



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**

cache-time *refresh-time*

Syntax Description

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		
	Routed	Transparent	Single	Multiple Context	System
	•	•	•	•	—

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
```

Related Commands

crl configure	Enters crl configuration mode.
crypto ca trustpoint	
enforcenextupdate	

call-agent

is accessible by using 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 call-agent` form of this command.

ip_address group_id

ip_address group_id

The ID of the call agent group, from 0 to 2147483647.

MGCP map configuration					—

3.1(1) This command was introduced.

Usage Guidelines

Call agents must 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.

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:

```
mgcp-map mgcp_inbound
  call-agent 10.10.11.5 101
  call-agent 10.10.11.6 101
  call-agent 10.10.11.7 102
  call-agent 10.10.11.8 102
  gateway 10.10.10.115 101
  gateway 10.10.10.116 102
```

debug mgcp

mgcp-map

show mgcp

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the `capture` command. To disable packet capture capabilities, use the `no capture` form of this command.

```
capture_name { [ interface_name [ buf_size ] | [ type packet-length bytes ] } [ access_list_name ]  
[ circular-buffer
```

```
no capture capture-name type asp-drop drop-code raw-data access-list access_list_name]  
[interface ]
```



Note

Syntax Description

available within a context. This keyword is required except when you specify

(Optional) Captures packets dropped by the accelerated security path. The `type` specifies the type of traffic that is dropped by the accelerated security path. See the `show security` command for a list of drop codes. If you do not enter the `type` argument, then all dropped packets are captured.

You can enter this keyword with `raw-data`, `raw-data`, and `raw-data`, but not with `raw-data`, `raw-data` or `raw-data`.

(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops.

Specifies the name of the packet capture. Use the same name on multiple 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.

(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.

(Optional) Selects an Ethernet type to capture. The default is IP packets.

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 `capture`.

(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.

(Optional) Captures inbound and outbound packets on one or more interfaces. This setting is the default.

(Optional) Lets you specify the type of data captured.

The defaults are as follows:

- The default `capture-buffer-size` is `1024`.
- The default `capture-buffer-size` is 512 KB.
- The default Ethernet type is IP.
- The default `capture-buffer-size` is 68 bytes.

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

Privileged EXEC					

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.

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` command. To save the capture to a file, use the `copy` 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 `capture` command with the `no-buffer` and `no-clear` keywords to stop the capture without deleting the capture buffer. To stop the capture and delete the buffer, enter `clear capture` without additional keywords.



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

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

```
access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
capture capttest access-list http packet-length 74 interface inside
```

On a web browser, the capture contents for a capture named "captest" can be viewed at the following location, depending on firewall mode and version:

Before version 3.1(7) and 3.2(2):

`https://171.69.38.95/capture/captest`

`https://171.69.38.95/capture/single_vf/captest`

`https://171.69.38.95/capture/context_name/captest`

Where context_name is the actual name of the context where the capture was configured. To download the binary capture file from the FWSM, append "/pcap" to the end of the URL. For example:

Clears the capture buffer.

Copies a capture file to a server.

Displays the capture configuration when no options are specified.

cd

flash:]

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

Privileged EXEC				—	

2.2(1) Support for this command was introduced.

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

Displays the current working directory.

certificate

quit

no

certificate ca ra-encrypt ra-sign ra-general

no certificate

Specifies the serial number of the certificate in hexadecimal format ending with the word quit.

Indicates that the certificate is a certificate authority issuing certificate.

Indicates that the certificate is a registration authority key encipherment certificate used in SCEP.

Indicates that the certificate is a registration authority certificate used for digital signing and key encipherment in SCEP messaging.

Indicates that the certificate is an registration authority digital signature certificate used in SCEP messaging.

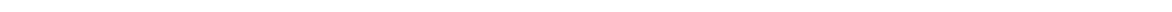
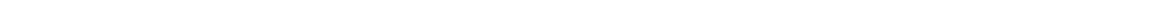
Crypto ca certificate chain configuration				—

3.1(1) This command was introduced.

requestor's information, the CA can then issue a certificate.

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



changeto

Syntax Description

Defaults

Command Modes

Command History

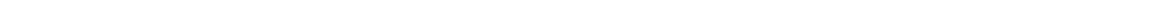
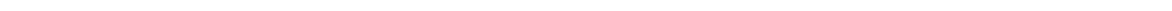
Usage Guidelines

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.

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

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

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



checkheaps

```
checkheaps {check-interval validate-checksum
```

```
no checkheaps {check-interval validate-checksum
```

check-interval

validate-checksum

show checkheaps

class

no

class

no class

Specifies the name as a string up to 20 characters long. To set the limits for the default class, enter for the name.

Global configuration	N/A	N/A	—	—

2.2(1) This command was introduced.



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 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.

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

```
limit-resource conns 10%
```

```
class gold
  limit-resource all 5%
  limit-resource fixups 10%
```

```
class silver
  limit-resource all 3%
  limit-resource rate syslogs 500
```

class (policy-map)

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Usage Guidelines

-
-
-

Examples

■ class (policy-map)

description This policy map defines a policy concerning connection to http server.

```
class myhttp
  set connection conn-max 256
```

Related Commands

Command	Description

Maximum Class Maps

Configuration Overview

- 1.
- 2.
- 3.

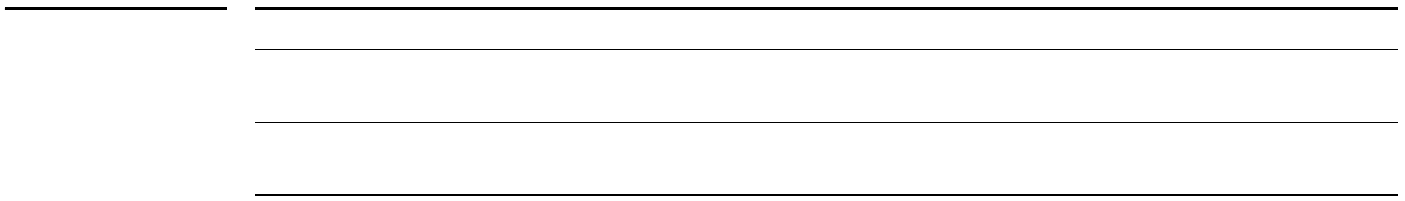
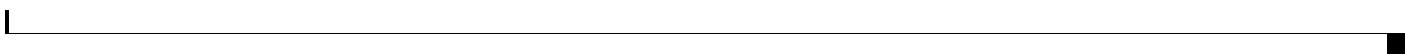
Examples

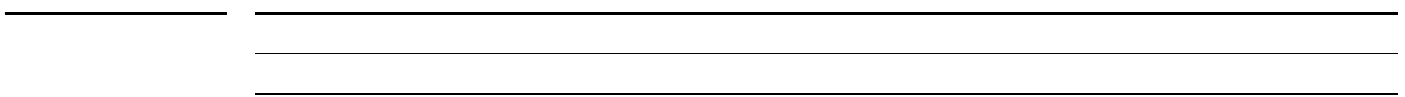
```
description "This class-map matches all UDP traffic"  
match access-list udp
```

```
class-map all_tcp  
description "This class-map matches all TCP traffic"  
match access-list tcp
```

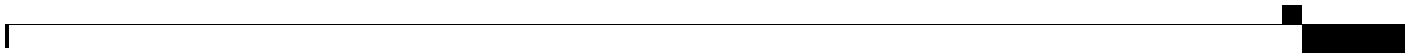
```
class-map all_http  
description "This class-map matches all HTTP traffic"  
match port tcp eq http
```

```
class-map to_server  
description "This class-map matches all traffic to server 10.1.1.1"  
match access-list host_foo
```





clear aaa local user authentication fail-attempts username anyuser



clear aaa local user authentication fail-attempts all

all}

all

username

username

all

clear aaa local user lockout

clear aaa local user lockout username anyuser

aaa local authentication attempts
max-fail

clear aaa local user fail-attempts

without modifying the user's locked-out status.

[]

Shows the list of usernames that are currently locked.

clear aaa-server statistics

LOCAL

host

protocol

LOCAL

host

protocol

kerberos

ldap

nt

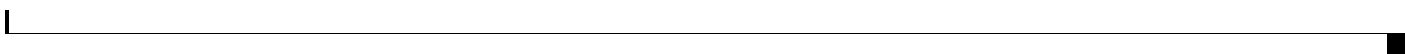
radius

sdi

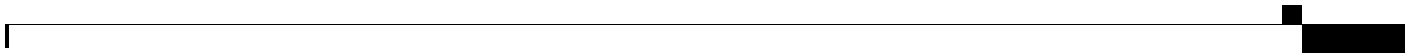
tacacs+

TACACS+):

```
clear aaa-server statistics protocol tacacs+
```



clear access-list inbound counters





`clear arp statistics`



no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oot
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

hostname#

clear blocks

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description

clear capture

Syntax Description

Defaults

Command Modes

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

Command History

Release	Modification

Usage Guidelines

Examples

Related Commands

Command	Description
