CHAPTER 5

cache-time through clear capture Commands

cache-time

To specify in minutes how long to allow a CRL to remain in the cache before considering it stale, use the **cache-time** command in ca-crl configuration mode. To return to the default value, use the **no** form of this command.

cache-time *refresh-time*

no cache-time

Syntax Description

refresh-time	Specifies the number of minutes to allow a CRL to remain in the cache. The range is 1 - 1440 minutes. If the NextUpdate field is not present in the CRL, the CRL is not cached.

Defaults

The default setting is 60 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
Ca-crl configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters ca-crl configuration mode, and specifies a cache time refresh value of 10 minutes for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
enforcenextupdate	Specifies how to handle the NextUpdate CRL field in a certificate.

call-agent

To specify a group of call agents, use the **call-agent** command in mgcp map configuration mode, which is accessible by using the **mgcp-map** command. To remove the configuration, use the **no** form of this command.

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

Syntax Description

ip_address	The IP address of the gateway.
group_id	The ID of the call agent group, from 0 to 2147483647.

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
mgcp map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **call-agent** command to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one a gateway sends a command to) so that any of the call agents can send the response. Call agents with the same *group_id* belong to the same group. A call agent may belong to more than one group. The *group_id* option is a number from 0 to 4294967295. The *ip_address* option specifies the IP address of the call agent.

Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables mgcp map configuration mode.
show mgcp	Displays MGCP configuration and session information.

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command in privileged EXEC mode. To disable packet capture capabilities, use the **no** form of this command.

capture *capture_name* [**type** {**asp-drop** [*drop-code*] | **raw-data** | **isakmp**}]
access-list *access_list_name* **interface** *interface_name* [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**]

no capture *capture-name* [**type** {**asp-drop** [*drop-code*] | **raw-data** | **isakmp**}] [**access-list** *access_list_name*] **[interface** *interface_name*]

Note If the ACE attached to capture is changed, it is highly recommended to reconfigure capture to make the changes in the ACL effective for capture.

Syntax Description

access-list *access_list_name*	Captures traffic that matches an access list. In multiple context mode, this is only available within a context. This keyword is required except when you specify **type asp-drop**.
asp-drop [*drop-code*]	(Optional) Captures packets dropped by the accelerated security path. The *drop-code* specifies the type of traffic that is dropped by the accelerated security path. See the **show asp drop frame** command for a list of drop codes. If you do not enter the *drop-code* argument, then all dropped packets are captured. You can enter this keyword with **packet-length**, **circular-buffer**, and **buffer**, but not with **interface**, **access-list** or **ethernet**.
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops.
capture_name	Specifies the name of the packet capture. Use the same name on multiple **capture** statements to capture multiple types of traffic. When you view the capture configuration using the **show capture** command, all options are combined on one line.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.
ethernet-type *type*	(Optional) Selects an Ethernet type to capture. The default is IP packets.
interface *interface_name*	Sets the name of the interface on which to use packet capture. You must configure an interface for any packets to be captured. You can configure multiple interfaces using multiple **capture** commands with the same name. This keyword is required except when you specify **type asp-drop**.
isakmp	(Optional) Captures ISAKMP traffic. In multiple context mode, this is only available within a context.
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces. This setting is the default.
type	(Optional) Lets you specify the type of data captured.

Defaults

The defaults are as follows:

- The default **type** is **raw-data**.
- The default **buffer** *size* is 512 KB.
- The default Ethernet type is IP.
- The default **packet-length** is 68 bytes.

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
1.1(1)	This command was introduced.
3.1(1)	Added the capability to capture all traffic, not just traffic that passes through the general-purpose processor.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. You can create multiple captures. To view the packet capture, use the **show capture** *name* command. To save the capture to a file, use the **copy capture** command.

The FWSM is capable of tracking all IP traffic that flows across it. It is also capable of capturing all the IP traffic that is destined to the FWSM, including all the management traffic (such as SSH and Telnet traffic) to the FWSM.

Enter the **no capture** command with the **access-list** and **interface** keywords to stop the capture without deleting the capture buffer. To stop the capture and delete the buffer, enter **no capture** *name* without additional keywords.

Note The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby unit during failover.

Examples

The following example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
hostname(config)# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname(config)# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname(config)# capture captest access-list http packet-length 74 interface inside
```

Related Commands

Command	Description
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.
show capture	Displays the capture configuration when no options are specified.

cd

To change the current working directory to the one specified, use the **cd** command in privileged EXEC mode.

cd [**flash:**] [*path*]

Syntax Description

flash:	Specifies the internal Flash memory, followed by a colon.
path	(Optional) The absolute path of the directory to change to.

Defaults

If you do not specify a directory, the directory is changed to the root 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
2.2(1)	Support for this command was introduced.

Examples

This example shows how to change to the “config” directory:

```
hostname# cd flash:/config/
```

Related Commands

Command	Description
pwd	Displays the current working directory.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain configuration mode. When you use this command, the FWSM interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate. To delete the certificate, use the **no** form of this command.

certificate {**ca** | **ra-encrypt** | **ra-sign** | **ra-general**} *certificate-serial-number*

no certificate *certificate-serial-number*

Syntax Description

ca	Indicates that the certificate is a certificate authority issuing certificate.
certificate-serial-number	Specifies the serial number of the certificate in hexadecimal format ending with the word quit.
ra-encrypt	Indicates that the certificate is a registration authority key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is a registration authority certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an registration authority digital signature certificate used in SCEP messaging.

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
Crypto ca certificate chain configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A certificate authority is an authority in a network that issues and manages security credentials and public key for message encryption. As part of a public key infrastructure, a CA checks with a registration authority to verify information provided by the requestor of a digital certificate. If the requestor information is verified by the RA, the CA can then issue a certificate.

Examples

The following example enters ca trustpoint mode for a trustpoint named central, then enters crypto ca certificate chain mode for central, and adds a CA certificate with a serial number 29573D5FF010FE25B45:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

Related Commands

Command	Description
clear configure crypto map	Clears all configuration for all crypto maps.
show running-config crypto map	Displays the crypto map configuration.
crypto ca certificate chain	Enters certificate crypto ca certificate chain configuration mode.
crypto ca trustpoint	Enters ca trustpoint configuration mode.
show running-config crypto map	Displays all configuration for all the crypto maps.

chain

To enable sending of a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. This action includes the root certificate and any subordinate CA certificates in the transmission. To return this command to the default, use the **no** form of this command.

chain

no chain

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command 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
Tunnel-group ipsec attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, enables sending a chain for an IPSec LAN-to-LAN tunnel group with the IP address of 209.165.200.225, which includes the root certificate and any subordinate CA certificates:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# chain
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map default-group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

changeto

To change between security contexts and the system, use the **changeto** command in privileged EXEC mode.

changeto {**system** | **context** *name*}

Syntax Description

context *name*	Changes to the context with the specified name.
system	Changes to the system execution space.

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
Privileged EXEC	•	•	—	•	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

If you log in to the system execution space or the admin context, you can change between contexts and perform configuration and monitoring tasks within each context. The "running" configuration that you edit in configuration mode, or that is used in the **copy** or **write** commands, depends on which execution space you are in. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context execution space, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) by entering the **show running-config** command. Only the current configuration appears.

Examples

The following example changes between contexts and the system in privileged EXEC mode:

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

The following example changes between the system and the admin context in interface configuration mode. When you change between execution spaces, and you are in a configuration mode, the mode changes to the global configuration mode in the new execution space.

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

Related Commands

Command	Description
admin-context	Sets a context to be the admin context.
context	Creates a security context in the system configuration and enters context configuration mode.
show context	Shows a list of contexts (system execution space) or information about the current context.

checkheaps

To configure checkheaps verification intervals, use the **checkheaps** command in global configuration mode. To set the value to the default, use the **no** form of this command. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

Syntax Description

check-interval	Sets the buffer verification interval. The buffer verification process checks the sanity of the heap (allocated and freed memory buffers). During each invocation of the process, the FWSM checks the entire heap, validating each memory buffer. If there is a discrepancy, the FWSM issues either an "allocated buffer error" or a "free buffer error." If there is an error, the FWSM dumps traceback information when possible and reloads.
validate-checksum	Sets the code space checksum validation interval. When the FWSM first boots up, the FWSM calculates a hash of the entire code. Later, during the periodic check, the FWSM generates a new hash and compares it to the original. If there is a mismatch, the FWSM issues a "text checksum checkheaps error." If there is an error, the FWSM dumps traceback information when possible and reloads.
seconds	Sets the interval in seconds between 1 and 2147483.

Defaults

The default intervals are 60 seconds each.

Command Modes

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

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

Command History

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

Examples

The following example sets the buffer allocation interval to 200 seconds and the code space checksum interval to 500 seconds:

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

Related Commands

Command	Description
show checkheaps	Shows checkheaps statistics.

class

To create a resource class to which to assign a security context, use the **class** command in global configuration mode. To remove a class, use the **no** form of this command.

class *name*

no class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To set the limits for the default class, enter **default** for the 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**
Global configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

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

The FWSM manages resources by assigning contexts to resource classes. Each context uses the resource limits set by the class.

Note The FWSM does not limit the bandwidth per context; however, the switch containing the FWSM can limit bandwidth per VLAN. See the switch documentation for more information.

When you create a class, the FWSM does not set aside a portion of the resources for each context assigned to the class; rather, the FWSM sets the maximum limit for a context. If you oversubscribe resources, or allow some resources to be unlimited, a few contexts can "use up" those resources, potentially affecting service to other contexts. See the **limit-resource** command to set the resources for the class.

All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default class.

If a context belongs to a class other than the default class, those class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, if you create a class with a 2 percent limit for all concurrent connections, but no other limits, then all other limits are inherited from the default class. Conversely, if you create a class with a 2 percent limit for all resources, the class uses no settings from the default class.

By default, the default class provides unlimited access to resources for all contexts, except for the following limits, which are by default set to the maximum allowed per context:

- Telnet sessions—5 sessions.
- SSH sessions—5 sessions.
- IPSec sessions—5 sessions.
- MAC addresses—65,535 entries.

Examples

The following example sets the default class limit for conns to 10 percent instead of unlimited:

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

All other resources remain at unlimited.

To add a class called gold with all resources set to 5 percent, except for fixups, with a setting of 10 percent, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource all 5%
hostname(config-class)# limit-resource fixups 10%
```

To add a class called silver with all resources set to 3 percent, except for system log messages, with a setting of 500 per second, enter the following commands:

```
hostname(config)# class silver
hostname(config-class)# limit-resource all 3%
hostname(config-class)# limit-resource rate syslogs 500
```

Related Commands

Command	Description
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.
show class	Shows the contexts assigned to a class.

class (policy-map)

To assign a class map to a policy map where you can assign actions to the class map traffic, use the **class** command in policy-map configuration mode. To remove a class map from a policy map, use the **no** form of this command.

class *classmap-name*

no class *classmap-name*

Syntax Description

classmap-name	Specifies the name for the class map. For a Layer 3/4 policy map (the **policy-map** command), you must specify a Layer 3/4 class map name (the **class-map** command). For an inspection policy map (the **policy-map type inspect** command), you must specify an inspection class map name (the **class-map type inspect** command).

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The configuration always includes a class map called “class-default” that matches all traffic. At the end of every Layer 3/4 policy map, the configuration includes the class-default class map with no actions defined. This is for internal use only, and cannot be modified.

Including the class-default class map, up to 63 **class** and **match** commands can be configured in a policy map.

After you add the class map to the policy map with the **class** command, you can define one or more actions to be performed on the traffic. Features supported in class configuration mode of a Layer 3/4 policy map include:

- Connection features
- Application inspection

Features supported in class configuration mode of an inspection policy map include:

- Dropping a packet
- Dropping a connection

- Resetting a connection
- Logging
- Masking content

Examples

The following is an example of a **policy-map** command for connection policy that includes the **class** command. It limits the number of connections allowed to the web server 10.1.1.1:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

The following example shows how multi-match works in a policy map:

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

The following example shows how traffic matches the first available class map, and will not match any subsequent class maps that specify actions in the same feature domain:

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

When a Telnet connection is initiated, it matches **class telnet_traffic**. Similarly, if an FTP connection is initiated, it matches **class ftp_traffic**. For any TCP connection other than Telnet and FTP, it will match **class tcp_traffic**. Even though a Telnet or FTP connection can match **class tcp_traffic**, the FWSM does not make this match because they previously matched other classes.

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
class-map type management	Creates a Layer 3/4 class map for management traffic.
clear configure policy-map	Removes all policy-map configuration, except for any policy-map that is in use in a service-policy command.
match	Defines the traffic-matching parameters.
policy-map	Configures a policy; that is, an association of one or more traffic classes, each with one or more actions.

class-map

When using the Modular Policy Framework, identify Layer 3 or 4 traffic to which you want to apply actions by using the **class-map** command (without the **type** keyword) in global configuration mode. To delete a class map, use the **no** form of this command.

class-map *class_map_name*

no class-map *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. The maximum number of class maps (Layer 3/4, inspection, and regular expression) is 255 in single mode or per context in multiple mode. This limit includes default class maps.

You can create multiple Layer 3/4 class maps for each Layer 3/4 policy map.

Default Class Maps

The configuration includes many internally-created default class maps, including a default Layer 3/4 class map that the FWSM uses in the default global policy. It is called **inspection_default** and matches the default inspection traffic:

```
class-map inspection_default
 match default-inspection-traffic
```

Another class map that exists in the default configuration is called class-default, and it matches all traffic:

```
class-map class-default
```

```
match any
```

This class map appears at the end of all Layer 3/4 policy maps and essentially tells the FWSM to not perform any actions on all other traffic. You can use the class-default class map if desired, rather than making your own **match any** class map.

Default class maps also include inspection class maps.

To view all default class maps, as well as any user-created class maps, enter the **show running-config all class-map** command.

Maximum Class Maps

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type inspect**
- **class-map type regex**
- **match** commands used in policy-map type inspection mode

This limit also includes default class maps of all types.

Configuration Overview

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.
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.

   Use the **class-map** command to enter class-map configuration mode. From class-map configuration mode, you can define the traffic to include in the class using the **match** command. A Layer 3/4 class map contains, at most, one **match** command that identifies the traffic included in the class map except if you have the **match default-inspection-traffic** command. In that case, you can specify a **match access-list** command along with the **match default-inspection-traffic** command to narrow the matched traffic. Because the **match default-inspection-traffic** command specifies the ports to match, any ports in the access list are ignored.

Examples

The following example creates four Layer 3/4 class maps:

```
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 all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

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
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type inspect

When using the Modular Policy Framework, match criteria that is specific to an inspection application by using the **class-map type inspect** command in global configuration mode. To delete an inspection class map, use the **no** form of this command.

class-map type inspect *application* [**match-all**] *class_map_name*

no class-map [**type inspect** *application* [**match-all**]] *class_map_name*

Syntax Description

application	Specifies the type of application traffic you want to match. Available types include: • **http** • **sip**
class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-all	(Optional) Specifies that traffic must match all criteria to match the class map. **match-all** is the default and only option.

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
4.0(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map. The class map contains one or more **match** commands. (You can alternatively use **match** commands directly in the inspection policy map if you want to pair a single criterion with an action). You can match criteria that is specific to an application. For example, for HTTP traffic, you can match text in a URL.

The difference between creating a class map and defining the traffic match directly in the inspection policy map is that the class map lets you group multiple match commands, and you can reuse class maps. For the traffic that you identify in this class map, you can specify actions such as dropping, resetting, and/or logging the connection in the inspection policy map.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type inspect**
- **class-map type regex**
- **match** commands used in policy-map type inspection mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates an HTTP class map that must match all criteria:

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map for through traffic.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
show running-config class-map	Displays the information about the class map configuration.

class-map type regex

When using the Modular Policy Framework, group regular expressions for use with matching text by using the **class-map type regex** command in global configuration mode. To delete a regular expression class map, use the **no** form of this command.

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

Syntax Description

class_map_name	Specifies the class map name up to 40 characters in length. The names "class-default" and any name that begins with "_internal" or "_default" are reserved. All types of class maps use the same name space, so you cannot resuse a name already used by another type of class map.
match-any	Specifies that the traffic matches the class map if it matches only one of the regular expressions. **match-any** is the only option.

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
4.0(1)	This command was introduced.

Usage Guidelines

Modular Policy Framework lets you configure special actions for many application inspections. When you enable an inspection engine in the Layer 3/4 policy map, you can also optionally enable actions as defined in an *inspection policy map* (see the **policy-map type inspect** command).

In the inspection policy map, you can identify the traffic you want to act upon by creating an inspection class map containing one or more **match** commands or you can use **match** commands directly in the inspection policy map. Some **match** commands let you identify text in a packet using a regular expression; for example, you can match URL strings inside HTTP packets. You can group regular expressions in a regular expression class map.

Before you create a regular expression class map, create the regular expressions using the **regex** command. Then, identify the named regular expressions in class-map configuration mode using the **match regex** command.

The maximum number of class maps of all types is 255 in single mode or per context in multiple mode. Class maps include the following types:

- **class-map**
- **class-map type inspect**
- **class-map type regex**
- **match** commands used in policy-map type inspection mode

This limit also includes default class maps of all types. See the **class-map** command for more information.

Examples

The following example creates two regular expressions, and adds them to a regular expression class map. Traffic matches the class map if it includes the string “example.com” or “example2.com.”

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2
```

Related Commands

Command	Description
class-map type inspect	Creates ain inspection class map to match traffic specific to an application.
policy-map	Creates a policy map by associating the traffic class with one or more actions.
policy-map type inspect	Defines special actions for application inspection.
service-policy	Creates a security policy by associating the policy map with one or more interfaces.
regex	Creates a regular expression.

clear aaa local user fail-attempts

To reset the number of failed user authentication attempts to zero without modifying a user locked-out status, use the **clear aaa local user fail-attempts** command in privileged EXEC mode.

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

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**
Privileged EXEC	•	•	•	•	—

Command History

Release	**Modification**
3.1(1)	This command was introduced.

Usage Guidelines

Use this command when a user fails authentication a few times, but you want to reset to counter to zero, for example, when the configuration has recently been modified.

After the configured number of failed authentication attempts, the user is locked out of the system and cannot successfully log in until either a system administrator unlocks the username or the system reboots.

The number of failed attempts resets to zero and the lockout status resets to No when the user successfully authenticates or when the FWSM reboots.

Locking or unlocking a username results in a syslog message.

A system administrator with a privilege level of 15 cannot be locked out.

Examples

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

The following example shows use of the **clear aaa local user authentication fail-attempts** command to reset the failed-attempts counter to 0 for all users:

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user lockout	Resets the number of failed user authentication attempts to zero without modifying a user locked-out status.
show aaa local user [**locked**]	Shows the list of usernames that are currently locked.

clear aaa local user lockout

To clear the lockout status of the specified users and set their failed-attempts counter to 0, use the **clear aaa local user lockout** command in privileged EXEC mode.

clear aaa local user lockout {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
name	Specifies a specific username for which the failed-attempts counter is reset to 0.
username	Indicates that the following parameter is a username, for which the failed-attempts counter is reset to 0.

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can specify a single user by using the **username** option or all users with the **all** option.

This command affects only the status of users that are locked out.

The administrator cannot be locked out of the device.

Locking or unlocking a username results in a syslog message.

Examples

The following example shows use of the **clear aaa local user lockout** command to clear the lockout condition and reset the failed-attempts counter to 0 for the username anyuser:

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures a limit on the number of failed user authentication attempts allowed.
clear aaa local user fail-attempts	Resets the number of failed user authentication attempts to zero without modifying the user locked-out status.
show aaa local user [**locked**]	Shows the list of usernames that are currently locked.

clear aaa-server statistics

To reset the statistics for AAA servers, use the **clear aaa-server statistics** command in privilged EXEC mode.

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

groupname	(Optional) Clears statistics for servers in a group.
host *hostname*	(Optional) Clears statistics for a particular server in the group.
LOCAL	(Optional) Clears statistics for the LOCAL user database.
protocol *protocol*	(Optional) Clears statistics for servers of the specificed protocol: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Defaults

Remove all AAA-server statistics across all groups.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following command shows how to reset the AAA statistics for a specific server in a group:

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

The following command shows how to reset the AAA statistics for an entire server group:

```
hostname(config)# clear aaa-server statistics svrgrp1
```

The following command shows how to reset the AAA statistics for all server groups:

```
hostname(config)# clear aaa-server statistics
```

The following command shows how to reset the AAA statistics for a particular protocol (in this case, TACACS+):

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

Related Commands

Command	Description
aaa-server protocol	Specifies and manages the grouping of AAA server connection data.
clear configure aaa-server	Removes all non-default aaa server groups or clear the specified group
show aaa-server	Displays AAA server statistics.
show running-config aaa-server	Displays the current AAA server configuration values.

clear access-list

To clear an access-list counter, use the **clear access-list** command in global configuration mode.

clear access-list [*id*] **counters**

Syntax Description

counters	Clears access list counters.
id	(Optional) Name or number of an access list.

Defaults

All the access list counters are cleared.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

When you enter the **clear access-list** command, all the access list counters are cleared if you do not specify an *id*.

Examples

The following example shows how to clear a specific access list counter:

```
hostname# clear access-list inbound counters
```

Related Commands

Command	Description
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
access-list standard	Adds an access list to identify the destination IP addresses of OSPF routes, which can be used in a route map for OSPF redistribution.
clear configure access-list	Clears an access list from the running configuration.
show access-list	Displays the access list entries by number.
show running-config access-listt	Displays the access list configuration that is running on the FWSM.

clear arp

To clear dynamic ARP entries or ARP statistics, use the **clear arp** command in privileged EXEC mode.

clear arp [**statistics**]

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
Privileged EXEC	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example clears all ARP statistics:

```
hostname# clear arp statistics
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	For transparent firewall mode, inspects ARP packets to prevent ARP spoofing.
show arp statistics	Shows ARP statistics.
show running-config arp	Shows the current configuration of the ARP timeout.

clear asp drop

To clear accelerated security path drop statistics, use the **clear asp drop** command in privileged EXEC mode.

clear asp drop [**flow** *type* | **frame** *type*]

Syntax Description

flow	(Optional) Clears the dropped flow statistics.
frame	(Optional) Clears the dropped packet statistics.
type	(Optional) Clears the dropped flow or packets statistics for a particular process. See the "Usage Guidelines" section for a list of types.

Defaults

By default, this command clears all drop statistics.

Command Modes

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

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

Command History

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

Usage Guidelines

Process types include the following:

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

Examples

The following example clears all drop statistics:

```
hostname# clear asp drop
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

clear blocks

To reset the packet buffer counters such as the low watermark and history information, use the **clear blocks** command in privileged EXEC mode.

clear blocks

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**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Also clears the history information stored during the last buffer allocation failure.

Examples

The following example clears the blocks:

```
hostname# clear blocks
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
show blocks	Shows the system buffer utilization.

clear capture

To clear the capture buffer, use the **clear capture** command in privileged EXEC mode.

clear capture *capture_name*

Syntax Description

capture_name	Name of the packet capture.

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
Priveleged EXEC	•	•	•	•	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

To prevent accidental clearing of all packet captures, the shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is not supported.

Examples

The following example shows how to clear the capture buffer for the capture buffer “capture1”:

```
hostname(config)# clear capture capture1
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
show capture	Displays the capture configuration when no options are specified.