CHAPTER 20

mac address through multicast-routing Commands

mac address

To specify the virtual MAC addresses for the active and standby units, use the **mac address** command in failover group configuration mode. To restore the default virtual MAC addresses, use the **no** form of this command.

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

Syntax Description

phy_if	The physical name of the interface to set the MAC address.
active_mac	The virtual MAC address for the active unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
standby_mac	The virtual MAC address for the standby unit. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Defaults

The defaults are as follows:

- Active unit default MAC address: 00a0.c9*physical_port_number.failover_group_id*01.
- Standby unit default MAC address: 00a0.c9*physical_port_number.failover_group_id*02.

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
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

If the virtual MAC addresses are not defined for the failover group, the default values are used.

If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address.

Examples

The following partial example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
```

```
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover mac address	Specifies a virtual MAC address for a physical interface.

mac-address

To manually assign a private MAC address to an interface or subinterface, use the **mac-address** command in interface configuration mode. In multiple context mode, this command can assign a different MAC address to the interface in each context. To revert the MAC address to the default, use the **no** form of this command.

mac-address *mac_address* [**standby** *mac_address*]

no mac-address [*mac_address* [**standby** *mac_address*]]

Syntax Description

mac_address	Sets the MAC address for this interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE. If you use failover, this MAC address is the active MAC address. **Note** Because auto-generated addresses (the **mac-address auto** command) start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.
standby *mac_address*	(Optional) Sets the standby MAC address for failover. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Defaults

The default MAC address is the burned-in MAC address of the physical interface. Subinterfaces inherit the physical interface MAC address. Some commands set the physical interface MAC address (including this command in single mode), so the inherited address depends on that configuration.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(5)	The use of A2 to start the MAC address was restricted when also used with the **mac-address auto** command.

Usage Guidelines

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for more information.

You can assign each MAC address manually with this command, or you can automatically generate MAC addresses for shared interfaces in contexts using the **mac-address auto** command. If you automatically generate MAC addresses, you can use the **mac-address** command to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

You can also set the MAC address using other commands or methods. The MAC address methods have the following priority:

1. **mac-address** command in interface configuration mode.

   This command works for physical interfaces and subinterfaces. In multiple context mode, you set the MAC address within each context. This feature lets you set a different MAC address for the same interface in multiple contexts.

2. **failover mac address** command for Active/Standby failover in global configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

3. **mac address** command for Active/Active failover in failover group configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

4. **mac-address auto** command in global configuration mode (multiple context mode only).

   This command applies to shared interfaces in contexts.

5. For Active/Active failover, auto-generation of active and standby MAC addresses for physical interfaces.

   This method applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

6. Burned-in MAC address. This method applies to physical interfaces.

   Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

Examples

The following example configures the MAC address for GigabitEthernet 0/1.1:

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address auto	Auto-generates MAC addresses (active and standby) for shared interfaces in multiple context mode.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

mac-address auto

To automatically assign private MAC addresses to each context interface, use the **mac-address auto** command in global configuration mode. To disable automatic MAC addresses, use the **no** form of this command.

mac-address auto prefix *prefix*

no mac-address auto

Syntax Description

prefix *prefix*	Sets the prefix used as part of the MAC address. The *prefix* is a decimal value between 0 and 65535. This prefix is converted to a 4-digit hexadecimal number. The prefix ensures that each security appliance uses unique MAC addresses, so you can have multiple security appliances on a network segment, for example. See the "MAC Address Format" section for more information about how the prefix is used.

Defaults

Auto-generation 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
7.2(1)	This command was introduced.
8.0(5)	The **prefix** keyword was added. The MAC address format was changed to use the prefix, to use a fixed starting value (A2), and to use a different scheme for the primary and secondary unit MAC addresses in a failover pair. The MAC addresess are also now persistent accross reloads. The command parser now checks if auto-generation is enabled; if you want to also manually assign a MAC address, you cannot start the manual MAC address with A2.

Usage Guidelines

To allow contexts to share interfaces, we suggest that you assign unique MAC addresses to each shared context interface. The MAC address is used to classify packets within a context. If you share an interface, but do not have unique MAC addresses for the interface in each context, then the destination IP address is used to classify packets. The destination address is matched with the context NAT configuration, and this method has some limitations compared to the MAC address method. See the *Cisco ASA 5500 Series Configuration Guide using the CLI* for information about classifying packets.

In the rare circumstance that the generated MAC address conflicts with another private MAC address in your network, you can manually set the MAC address for the interface within the context. See the **mac-address** command to manually set the MAC address.

Default MAC Address

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

All auto-generated MAC addresses start with A2. The auto-generated MAC addresses are persistent across reloads.

Interaction with Manual MAC Addresses

If you manually assign a MAC address and also enable auto-generation, then the manually assigned MAC address is used. If you later remove the manual MAC address, the auto-generated address is used.

Because auto-generated addresses start with A2, you cannot start manual MAC addresses with A2 if you also want to use auto-generation.

Failover MAC Addresses

For use with failover, the security appliance generates both an active and standby MAC address for each interface. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption. See the "MAC Address Format" section for more information.

For upgrading failover units with the legacy version of the **mac-address auto** command before the **prefix** keyword was introduced, see the "Legacy MAC Address Format When Not Using the prefix Keyword" section.

MAC Address Format

The security appliance generates the MAC address using the following format:

A2xx.yyzz.zzzz

Where xx.yy is a user-defined prefix, and zz.zzzz is an internal counter generated by the security appliance. For the standby MAC address, the address is identical except that the internal counter is increased by 1.

For an example of how the prefix is used, if you set a prefix of 77, then the security appliance converts 77 into the hexadecimal value 004D (yyxx). When used in the MAC address, the prefix is reversed (xxyy) to match the security appliance native form:

A2**4D.00**zz.zzzz

For a prefix of 1009 (03F1), the MAC address is:

A2**F1.03**zz.zzzz

When the MAC Address is Generated

When you configure a **nameif** command for the interface in a context, the new MAC address is generated immediately. If you enable this command after you configure context interfaces, then MAC addresses are generated for all interfaces immediately after you enter the command. If you use the **no mac-address auto** command, the MAC address for each interface reverts to the default MAC address. For example, subinterfaces of GigabitEthernet 0/1 revert to using the MAC address of GigabitEthernet 0/1.

Setting the MAC Address Uisng Other Methods

You can also set the MAC address using other commands or methods. The MAC address methods have the following priority:

1. **mac-address** command in interface configuration mode.

   This command works for physical interfaces and subinterfaces. In multiple context mode, you set the MAC address within each context. This feature lets you set a different MAC address for the same interface in multiple contexts.

2. **failover mac address** command for Active/Standby failover in global configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

3. **mac address** command for Active/Active failover in failover group configuration mode.

   This command applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

4. **mac-address auto** command in global configuration mode (multiple context mode only).

   This command applies to shared interfaces in contexts.

5. For Active/Active failover, auto-generation of active and standby MAC addresses for physical interfaces.

   This method applies to physical interfaces. Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

6. Burned-in MAC address. This method applies to physical interfaces.

   Subinterfaces inherit the MAC address of the physical interface unless set separately by the **mac-address** or **mac-address auto** command.

Viewing MAC Addresses in the System Configuration

To view the assigned MAC addresses from the system execution space, enter the **show running-config all context** command.

The **all** option is required to view the assigned MAC addresses. Although this command is user-configurable in global configuration mode only, the **mac-address auto** command appears as a read-only entry in the configuration for each context along with the assigned MAC address. Only allocated interfaces that are configured with a **nameif** command within the context have a MAC address assigned.

Note If you manually assign a MAC address to an interface, but also have auto-generation enabled, the auto-generated address continues to show in the configuration even though the manual MAC address is the one that is in use. If you later remove the manual MAC address, the auto-generated one shown will be used.

Viewing MAC Addresses Within a Context

To view the MAC address in use by each interface within the context, enter the **show interface | include (Interface)|(MAC)** command.

Note The **show interface** command shows the MAC address in use; if you manually assign a MAC address and also have auto-generation enabled, then you can only view the unused auto-generated address from within the system configuration.

Legacy MAC Address Format When Not Using the prefix Keyword

Prior to Version 8.0(5), the **mac-address auto** command did not include the **prefix** keyword. This old version of the command is still accepted so you can perform upgrades between failover pairs; the command is not automatically converted when you upgrade so the commands continue to match between the upgraded and non-upgraded failover units. After you upgrade both units to the new software version, you should change this command to use the **prefix** keyword.

Without the **prefix** keyword, the MAC address is generated using the following format:

- Active unit MAC address: 12_*slot.port_subid.contextid*.
- Standby unit MAC address: 02_*slot.port_subid.contextid*.

For platforms with no interface slots, the slot is always 0. The *port* is the interface port. The *subid* is an internal ID for the subinterface, which is not viewable. The *contextid* is an internal ID for the context, viewable with the **show context detail** command. For example, the interface GigabitEthernet 0/1.200 in the context with the ID 1 has the following generated MAC addresses, where the internal ID for subinterface 200 is 31:

- Active: 1200.0131.0001
- Standby: 0200.0131.0001

This legacy MAC address generation method does not allow for persistent MAC addresses across reloads, does not allow for multiple security appliances on the same network segment (because unique MAC addresses are not guaranteed), and does not prevent overlapping MAC addresses with manually assigned MAC addresses.

Examples

The following example enables automatic MAC address generation with a prefix of 78:

```
hostname(config)# mac-address auto prefix 78
```

The following output from the **show running-config all context admin** command shows the primary and standby MAC address assigned to the Management0/0 interface:

```
hostname# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

The following output from the **show running-config all context** command shows all the MAC addresses (primary and standby) for all context interfaces. Note that because the GigabitEthernet0/0 and GigabitEthernet0/1 main interfaces are not configured with a **nameif** command inside the contexts, no MAC addresses have been generated for them.

```
hostname# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
```

```
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

Related Commands

Command	Description
failover mac address	Sets the active and standby MAC address of a physical interface for Active/Standby failover.
mac address	Sets the active and standby MAC address of a physical interface for Active/Active failover.
mac-address	Manually sets the MAC address (active and standby) for a physical interface or subinterface. In multiple context mode, you can set different MAC addresses in each context for the same interface.
mode	Sets the security context mode to multiple or single.
show interface	Shows the interface characteristics, including the MAC address.

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
7.0(1)	This command was introduced.

Usage Guidelines

No usage guidelines.

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. 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 security appliance drops the traffic and generates a system message.

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

Syntax Description

interface_name	The source interface.
mac_address	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
7.0(1)	This command was introduced.

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

mac-learn *interface_name* **disable**

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

Syntax Description

interface_name	The interface on which you want to disable MAC learning.
disable	Disables 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
7.0(1)	This command was introduced.

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.
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
Preexisting	This command was preexisting.

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.

mail-relay

To configure a local domain name, use the **mail-relay** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

Syntax Description

domain_name	Specifies the domain name.
drop-connection	Closes the connection.
log	Generates a system log message.

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**
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a mail relay for a specific domain:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mail-relay mail action drop-connection
```

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.

management-access

To allow management access to an interface other than the one from which you entered the security appliance when using VPN, use the **management-access** command in global configuration mode. To disable management 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 security appliance 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
Preexisting	This command was preexisting.

Usage Guidelines

This command allows you to connect to an interface other than the one you entered the security appliance from when using a full tunnel IPSec VPN or SSL VPN client (AnyConnect 2.x client, SVC 1.x) or across a site-to-site IPSec tunnel. For example, if you enter the security appliance 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 use the following applications:

- SNMP polls
- HTTPS requests
- ASDM access
- Telnet access
- SSH access
- PING
- Syslog polls
- NTP requests

You can define only one management-access interface.

Note Do not apply a static NAT statement to the management access interface; if you do so, then remote VPN users will not be able to access 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 internal interface for management access of the security appliance.
show management-access	Displays the name of the internal interface configured for management access.

Usage Guidelines

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.

Defaults

The Management 0/0 interface on the ASA 5510 and higher adaptive security appliance is set to management-only mode 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
7.0(1)	This command was introduced.

Usage Guidelines

The ASA 5510 and higher adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA 5510 and higher adaptive security appliance, you can use the Management 0/0 interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only. You can also set the IP address of this interface in transparent mode if you want this interface to be on a different subnet from the management IP address, which is assigned to the security appliance or context, and not to individual interfaces.

Examples

The following example disables management-only mode on the management interface:

```
hostname(config)# interface management0/0
hostname(config-if)# no management-only
```

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

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# management-only
```

Related Commands

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

map-name

To map a user-defined attribute name to a Cisco attribute name, use the **map-name** command in ldap-attribute-map configuration mode.

To remove this mapping, use the **no** form of this command.

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

Syntax Description

user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute.
Cisco-attribute-name	Specifies the Cisco attribute name that you are mapping to the user-defined name.

Defaults

By default, no name mappings exist.

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
ldap-attribute-map configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **map-name** command, you can create map yourown attribute names to Cisco attribute names. You can then bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example commands map a user-defined attribute name Hours to the Cisco attribute name cVPN3000-Access-Hours in the LDAP attribute map myldapmap:

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
hostname(config-ldap-attribute-map)#
```

Within ldap-attribute-map mode, you can enter "?" to display the complete list of Cisco LDAP attribute names, as shown in the following example:

```
hostname(config-ldap-attribute-map)# map-name ?
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-value	Maps a user-defined attribute value to a Cisco attribute.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP attribute maps.

map-value

To map a user-defined value to a Cisco LDAP attribute, use the **map-value** command in ldap-attribute-map configuration mode. To delete an entry within a map, use the **no** form of this command.

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

Syntax Description

cisco-value-string	Specifies the Cisco value string for the Cisco attribute.
user-attribute-name	Specifies the user-defined attribute name that you are mapping to the Cisco attribute name.
user-value-string	Specifies the user-defined value string that you are mapping to the Cisco attribute value.

Defaults

By default, there are no user-defined values mapped to Cisco attributes.

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
ldap-attribute-map configuration	•	•	•	•	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

With the **map-value** command, you can map your own attribute values to Cisco attribute names and values. You can tthen bind the resulting attribute map to an LDAP server. Your typical steps would include:

1. Use the **ldap attribute-map** command in global configuration mode to create an unpopulated attribute map. This commands enters ldap-attribute-map mode.
2. Use the **map-name** and **map-value** commands in ldap-attribute-map mode to populate the attribute map.
3. Use the **ldap-attribute-map** command in aaa-server host mode to bind the attribute map to an LDAP server. Note the hyphen after “ldap” in this command.

Note To use the attribute mapping features correctly, you need to understand both the Cisco LDAP attribute names and values as well as the user-defined attribute names and values.

Examples

The following example, entered in ldap-attribute-map mode, sets the user-defined value of the user attribute Hours to a user-defined time policy named workDay and a Cisco-defined time policy named Daytime:

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-value Hours workDay Daytime
hostname(config-ldap-attribute-map)#
```

Related Commands

Command	Description
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.
ldap-attribute-map (aaa-server host mode)	Binds an LDAP attribute map to an LDAP server.
map-name	Maps a user-defined LDAP attribute name with a Cisco LDAP attribute name.
show running-config ldap attribute-map	Displays a specific running LDAP attribute map or all running attribute maps.
clear configure ldap attribute-map	Removes all LDAP maps.

mask

When using the Modular Policy Framework, mask out part of the packet that matches a **match** command or class map by using the **mask** command in match or class configuration mode. This mask action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. For example, you can you use **mask** command for the DNS application inspection to mask a header flag before allowing the traffic through the security appliance. To disable this action, use the **no** form of this command.

mask [**log**]

no mask [**log**]

Syntax Description

log	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
7.2(1)	This command was introduced.

Usage Guidelines

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 dns dns_policy_map** command where dns_policy_map is the name of the inspection policy map.

Examples

The following example masks the RD and RA flags in the DNS header before allowing the traffic through the security appliance:

```
hostname(config-cmap)# policy-map type inspect dns dns-map1
```

```
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log
hostname(config-pmap-c)# match header-flag RA
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-banner

To obfuscate the server banner, use the **mask-banner** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

mask-banner

no mask-banner

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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to mask the server banner:

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

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.

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
7.0(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 security appliance 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)#
```

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.

Commands	Description
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
7.0(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 security appliance 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 to match, any ports 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
7.0(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

This 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 apn

To configure a match condition for an access point name in GTP messages, use the **match apn** command in class-map or policy-map configuration mode. To remove the match condition, use the **no** form of this command.

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for an access point name in an GTP inspection class map:

```
hostname(config-cmap)# match apn class gtp_regex_apn
```

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 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
7.2(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
7.2(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
7.2(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 certificate

During the PKI certificate validation process, the security appliance checks certificate revocation status to maintain security. It can use either CRL checking or Online Certificate Status Protocol (OCSP) to accomplish this task. With CRL checking, the security appliance retrieves, parses, and caches Certificate Revocation Lists, which provide a complete list of revoked certificates. OCSP offers a more scalable method of checking revocation status in that it localizes certificate status on a Validation Authority, which it queries for the status of a specific certificate.

Certificate match rules let you configure OCSP URL overrides, which specify a URL to check for revocation status, rather than the URL in the AIA field of the remote user certificate. Match rules also let you configure trustpoints to use to validate OCSP responder certificates, which lets the security appliance validate responder certificates from any CA, including self-signed certificates and certificates external to the validation path of the client certificate.

To configure a certificate match rule, use the **match certificate** command in crypto ca trustpoint mode. To remove the rule from the configuration, use the **no** form of this command.

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

Syntax Description

map-name	Specifies the name of the certificate map to match to this rule. You must configure the certificate map prior to configuring a match rule. Maximum 65 characters.
match certificate	Specifies the certificate map for this match rule.
override ocsp	Specifies that the purpose of the rule is to override an OCSP URL in a certificate.
seq-num	Sets the priority for this match rule. Range is 1 to 10000. The security appliance evaluates the match rule with the lowest sequence number first, followed by higher numbers until it finds a match.
trustpoint	(Optional) Specifies using a trustpoint for verifying the OCSP responder certificate.
trustpoint-name	(Optional) Identifies the trustpoint. to use with the override to validate responder certificates.
url	Specifies accessing a URL for OCSP revocation status.
URL	Identifies the URL to access for OCSP revocation status.

Defaults

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
crypto ca trustpoint mode	•	•	•	•	•

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Be aware of the following tips when configuring OCSP:

- You can configure multiple match rules within a trustpoint configuration, but you can have only one match rule for each crypto ca certificate map. You can, however, configure multiple crypto ca certificate maps and associate them with the same trustpoint.
- You must configure the certificate map before configuring a match rule.
- To configure a trustpoint to validate a self-signed OCSP responder certificates, you import the self-signed responder certificate into its own trustpoint as a trusted CA certificate. Then you configure the **match certificate** command in the client certificate validating trustpoint to use the trustpoint that contains the self-signed OCSP responder certificate to validate the responder certificate. The same applies for validating responder certificates external to the validation path of the client certificate.
- A trustpoint can validate both the client certificate and the responder certificate if the same CA issues both of them. But if different CAs issue the client and responder certificates, you need to configure two trustpoints, one trustpoint for each certificate.
- The OCSP server (responder) certificate typically signs the OCSP response. After receiving the response, the security appliance tries to verify the responder certificate. The CA normally sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of it being compromised.The CA typically also includes an ocsp-no-check extension in the responder certificate indicating that this certificate does not need revocation status checking. But if this extension is not present, the security appliance tries to check its revocation status using the same method specified in the trustpoint. If the responder certificate is not verifiable, revocation checks fails. To avoid this possibility, configure **revocation-check none** in the responder certificate validating trustpoint, while configuring **revocation-check ocsp** for the client certificate.
- If the security appliance does not find a match, it uses the URL in the **ocsp url** command. If you have not configured the **ocsp url** command, it uses the AIA field of the remote user certificate. If the certificate does not have an AIA extension, revocation status checking fails.

Examples

The following example shows how to create a certificate match rule for a trustpoint called newtrust. The rule has a map name called mymap, sequence number of 4, a trustpoint called mytrust, and specifies a URL of 10.22.184.22.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
hostname(config-ca-trustpoint)#
```

The next example shows step-by-step how to configure a crypto ca certificate map, and then a match certificate rule to identify a trustpoint that contains a CA certificate to validate the responder certificate. This is necessary if the CA identified in the newtrust trustpoint does not issue an OCSP responder certificate.

Step 1 Configure the certificate map that identifies the client certificates to which the map rule applies. In this example the name of the certificate map is mymap and the sequence number is 1. Any client certificate with a subject-name that contains a CN attribute equal to mycert matches the mymap entry.

```
hostname(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
hostname(config-ca-cert-map)#
```

Step 2 Configure a trustpoint that contains the CA certificate to use to validate the OCSP responder certificate. In the case of self-signed certificates, this is the self-signed certificate itself, which is imported and locally trusted. You can also obtain a certificate for this purpose through external CA enrollment. When prompted to do so, paste in the CA certificate.

```
hostname(config-ca-cert-map)# exit
hostname(config)# crypto ca trustpoint mytrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

Step 3 Configure the original trustpoint, newtrust, with OCSP as the revocation checking method. Then set a match rule that includes the certificate map, mymap, and the self-signed trustpoint, mytrust, configured in Step 2.

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud113D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
```

```
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust 4
url 10.22.184.22
```

Any connection that uses the newtrust trustpoint for client certificate authentication checks to see if the client certificate matches the attribute rules specified in the mymap certificate map. If so, the security appliance accesses the OCSP responder at 10.22.184.22 for certificate revocation status. It then uses the mytrust trustpoint to validate the responder certificate.

Note The newtrust trustpoint is configured to perform revocation checking via OCSP for the client certificates. However, the mytrust trustpoint is configured for the default revocation-check method which is none, so no revocation checking is performed on the OCSP responder certificate.

Related Commands

Command	Description
crypto ca certificate map	Creates crypto ca certificate maps. Use this command in global configuration mode.
crypto ca trustpoint	Enters crypto ca trustpoint mode. Use this command in global configuration mode.
ocsp disable-nonce	Disables the nonce extension of the OCSP request.
ocsp url	Specifies the OCSP server to use to check all certificates associated with a trustpoint.
revocation-check	Specifies the method(s) to use for revocation checking, and the order in which to try them.

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
7.2(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 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
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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
dcerpc	tcp	N/A	135
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
im	tcp	N/A	1-65539
ipsec-pass-thru	udp	N/A	500
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
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.

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

match dns-class

To configure a match condition for the Domain System Class in a DNS Resource Record or Question section, use the **match dns-class** command in class-map or policy-map configuration mode. To remove a configured class, use the **no** form of this command.

match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

Syntax Description

eq	Specifies an exact match.
c_well_known	Specifies DNS class by well-known name, IN.
c_val	Specifies an arbitrary value in the DNS class field (0-65535).
range	Specifies a range.
c_val1 c_val2	Specifies values in a range match. Each value between 0 and 65535.

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**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects all fields (questions and RRs) of a DNS message and matches the specified class. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: **match not header-flag QR** and **match question**.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS class in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-class eq IN
```

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 dns-type

To configure a match condition for a DNS type, including Query type and RR type, use the **match dns-type** command in class-map or policy-map configuration mode. To remove a configured dns type, use the **no** form of this command.

match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

Syntax Description

eq	Specifies an exact match.
t_well_known	Specifies DNS type by well-known name: A, NS, CNAME, SOA, TSIG, IXFR, or AXFR.
t_val	Specifies an arbitrary value in the DNS type field (0-65535).
range	Specifies a range.
t_val1 t_val2	Specifies values in a range match. Each value between 0 and 65535.

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**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects all sections of a DNS message (questions and RRs) and matches the specified type. Both DNS query and response are examined.

The match can be narrowed down to the question portion of a DNS query by the following two commands: **match not header-flag QR** and **match question**.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS type in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
```

```
hostname(config-pmap)# match dns-type eq a
```

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 domain-name

To configure a match condition for a DNS message domain name list, use the **match domain-name** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match [**not**] **domain-name regex** *regex_id*

match [**not**] **domain-name regex class** *class_id*

no match [**not**] **domain-name regex** *regex_id*

no match [**not**] **domain-name regex class** *class_id*

Syntax Description

regex	Specifies a regular expression.
regex_id	Specifies the regular expression ID.
class	Specifies the class map that contains multiple regular expression entries.
class_id	Specifies the regular expression class map ID.

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**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command matches domain names in the DNS message against predefined list. Compressed domain names will be expanded before matching. The match condition can be narrowed down to a particular field in conjunction with other DNS **match** commands.

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to match the DNS domain name in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match domain-name regex
```

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 dscp

To identify the IETF-defined DSCP value (in an IP header) in a class map, use the **match dscp** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match dscp {*values*}

no match dscp {*values*}

Syntax Description

values	Specifies up to eight different the IETF-defined DSCP values in the IP header. Range is 0 to 63.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Using the **match dscp** command, you can match the IETF-defined DSCP values in the IP header.

Examples

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match dscp af43 cs1 ef
hostname(config-cmap)#
```

Related Commands

Command	Description
class-map	Applies a traffic class to an interface.
clear configure class-map	Removes all of the traffic map definitions.
match access-list	Identifies access list traffic within a class map.
match port	Specifies the TCP/UDP ports as the comparison criteria for packets received on that interface.
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
7.2(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 filename

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
/root
hostname(config-cmap)# match username regex class ftp_regex_user
hostname(config-cmap)# match filename regex ftp-file
```

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 filetype

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

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 flow ip destination-address

To specify the flow IP destination address in a class map, use the **match flow ip destination-address** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match flow ip destination-address

no match flow ip destination-address

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
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

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
7.2(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 header-flag

To configure a match condition for a DNS header flag, use the **match header-flag** command in class-map or policy-map configuration mode. To remove a configured header flag, use the **no** form of this command.

match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

no match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

Syntax Description

eq	Specifies an exact match. If not configured, specifies a **match-all** bit mask match.
f_well_known	Specifies DNS header flag bits by well-known name. Multiple flag bits may be entered and logically OR'd. QR (Query, note: QR=1, indicating a DNS response) AA (Authoritative Answer) TC (TrunCation) RD (Recursion Desired) RA (Recursion Available)
f_value	Specifies an arbitrary 16-bit value in hexidecimal form.

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**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match header-flag AA
```

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 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
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for 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 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
7.2(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	Name an access list. Multiple access lists can be specified.

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
Preexisting	This command was preexisting.

Usage Guidelines

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

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. Multiple ACLs can be specified.
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
Preexisting	This command was preexisting.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *acl* argument.

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

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

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(config)# 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 ACLs, 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...*}

Syntax Description

acl	Name of an ACL. Multiple ACLs can be specified.
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
Preexisting	This command was preexisting.

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

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

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

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

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for a client login name in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match login-name regex login
```

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.
show running-config class-map	Displays the information about the class map configuration.

match media-type

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

match [**not**] **media-type [audio | data | video]**

no match [**not**] **media-type [audio | data | video]**

Syntax Description

audio	Specifies to match audio media type.
data	Specifies to match data media type.
video	Specifies to match video media 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
7.2(1)	This command was introduced.

Examples

The following example shows how to configure a match condition for audio media type in an H.323 inspection class map:

```
hostname(config-cmap)# match media-type audio
```

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 message id

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

match [**not**] **message id** [*message_id* | **range** *lower_range upper_range*]

no match [**not**] **message id** [*message_id* | **range** *lower_range upper_range*]

Syntax Description

message_id	Specifies an alphanumeric identifier between 1 and 255.
range *lower_range upper_range*	Specifies a lower and upper range of IDs.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config-cmap)# match message id 33
```

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 message length

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

match [**not**] **message length min** *min_length* **max** *max_length*

no match [**not**] **message length min** *min_length* **max** *max_length*

Syntax Description

min *min_length*	Specifies a minimum message ID length. Value is between 1 and 65536.
max *max_length*	Specifies a maximum message ID length. Value is between 1 and 65536.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config-cmap)# match message length min 8 max 200
```

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 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
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config-cmap)# match 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 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
7.2(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 peer-ip-address

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

match [**not**] **peer-ip-address** *ip_address ip_address_mask*

no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

Syntax Description

ip_address	Specifies a hostname or IP address of the client or server.
ip_address_mask	Specifies the netmask for the client or server IP address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for the peer IP address in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

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.
show running-config class-map	Displays the information about the class map configuration.

match peer-login-name

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

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure a match condition for the peer login name in an instant messaging class map:

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match peer-login-name regex peerlogin
```

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.
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
7.0(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** or **class-map type management** command.

   After you enter the **class-map** command, you can enter the **matchport** command to identify the traffic. Alternatively, you can enter a different type of **match** command, such as the **match access-list** command (the **class-map type management** command only allows the match port 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 precedence

To specify a precedence value in a class map, use the **match precedence** command in class-map configuration mode. To remove this specification, use the **no** form of this command.

match precedence *value*

no match precedence *value*

Syntax Description

value	Specifies up to four precedence values separated by a space. Range is 0 to 7.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Use the **match precedence** command to specify the value represented by the TOS byte in the IP header.

Examples

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

```
hostname(config)# class-map cmap
hostname(config-cmap)# match precedence 1
hostname(config-cmap)#
```

Related Commands

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

match protocol

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

match [**not**] **protocol** {**msn-im** | **yahoo-im**}

no match [**not**] **protocol** {**msn-im** | **yahoo-im**}

Syntax Description

msn-im	Specifies to match the MSN instant messaging protocol.
yahoo-im	Specifies to match the Yahoo instant messaging protocol.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# class-map type inspect im im_class
hostname(config-cmap)# match protocol yahoo-im
```

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.
show running-config class-map	Displays the information about the class map configuration.

match question

To configure a match condition for a DNS question or resource record, use the **match question** command in class-map or policy-map configuration mode. To remove a configured section, use the **no** form of this command.

match {**question** | {**resource-record answer** | **authority** | **additional**}}

no match {**question** | {**resource-record answer** | **authority** | **additional**}}

Syntax Description

question	Specifies the question portion of a DNS message.
resource-record	Specifies the resource record portion of a DNS message.
answer	Specifies the Answer RR section.
authority	Specifies the Authority RR section.
additional	Specifies the Additional RR section.

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**
Class-map or policy map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

By default, this command inspects the DNS header and matches the specified field. It can be used in conjunction with other DNS **match** commands to define inspection of a particular question or RR type..

This command can be configured within a DNS class map or policy map. Only one entry can be entered within a DNS class-map.

Examples

The following example shows how to configure a match condition for a DNS question in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match question
```

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 req-resp

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command enables the following checks:

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

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

The following is the list of supported content types.

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

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

Examples

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

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

Related Commands

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

match request-command

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

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

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

Syntax Description

ftp_command	Specifies one or more FTP commands to restrict.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

match request-method

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

match request method

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Table 20-1 Built-in Regex Values

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

Examples

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

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

Related Commands

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

match route-type

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

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

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

Syntax Description

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

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
Preexisting	This command was preexisting.

Usage Guidelines

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

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

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

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

Examples

The following example shows how to redistribute internal routes:

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

Related Commands

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

match rtp

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

match rtp *starting_port range*

no match rtp *starting_port range*

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

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

Related Commands

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

match sender-address

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

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

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

Related Commands

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

match server

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

match service

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

match third-party-registration

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

match tunnel-group

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

match tunnel-group *name*

no match tunnel-group *name*

Syntax Description

name	Text for the tunnel group name.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

match uri

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

match url-filter

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# regex badurl www.url1.com/rtsp.avi
hostname(config)# policy-map type inspect rtsp rtsp-map
hostname(config-pmap)# match url-filter regex badurl
hostname(config-pmap-p)# drop-connection
```

Related Commands

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

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

match username

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

match version

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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

max-failed-attempts

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

max-failed-attempts *number*

no max-failed-attempts

Syntax Description

number	An integer in the range 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
7.0(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
hostname(config-aaa-server-group)#
```

Related Commands

Command	Description
aaa-server *server-tag* **protocol** *protocol*	Enters AAA server group configuration mode so 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
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

max-header-length

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

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

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

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Related Commands

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

max-object-size

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

max-object-size *integer range*

Syntax Description

integer range	0 - 10000 KB

Defaults

1000 KB

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

max-retry-attempts

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

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

max-retry-attempts *retries*

no max-retry-attempts

Syntax Description

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

Defaults

The default value for this command is 3.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

This command applies to both types of SSO Servers.

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

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

Examples

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

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

Related Commands

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

max-uri-length

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

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

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

Syntax Description

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Related Commands

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

mcc

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

media-termination address

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

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

media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

no media-termination address *ip_address* [**rtp-min-port** *port1* **rtp-maxport** *port2*]

Syntax Description

ip_address	Specifies the virtual IP address that will be created for the phone proxy to use during media termination. Only one virtual interface can be configured per phone-proxy instance. The ASA phone proxy inserts the media termination IP address into the media address portion of the signaling messages.
rtp-max-port *port2*	Specifies the maximum value for the RTP port range for the media termination point, where *port2* can be a value from 32767 to 65535.
rtp-min-port *port1*	Specifies the minimum value for the RTP port range for the media termination point, where *port1* can be a value from 1024 to 16384.

Defaults

By default, the *port1* value for the **rtp-min-port** keyword is 16384 and the *port2* value for the **rtp-max-port** keyword is 32767.

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
phone-proxy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The security appliance must have an IP address for media termination that meets the following criteria:

- The IP address is a publicly routable address that is an unused IP address on an attached network to the security appliance interface that will never be used by another device in your network.
- The IP address cannot be the same as the security appliance interface IP address. Specifically, it cannot be the same as the least secure interface on the security appliance.
- The IP address cannot overlap with existing static NAT rules.
- The IP address cannot be the same as the CUCM or TFTP server IP address.

- Add routes to the other interfaces so that IP phones on other interfaces can reach the media termination address.

Configure the RTP port range for the media termination point when you need to scale the number of calls that the Phone Proxy supports.

Examples

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

```
hostname(config-phone-proxy)# media-termination address 192.168.1.4
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

media-type

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

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

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

Syntax Description

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

Defaults

The default is **rj45**.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.

Usage Guidelines

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

Examples

The following example sets the media type to SFP:

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

Related Commands

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

member

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

member *class_name*

no member *class_name*

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

member-interface

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

member-interface *physical_interface*

no member-interface *physical_interface*

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

Examples

The following example creates two redundant interfaces:

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

Related Commands

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

memberof

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

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

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

Syntax Description

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

Defaults

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

memory delayed-free-poisoner enable

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

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

Examples

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

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

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

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

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

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

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

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

Table 20-2 describes the significant portion of the output.

Table 20-2 Illegal Memory Usage Output Description

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

Table 20-2 Illegal Memory Usage Output Description

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

Related Commands

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

memory delayed-free-poisoner validate

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

memory delayed-free-poisoner validate

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

memory caller-address

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

memory caller-address *startPC endPC*

no memory caller-address

Syntax Description

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

Defaults

The actual caller PC is recorded for memory tracing.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

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

Note The security appliance 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 security appliance.
show memory-caller address	Displays the address ranges configured on the security appliance.

memory profile enable

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

memory profile enable peak *peak_value*

no memory profile enable peak *peak_value*

Syntax Description

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

Defaults

Memory profiling is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

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

Note The security appliance 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 security appliance.

memory profile text

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

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

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

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

Note The security appliance 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 security appliance.
show memory-caller address	Displays the address ranges configured on the security appliance.

memory-size

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

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

memory-size {percent | kb} *size*

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

Syntax Description

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

Defaults

No default behavior or value.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

```
hostname(config-webvpn)#
```
hostname(config-webvpn)# **reload**

Command	Description
show memory webvpn	Displays WebVPN memory usage statistics.

memory tracking enable

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

memory tracking enable

no memory tracking enable

Syntax Description

This command has no arguments or keywords.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(8)	This command was introduced.

Usage Guidelines

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

Examples

The following example enables tracking heap memory requests:

```
hostname# memory tracking enable
```

Related Commands

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

merge-dacl

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

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

no merge dacl

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

message-length

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

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
GTP map configuration	•	•	•	•	No

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

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
7.1(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 GigabitEthernet 0/0
hostname(config-if)# no mfib forwarding
```

Related Commands

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

min-object-size

To set a minimum size for objects that the security appliance can cache for WebVPN sessions, use the min-object-size command in cache mode. To change the size, use the command again. To set no minimum object size, enter a value of zero (0).

min-object-size *integer range*

Syntax Description

integer range	0 - 10000 KB.

Defaults

The default size is 0 KB.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The minimum object size must be smaller than the maximum object size. The security appliance calculates the size after compressing the object, if cache compression is enabled.

Examples

The following example shows how to set a maximum object size of 40 KB:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# min-object-size 40
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.
expiry-time	Configures the expiration time for caching objects without revalidating them.

Command	Description
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.

mkdir

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

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

Syntax Description

noconfirm	(Optional) Suppresses the confirmation prompt.
disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
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
7.0	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. You can partition a single security appliance 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 security appliance 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.

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
7.0(1)	This command was introduced.

Usage Guidelines

In multiple context mode, the security appliance 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 security appliance. 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 security appliance 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 security appliance 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 security appliance; 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 *Cisco ASA 5500 Series Configuration Guide using the CLI* 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 physical interfaces is enabled by default; 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
7.0(1)	This command was introduced.

Usage Guidelines

The number of interfaces that can be monitored for the security appliance is 250. Hello messages are exchanged during every interface poll frequency time period between the security appliance 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.

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	Restores the default interface health monitoring for all interfaces.
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.

more *{***/ascii | /binary| /ebcdic | disk0: | disk1: | 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.
disk0*:*	(Optional) Displays a file on the internal Flash memory.
disk1:	(Optional) Displays a file on the external Flash memory card.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
ftp:	(Optional) Displays a file on an FTP server.
http:	(Optional) Displays a file on a web site.
https:	(Optional) Displays a file on a secure web site.
system:	(Optional) Displays the file system.
tftp:	(Optional) Displays a file on a TFTP server.
filename	Specifies the name of the file to display.

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
7.0(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

This 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.

mount (CIFS)

To make a Common Internet File System (CIFS) accessible to the security appliance, use the **mount** command in global configuration mode. This command lets you enter config-mount-cifs configuration mode. To un-mount the CIFS network file system, use the **no** form of this command.

mount *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

[**no**] **mount** *name* **type cifs server** *server-name* **share** *share* **status enable | status disable [domain** *domain-name* **] username** *username* **password** *password*

Syntax Description

domain *domain-name*	(Optional) For CIFS file systems only, this argument specifies the Windows NT domain name. A maximum of 63 characters is permitted.
name	Specifies the name of an existing file system to be assigned to the Local CA.
no	Removes an already mounted CIFS file system and renders it inaccessible.
password *password*	Identifies the authorized password for file-system mounting.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the CIFS file-system server.
share *sharename*	Explicitly identifies a specific server share (a folder) by name to access file data within a server.
status enable/disable	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
type	Specifies the CIFS type of file system to mount. For alternative **type** keywords, refer to the **mount (FTP)** command.
type cifs	Specifies that the file system being mounted is CIFS, a file system that provides volume-mounting capabilities for CIFS-shared directories.
user *username*	The authorized username for file-system mounting.

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**
config-mount-cifs configuration	•	•	•	—	•
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **mount** command uses the Installable File System (IFS) to mount the CIFS file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

The **mount** command attaches the CIFS file system on the security appliance to the UNIX file tree. Conversely, the **no mount** command detaches it.

The *mount-name* specified in the **mount** command is used by other CLI commands to refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of an existing mounted file system to save database files to non-flash storage.

The CIFS remote file-access protocol is compatible with the way applications share data on local disks and network file servers. Running over TCP/IP and using the Internet's global DNS, CIFS is an enhanced version of Microsoft's open, cross-platform Server Message Block (SMB) protocol, the native file-sharing protocol in the Windows operating systems.

Always exit from the root shell after using the **mount** command. The **exit** keyword in mount-cifs-config mode returns the user to global configuration mode.

In order to reconnect, remap your connections to storage.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

The following example mounts *cifs://amer;chief:big-boy@myfiler02/my_share* as the label, *cifs_share:*

```
hostname(config)# mount cifs_share type CIFS
hostname (config-mount-cifs)# server myfiler02a
```

Related Commands

Command	Description
debug cifs	Logs CIFS debug messages.
debug ntdomain	Logs Web VPN NT Domain debug messages
debug webvpn cifs	Logs WebVPN CIFS debug messages.
dir all-filesystems	Displays the files of all filesystems mounted on the security appliance.

mount (FTP)

To make a File Transfer Protocol (FTP) file system accessible to the security appliance, use the **mount** *name* **type ftp** command in global configuration mode to enter Mount FTP configuration mode. The **no mount** *name* **type ftp** command is used to un-mount the FTP network file system.

[**no**] **mount** *name* **type FTP server** *server-name* **path** *pathname* **status enable | status disable mode active | mode passive username** *username* **password** *password*

Syntax Description

exit	Exit from Mount-FTP Configuration mode and return to Global Configuration mode.
ftp	Specifies that the file system being mounted is FTP, a Linux kernel module, enhancing the Virtual File System (VFS) with FTP volume-mounting capabilities that allow you to mount FTP-shared directories.
mode	Identifies the FTP Transfer Mode as either Active or Passive.
no	Removes an already mounted FTP file system, rendering it inaccessible.
password *password*	Identifies the authorized password for file-system mounting.
path *pathname*	Specifies the directory pathname to the specified FTP file-system server. The pathname cannot contain spaces.
server *server-name*	Specifies the predefined name (or the IP address in dotted decimal notation) of the FTPFS file-system server.
status enable/disable	Identifies the state of the file system as mounted or un-mounted (available or unavailable).
username *username*	Specifies the authorized username for file-system mounting

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**
config-mount-ftp	•	•	•	—	•
Global Configuration	•	•	•	—	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **mount** *name* **type ftp** command uses the Installable File System (IFS) to mount the specified network file system. IFS, a filesystem API, enables the security appliance to recognize and load drivers for file systems.

To confirm that the FTP file system actually is mounted, use the **dir all-filesystems** instruction

The mount-name specified in the **mount** command is used when other CLI commands refer to the filesystem already mounted on the security appliance. For example, the **database** command, which sets up file storage for the Local Certificate Authority, needs the mount name of a mounted file system to save database files to non-flash storage.

Note Using the **mount** command when you create an FTP-type mount requires that the FTP Server must have a UNIX directory listing style. Microsoft FTP servers have a default of MS-DOS directory listing style.

Note Mounting of CIFS and FTP file systems are supported. (See the **mount** *name* **type ftp** command.) Mounting Network File System (NFS) volumes is not supported for this release.

Examples

This example mounts *ftp://amor;chief:big-kid@myfiler02* as the label, *my ftp:*

```
hostname(config)# mount myftp type ftp server myfiler02a path status enable username
chief password big-kid
```

Related Commands

Command	Description
debug webvpn	Logs WebVPN debug messages.
ftp mode passive	Controls interaction between the FTP client on the security appliance and the FTP server.

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* [**dense** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [**dense** *output_if_name*] | *rpf_addr*} [*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_addr	Specifies the incoming interface for the mroute. If the RPF address PIM neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-addr* argument can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system.
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
Preexisting	This command was preexisting.

Usage Guidelines

This command lets you statically configure where multicast sources are located. The security appliance 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.

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
clear configure mroute	Removes the **mroute** commands from the configuration.
show mroute	Displays the IPv4 multicast routing table.
show running-config mroute	Displays the **mroute** commands in the configuration.

msie-proxy except-list

To configure Microsoft Internet Explorer browser proxy exception list settings for a local bypass on the client PC, enter the **msie-proxy except-list** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

Syntax Description

none	Indicates that there is no IP address/hostname or port and prevents inheriting an exception list.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client PC. The port num ber is optional.

Defaults

By default, msie-proxy except-list is disabled.

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**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Examples

The following example shows how to set a Microsoft Internet Explorer proxy exception list, consisting of the server at IP address 192.168.20.1, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy local-bypass

To configure Microsoft Internet Explorer browser proxy local-bypass settings for a client PC, enter the **msie-proxy local-bypass** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

Syntax Description

disable	Disables Microsoft Internet Explorer browser proxy local-bypass settings for a client PC.
enable	Enables Microsoft Internet Explorer browser proxy local-bypass settings for a client PC.

Defaults

By default, msie-proxy local-bypass is disabled.

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
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to enable Microsoft Internet Explorer proxy local-bypass for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy method

To configure the browser proxy actions ("methods") for a client PC, enter the **msie-proxy method** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]

Note See the Usage Guidelines section for qualifications that apply to this syntax.

Syntax Description

auto-detect	Enables the use of automatic proxy server detection in Internet Explorer or Firefox for the client PC.
no-modify	Leaves the HTTP browser proxy server setting in the browser unchanged for this client PC.
no-proxy	Disables the HTTP proxy setting in the browser for the client PC.
use-pac-url	Directs Internet Explorer to retrieve the HTTP proxy server setting from the proxy auto-configuration file URL specified in the **msie-proxy pac-url** command. This option is valid only for Internet Explorer.
use-server	Sets the HTTP proxy server setting in the browser to use the value configured in the **msie-proxy server** command.

Defaults

The default method is use-server.

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**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Added the use-pac-url option.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number can contain up to 100 characters.

The Safari browser does not support auto-detect. The Firefox and Safari browsers support the use of only one of these command options at a time. Microsoft Internet Explorer supports the following combinations of options for this command:

[no] msie-proxy method no-proxy

[no] msie-proxy method no-modify

[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. The .pac file resides on a web server. When you specify **use-pac-url**, Internet Explorer uses the .pac file to determine the proxy settings. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file.

Examples

The following example shows how to configure auto-detect as the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

The following example configures the Microsoft Internet Explorer proxy setting for the group policy named FirstGroup to use the server QAserver, port 1001 as the server for the client PC:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy pac-url	Specifies a URL from which to retrieve a proxy auto-configuration file.
msie-proxy server	Configures a Microsoft Internet Explorer browser proxy server and port for a client PC.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy pac-url

To tell a browser where to look for proxy information, enter the **msie-proxy pac-url** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy pac-url {**none** | **value** *url*}

no msie-proxy pac-url

Syntax Description

none	Specifies that there is no URL value.
value *url*	Specifies the URL of the website at which the browser can get the proxy auto-configuration file that defines the proxy server or servers to use.

Defaults

The default value is none.

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**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Requirements

To use the proxy auto-configuration feature, the remote user must use the Cisco AnyConnect VPN Client. To enable the use of the proxy auto-configuration URL, you must also configure the **msie-proxy method** command with the **use-pac-url** option.

Why Use This Command

Many network environments define HTTP proxies that connect a web browser to a particular network resource. The HTTP traffic can reach the network resource only if the proxy is specified in the browser and the client routes the HTTP traffic to the proxy. SSLVPN tunnels complicate the definition of HTTP proxies because the proxy required when tunneled to an enterprise network can differ from that required when connected to the Internet via a broadband connection or when on a third-party network.

In addition, companies with large networks might need to configure more than one proxy server and let users choose between them, based on transient conditions. By using .pac files, an administrator can author a single script file that determines which of numerous proxies to use for all client computers throughout the enterprise.

The following are some examples of how you might use a PAC file:

- Choosing a proxy at random from a list for load balancing.
- Rotating proxies by time of day or day of the week to accommodate a server maintenance schedule.
- Specifying a backup proxy server to use in case the primary proxy fails.
- Specifying the nearest proxy for roaming users, based on the local subnet.

How to Use the Proxy Auto-Configuration Feature

You can use a text editor to create a proxy auto-configuration (.pac) file for your browser. A .pac file is a JavaScript file that contains logic that specifies one or more proxy servers to be used, depending on the contents of the URL. Use the **msie-proxy pac-url** command to specify the URL from which to retrieve the .pac file. Then, when you specify **use-pac-url** in the **msie-proxy method** command, the browser uses the .pac file to determine the proxy settings.

Examples

The following example shows how to configure a browser to get its proxy setting from the URL www.mycompanyserver.com for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url value http://www.mycompanyserver.com
hostname(config-group-policy)#
```

The following example disables the proxy auto-configuration feature for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy pac-url none
hostname(config-group-policy)#
```

Related Commands

Command	Description
msie-proxy method	Configures the browser proxy actions (“methods”) for a client PC.
msie-proxy server	Configures a Microsoft Internet Explorer browser proxy server and port for a client PC.
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

msie-proxy server

To configure a Microsoft Internet Explorer browser proxy server and port for a client PC, enter the **msie-proxy server** command in group-policy configuration mode. To remove the attribute from the configuration, use the **no** form of the command.

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

Syntax Description

none	Indicates that there is no IP address/hostname or port specified for the proxy server and prevents inheriting a server.
value *server:port*	Specifies the IP address or name of an MSIE server and port that is applied for this client PC. The port number is optional.

Defaults

By default, no msie-proxy server is specified.

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**
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The line containing the proxy server IP address or hostname and the port number must be less than 100 characters long.

Examples

The following example shows how to configure the IP address 192.168.10.1 as a Microsoft Internet Explorer proxy server, using port 880, for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

Related Commands

Command	Description
show running-configuration group-policy	Shows the value of the configured group-policy attributes.
clear configure group-policy	Removes all configured group-policy attributes.

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
Preexisting	This command was preexisting.

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 security appliance 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 security appliance 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

This 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 boundary

To configure a multicast boundary for administratively-scoped multicast addresses, use the **multicast boundary** command in interface configuration mode. To remove the boundary, use the **no** form of this command. A multicast boundary restricts multicast data packet flows and enables reuse of the same multicast group address in different administrative domains.

multicast boundary *acl* [**filter-autorp**]

no multicast boundary *acl* [**filter-autorp**]

Syntax Description

acl	Specifies an access list name or number. The access list defines the range of addresses affected by the boundary. Use only standard ACLs with this command; extended ACLs are not supported.
filter-autorp	Filters Auto-RP messages denied by the boundary ACL. If not specified, all Auto-RP messages are passed.

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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command to configure an administratively scoped boundary on an interface to filter multicast group addresses in the range defined by the *acl* argument. A standard access list defines the range of addresses affected. When this command is configured, no multicast data packets are allowed to flow across the boundary in either direction. Restricting multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Examples

The following example sets up a boundary for all administratively scoped addresses and filters the Auto-RP messages:

```
hostname(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
hostname(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# multicast boundary boundary_test filter-autorp
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the security appliance.

multicast-routing

To enable IP multicast routing on the security appliance, 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
7.0(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 20-3 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 20-3 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 security appliance:

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

Related Commands

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