifying the "violation" keyword. Content-type verification will check the "magic number" in the body of the HTTP message against the mime-type's magic number to ensure that some other type is not being smuggled.

The following types are built-in. Many have magic numbers associated with them and can be verified. The **count**, **length**, and **regex** keywords operate the same as for the other fields as described above.

```
hostname(config-pmap)# match { request | response }  header content-type ?
```

Content type	Match on
application/msword	Match on 'application/msword
application/octet-stream	Match on 'application/octet-stream
application/pdf	Match on 'application/pdf'
application/postscript	Match on 'application/postscript'
application/vnd.ms-excel	Match on 'application/vnd.ms-excel
application/vnd.ms-powerpoint	Match on 'application/vnd.ms-powerpoint
application/x-gzip	Match on 'application/x-gzip
application/x-java-archive	Match on 'application/x-java-archive
application/x-java-vm	Match on 'application/x-java-vm'
application/x-msn-messenger	Match on 'application/x-msn-messenger'
application/zip	Match on 'application/zip
audio/basic	Match on 'audio/basic
audio/midi	Match on 'audio/midi'
audio/mpeg	Match on 'audio/mpeg
audio/x-adpcm	Match on 'audio/x-adpcm
audio/x-aiff	Match on 'audio/x-aiff'
audio/x-ogg	Match on 'audio/x-ogg
audio/x-wav	Match on 'audio/x-wav'
count	Specify that the match should count the number of instances of this header
image/gif	Match on 'image/gif'
image/jpeg	Match on 'image/jpeg
image/mpeg	Match on 'image/mpeg

Content type	Match on
image/tiff	Match on 'image/tiff
image/x-3ds	Match on 'image/x-3ds
image/x-bitmap	Match on 'image/x-bitmap
image/x-niff	Match on 'image/x-niff'
image/x-png	Match on 'image/x-png
image/x-portable-bitmap	Match on 'image/x-portable-bitmap
image/x-portable-graymap	Match on 'image/x-portable-graymap
image/x-xpm	Match on 'image/x-xpm
length	Specify that the match is a length check
regex	Specify a regex or regex class
text/css	Match on 'text/css
text/html	Match on 'text/html
text/plain	Match on 'text/plain
text/richtext	Match on 'text/richtext'
text/sgml	Match on 'text/sgml
text/xmcd	Match on 'text/xmcd'
text/xml	Match on 'text/xml
unknown	Specify that the mime-type must match a built-in 'known' mime-type
video/flc	Match on 'video/flc
video/mpeg	Match on 'video/mpeg
video/quicktime	Match on 'video/quicktime
video/sgi	Match on 'video/sgi
video/x-fli	Match on 'video/x-fli
violation	Specify that the 'magic number' in the body must correspond to the mime-type in the content-type header field

Transfer-Encoding Header Check

In addition to the length, count and regex checks described above, the user can perform various special checks on the transfer-encoding field:

- The user can match the transfer encoding in the header's value against a set of built-in keywords for the known transfer-encodings.
- The user can also specify that the transfer-encoding must be populated by using the "empty" keyword.
- The following types are built-in. Many of them have magic numbers associated with them and can be verified. The "count", "length" and "regex" options operate the same as for the other fields as described above.

```
hostname(config-pmap)# match { request | response } header transfer-encoding ?
```

See the following **mpf-class-map** mode commands and options:

Command	Match on
chunked	Match on 'chunked'
compress	Match on 'compress'
count	Specify that the match should count the number of instances of this header
deflate	Match on 'deflate'
empty	Match an empty transfer-encoding field
gzip	Match on 'gzip'
identity	Match on 'identity'
length	Specify that the match is a length check
regex	Specify a regex or regex class

Examples

The following example shows the use of the **match request, response** command to performs a regex scan of the entire header of the HTTP message:

```
hostname(config-pmap)# match request header regex class classmap1 regex1
```

Related Commands

Command	Description
policy map type inspect	When using the Modular Policy Framework, defines special actions for inspection application traffic.
inspect http	Inspects HTTP traffic.

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	Match OSPF external routes (type 1 or type 2).
internal	Match OSPF intra-area and interarea routes.
local	Match a locally generated route.
nssa-external	Match OSPF NSSA external route (type 1 or type 2).
type-1	(Optional) Match only type 1 routes.
type-2	(Optional) Match only type 2 routes.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set** configuration commands let you 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.

Examples

The following example shows how to redistribute internal routes:

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

Related Commands

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

match sender-address

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

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

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

Related Commands

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

match third-party-registration

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

match uri

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

max-failed-attempts

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

max-failed-attempts *number*

no max-failed-attempts

Syntax Description

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

Defaults

The default value of *number* is 3.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

max-forwards-validation

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

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

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

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

max-header-length

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

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

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

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

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

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

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-uri-length

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

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

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

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

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

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

Related Commands

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

mcc

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

member

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

member *class_name*

no member *class_name*

Syntax Description

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

Defaults

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

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Context configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, all security contexts have unlimited access to the resources of the FWSM, 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 FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

Examples

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

```
hostname(config)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0
```

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.

memory caller-address

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

memory caller-address *startPC endPC*

no memory caller-address

Syntax Description

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

Defaults

The actual caller PC is recorded for memory tracing.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

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

Related Commands

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

memory delayed-free-poisoner enable

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

memory delayed free poisoner enable

no memory delayed free poisoner enable

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Table 20-1 describes the significant portion of the output.

Table 20-1 Illegal Memory Usage Output Description

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

Table 20-1 Illegal Memory Usage Output Description

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

Related Commands

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

memory delayed-free-poisoner validate

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

memory delayed free poisoner enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

memory profile enable

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

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

Syntax Description

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

Defaults

Memory profiling is disabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

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

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

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

The following example enables memory profiling:

```
hostname# memory profile enable
```

Related Commands

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

memory profile text

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

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

Related Commands

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

message-length

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

mfib forwarding

To reenable MFIB forwarding on an interface, use the **mfib forwarding** command in interface configuration mode. To disable MFIB forwarding on an interface, use the **no** form of this command.

mfib forwarding

no mfib forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables MFIB forwarding on all interfaces by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable multicast routing, MFIB forwarding is enabled on all interfaces by default. Use the **no** form of the command to disable MFIB forwarding on a specific interface. Only the **no** form of the command appears in the running configuration.

When MFIB forwarding is disabled on an interface, the interface does not accept any multicast packets unless specifically configured through other methods. IGMP packets are also prevented when MFIB forwarding is disabled.

Examples

The following example disables MFIB forwarding on the specified interface:

```
hostname(config)# interface Vlan55
hostname(config-if)# no mfib forwarding
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing.
pim	Enables PIM on an interface.

mgcp-map

To identify a specific map for defining the parameters for MGCP inspection, use the **mgcp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

mgcp-map *map_name*

no mgcp-map *map_name*

Syntax Description

map_name	The name of the MGCP map. The maximum number of characters is 64.

Defaults

The default for the MGCP command queue is 200.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **mgcp-map** command to identify a specific map to use for defining the parameters for MGCP inspection. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. After defining the MGCP map, you use the **inspect mgcp** command to enable the map. You use Modular Policy Framework to apply the **inspect** command to a defined class of traffic and to apply the policy to a specific interface. The following are the commands available in MGCP map configuration mode.

- **call-agent**—Specifies a group of call agents.
- **command-queue**—Specifies the maximum number of MGCP commands that can be queued.
- **gateway**—Specifies the group of call agents that are managing a particular gateway.
- **no**—Negates a command or sets a parameter to its default value.

Examples

The following example shows how to use the **mgcp-map** command to identify a specific map (mgcp-policy) to use for defining the parameters for MGCP inspection.

```
hostname(config)# mgcp-map mgcp-policy
hostname(config-mgcp-policy)#
```

The following example shows how to identify MGCP traffic, define a MGCP map, define a policy, and apply the policy to the outside interface. You enable the MGCP inspection engine as shown in the following example, which creates a class map to match MGCP traffic on the default port (2427). The service policy is then applied to the outside interface.

```
hostname(config)# class-map mgcp-port
hostname(config-cmap)# match port tcp eq 2427
hostname(config-cmap)# exit
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config)# policy-map mgcp_policy
hostname(config-pmap)# class mgcp-port
hostname(config-pmap-c)# inspect mgcp mgcp_inbound
hostname(config-pmap-c)# exit
hostname(config)# service-policy mgcp_policy interface outside
```

This allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117. The maximum number of MGCP commands that can be queued is 150.

To enable MGCP inspection for all interfaces, use the **global** parameter in place of **interface outside**.

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
show mgcp	Displays MGCP configuration and session information.
timeout	Configures the idle timeouts related to MGCP.

mkdir

To create a new directory, use the **mkdir** command in privileged EXEC mode.

mkdir [**/noconfirm**] [**flash:**]*path*

Syntax Description

flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
noconfirm	(Optional) Suppresses the confirmation prompt.
path	The name and path of the directory to create.

Defaults

If you do not specify a path, the directory is created in the current working directory.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

If a directory with the same name already exists, then the new directory is not created.

Examples

This example shows how to make a new directory called “backup”:

```
hostname# mkdir backup
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
dir	Displays the directory contents.
rmdir	Removes the specified directory.
pwd	Display the current working directory.

mode

To set the security context mode to single or multiple, use the **mode** command in global configuration mode.

mode {**single** | **multiple**} [**noconfirm**]

Syntax Description

multiple	Sets multiple context mode.
noconfirm	(Optional) Sets the mode without prompting you for confirmation. This option is useful for automated scripts.
single	Sets the context mode to single.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

You can partition a single FWSM into multiple virtual devices, known as security contexts. Each context behaves like an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone appliances. In single mode, the FWSM has a single configuration and behaves as a single device. In multiple mode, you can create multiple contexts, each with its own configuration. The number of contexts allowed depends on your license.

In multiple context mode, the FWSM includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a stand-alone device (see the **config-url** command to identify the context configuration location). The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the FWSM. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

When you change the context mode using the **mode** command, you are prompted to reboot.

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the FWSM converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The FWSM automatically adds an entry for the admin context to the system configuration with the name "admin."

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the FWSM; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device.

Not all features are supported in multiple context mode. See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for more information.

Examples

The following example sets the mode to multiple:

```
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

The following example sets the mode to single:

```
hostname(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....

Booting system, please wait...
```

Related Commands

Command	Description
context	Configures a context in the system configuration and enters context configuration mode.
show mode	Shows the current context mode, either single or multiple.

monitor-interface

To enable health monitoring on a specific interface, use the **monitor-interface** command in global configuration mode. To disable interface monitoring, use the **no** form of this command.

monitor-interface *if_name*

no monitor-interface *if_name*

Syntax Description

if_name	Specifies the name of the interface being monitored.

Defaults

Monitoring of logical interfaces is disabled by default.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The number of interfaces that can be monitored for the FWSM is 250. Hello messages are exchanged during every interface poll frequency time period between the FWSM failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

In Active/Active failover, this command is only valid within a context.

If a VLAN interface is down or shut down (by whatever intentional means, for example, when the VLAN was removed from the configuration on the MSFC or shutdown on FWSM), then the **monitor-interface** command should be removed for that interface.

Examples

The following example enables monitoring on an interface named "inside":

```
hostname(config)# monitor-interface inside
hostname(config)#
```

Related Commands

Command	Description
clear configure monitor-interface	Removes the **monitor-interface** commands from the running configuration.
failover interface-policy	Specifies the number or percentage of monitored interface that must fail for failover to occur.
failover polltime	Specifies the interval between hello messages on an interface (Active/Standby failover).
polltime interface	Specifies the interval between hello messages on an interface (Active/Active failover).
show running-config monitor-interface	Displays the **monitor-interface** commands in the running configuration.

more

To display the contents of a file, use the **more** command in privileged EXEC mode.

more *{*/ascii | /binary| /ebcdic | flash: | ftp: | http: | https: | system: | tftp:*}filename*

Syntax Description

/ascii	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
/ebcdic	(Optional) Displays binary files in EBCDIC.
filename	Specifies the name of the file to display.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a website.
https:	(Optional) Displays a file on a secure website.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.

Defaults

ACSII mode.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

The **more filesystem:** command prompts you to enter the alias of the local directory or file systems.

Examples

The following example shows how to display the contents of a local file named “test.cfg”:

```
hostname# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005

XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
```

```
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

Command	Description
cd	Changes to the specified directory.
pwd	Displays the current working directory.

mroute

To configure a static multicast route, use the **mroute** command in global configuration mode. To remove a static multicast route, use the **no** form of this command.

mroute *src smask* {*in_if_name* | *rpf_neighbor*} [**dense** *output_if_name*] [*distance*]

no mroute *src smask* {*in_if_name* | *rpf_neighbor*} [**dense** *output_if_name*] [*distance*]

Syntax Description

dense *output_if_name*	(Optional) The interface name for dense mode output. The **dense** *output_if_name* keyword and argument pair is only supported for SMR stub multicast routing (igmp forwarding).
distance	(Optional) The administrative distance of the route. Routes with lower distances have preference. The default is 0.
in_if_name	Specifies the incoming interface name for the mroute.
rpf_neighbor	Specifies the RPF neighbor for the security appliance.
smask	Specifies the multicast source network address mask.
src	Specifies the IP address of the multicast source.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command lets you statically configure where multicast sources are located. The FWSM expects to receive multicast packets on the same interface as it would use to send unicast packets to a specific source. In some cases, such as bypassing a route that does not support multicast routing, multicast packets may take a different path than the unicast packets.

Static multicast routes are not advertised or redistributed.

Note You can specific the interface name or the RPF neighbor using this command, but not at the same time.

Use the **show mroute** command displays the contents of the multicast route table. Use the **show running-config mroute** command to display the mroute commands in the running configuration.

Examples

The following example shows how configure a static multicast route using the **mroute** command:

```
hostname(config)# mroute 172.16.0.0 255.255.0.0 inside
```

Related Commands

Command	Description
show running-config mroute	Displays the **mroute** commands in the configuration.

mtu

To specify the maximum transmission unit for an interface, use the **mtu** command in global configuration mode. To reset the MTU block size to 1500 for Ethernet interfaces, use the **no** form of this command. This command supports IPv4 and IPv6 traffic.

mtu *interface_name bytes*

no mtu *interface_name bytes*

Syntax Description

bytes	Number of bytes in the MTU; valid values are from 64 to 65,535 bytes.
interface_name	Internal or external network interface name.

Defaults

The default *bytes* is 1500 for Ethernet interfaces.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **mtu** command lets you to set the data size that is sent on a connection. Data that is larger than the MTU value is fragmented before being sent.

The FWSM supports IP path MTU discovery (as defined in RFC 1191), which allows a host to dynamically discover and cope with the differences in the maximum allowable MTU size of the various links along the path. Sometimes, the FWSM cannot forward a datagram because the packet is larger than the MTU that you set for the interface, but the “don’t fragment” (DF) bit is set. The network software sends a message to the sending host, alerting it to the problem. The host has to fragment packets for the destination so that they fit the smallest packet size of all the links along the path.

The default MTU is 1500 bytes in a block for Ethernet interfaces (which is also the maximum). This value is sufficient for most applications, but you can pick a lower number if network conditions require it.

When using the Layer 2 Tunneling Protocol (L2TP), we recommend that you set the MTU size to 1380 to account for the L2TP header and IPSec header length.

Examples

The followig example shows how to specify the MTU for an interface:

```
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
hostname(config)# mtu inside 8192
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

Related Commands

Command	Description
clear configure mtu	Clears the configured maximum transmission unit values on all interfaces.
show running-config mtu	Displays the current maximum transmission unit block size.

multicast-routing

To enable IP multicast routing on the FWSM, use the **multicast routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

multicast-routing

no multicast-routing

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM and IGMP on all interfaces by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **multicast-routing** command enables PIM and IGMP on all interfaces.

Note PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

If the security appliance is the PIM RP, use the untranslated outside address of the security appliance as the RP address.

The number of entries in the multicast routing tables are limited by the amount of RAM on the system. Table 20-2 lists the maximum number of entries for specific multicast tables based on the amount of RAM on the security appliance. Once these limits are reached, any new entries are discarded.

Table 20-2 Entry Limits for Multicast Tables

Table	16 MB	128 MB	128+ MB
MFIB	1000	3000	5000
IGMP Groups	1000	3000	5000
PIM Routes	3000	7000	12000

Examples

The following example enables IP multicast routing on the FWSM:

```
hostname(config)# multicast-routing
```

Related Commands

Command	Description
igmp	Enables IGMP on an interface.
pim	Enables PIM on an interface.