CHAPTER 5

cache through clear compression Commands

cache

To enter cache mode and set values for caching attributes, enter the **cache** command in webvpn configuration mode. To remove all cache related commands from the configuration and reset them to their default values, enter the **no** form of this command.

cache

no cache

Defaults

Enabled with default settings for each cache attribute.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, so that many applications run much more efficiently.

Examples

The following example shows how to enter cache mode:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache-static-content	Caches content not subject to rewriting.
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.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

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, which is accessible from crypto ca trustpoint 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
7.0(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. 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

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

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
7.0(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 call agents in the group (other than the one to which a gateway sends a command) 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.

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 debugging information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

call-duration-limit

To configure the call duration for an H.323 call, use the **call-duration-limit** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

Syntax Description

hh:mm:ss	Specifies the duration in hours, minutes, and seconds.

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 the call duration for an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-duration-limit 0:1:0
```

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 or 4 policy map.
show running-config policy-map	Displays all current policy map configurations.

call-party-numbers

To enforce sending call party numbers during an H.323 call setup, use the **call-party-numbers** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

call-party-numbers

no call-party-numbers

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 enforce call party numbers during call setup for an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-party-numbers
```

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 or 4 policy map.
show running-config policy-map	Displays all current policy map configurations.

call-home

To enter call home configuration mode, use the **call-home** command in global configuration mode.

call-home

Syntax Description

This command has no arguments or keywords.

Command Default

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
8.2(2)	This command was introduced.

Usage Guidelines

After you enter the **call-home** command, the prompt changes to hostname (cfg-call-home)#, and you have access to the following Call Home configuration commands:

- [**no**] **alert-group** {**group name | all**}—Enables or disables the Smart Call Home group. The default is enabled for all alert-groups.
  group name: Syslog, diagnostic, environment, inventory, configuration, snapshot, threat, telemetry, test.
- [**no**] **contact-e-mail-addr e-mail-address**—Specifies the customer contact e-mail address. This field is required.
  e-mail-address: A customer e-mail address of up to 127 characters.
- [**no**] **contact-name contact name**—Specifies the customer name.
  e-mail-address: A customer name of up to 127 characters.
- **copy profile src-profile-name dest-profile-name**—Copies the content of an existing profile (**src-profile-name**) to a new profile (**dest-profile-name**).
  src-profile-name: An existing profile name of up to 23 characters.
  dest-profile-name: A new profile name of up to 23 characters.
- **rename profile src-profile-name dest-profile-name**—Changes the name of an existing profile.
  src-profile-name: An existing profile name of up to 23 characters.
  dest-profile-name: A new profile name of up to 23 characters.
- **no configuration all**—Clears the Smart Call-home configuration.
  [**no**] **customer-id customer-id-string**—Specifies the customer ID.
  customer-id-string: A customer ID of up to 64 characters. This field is required for XML format messages.

- [**no**] **event-queue-size queue_size**—Specifies the event queue size.
  queue-size: The number of events from 5-60. The default is 10.
- [**no**] **mail-server ip-address | name priority 1-100 all**—Specifies the SMTP mail server. Customers can specify up to five mail servers. At least one mail server is required for using e-mail transport for Smart Call Home messages.
  ip-address: The IPv4 or IPv6 address of the mail server.
  name: The hostname of the mail server.
  1-100: The priority of the mail server. The lower the number, the higher the priority.
- [**no**] **phone-number phone-number-string**—Specifies the customer phone number. This field is optional.
  phone-number-string: The phone number.
- [**no**] **rate-limit msg-count**—Specifies the number of messages that Smart Call Home can send per minute.
  msg-count: The number of messages per minute. The default is 10.
- [**no**] **sender** {**from e-mail-address | reply-to e-mail-address**} —Specifies the from/reply-to e-mail address of an e-mail message. This field is optional.
  e-mail-address: The from and reply-to e-mail address.
- [**no**] **site-id site-id-string**—Specifies the customer site ID. This field is optional.
  site-id-string: A site ID to identify the location of the customer.
- [**no**] **street-address street-address**—Specifies the customer address. This field is optional.
  street-address: A free-format string of up to 255 characters.
- [**no**] **alert-group-config environment**—Enters environment group configuration mode.
  [**no**] **threshold** {**cpu | memory**} **low-high**—Specifies the environmental resource threshold.
  low, high: Valid values are 0-100. The default is 85-90.
- [**no**] **alert-group-config snapshot**—Enters snapshot group configuration mode.
  system, user: To run the CLI in sysem or user context (available only in multimode).
- [**no**] **add-command "cli command"** [{**system | user**}] —Specifies CLI commands to capture in the snapshot group.
  cli command: The CLI command to be entered.
  system, user: To run the CLI in the system or in user context (available only in multiple mode). If both the system and user are not specified, the CLI will be run in both the system and user contexts. The default is the user context.
- [**no**] **profile profile-name | no profile all**—Creates, deletes, or edits a profile. Enters profile configuration mode and changes the prompt to hostname (cfg-call-home-profile)#.
  profile-name: A profile name of up to 20 characters.
- [**no**] **active**—Enables or disables a profile. The default is enabled.
  no destination address {**e-mail | http**} **all** | [**no**] **destination** {**address** {**e-mail | http**} **e-mail-address | http-url [msg-format short-text | long-text | xml] | message-size-limit max-size | preferred-msg-format short-text | long-text | xml | transport-method e-mail | http**}—Configures the destination, message size, message format, and transport method for the Smart Call Home message receiver. The default message format is XML, and the default enabled transport method is e-mail.
  e-mail-address: The e-mail address of the Smart Call Home receiver, which can be up to 100 characters.
  http-url: The HTTP or HTTPS URL.
  max-size: The maximum message size in bytes. 0 means no limit. The default is 5 MB.

- [**no**] **subscribe-to-alert-group alert-group-name** [**severity** {**catastrophic** | **disaster** | **emergencies** | **alert** | **critical** | **errors** | **warning** | **notifications** | **informational** | **debugging**}]—Subscribes to events of a group with a specified severity level.
  alert-group-name: Syslog, diagnostic, environment, or threat are valid values.
- [**no**] **subscribe-to-alert-group syslog** [{**severity** {**catastrophic** | **disaster** | **emergencies** | **alert** | **critical** | **errors** | **warning** | **notifications** | **informational** | **debugging**} | **message start** [**-end**]}]—Subscribes to syslogs with a severity level or message ID.
  start-[**end**]: One syslog message ID or a range of syslog message IDs.
- [**no**] **subscribe-to-alert-group inventory** [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]]—Subscribes to inventory events.
  day_of_month: Day of the month, 1-31.
  day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: Hours and minutes of a day, in 24-hour time.
- [**no**] **subscribe-to-alert-group configuration** [**export full** | **minimum**] [**periodic** {**daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]]—Subscribes to configuration events.
  full: Configuration to export the running configuration, startup configurtion, feature list, number of elements in an access list, and the context name in multimode.
  minimum: Configuration to export-only feature list, number of elements in an access list, and the context name in multimode.
  day_of_month: Day of the month, 1-31.
  day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: Hours and minutes of a day, in 24-hour time.
- [**no**] **subscribe-to-alert-group telemetry periodic** {**hourly** | **daily** | **monthly day_of_month** | **weekly day_of_week** [**hh:mm**]—Subscribes to telemetry periodic events.
  day_of_month: Day of the month, 1-31.
  day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: Hours and minutes of a day, in 24-hour time.
- [**no**] **subscribe-to-alert-group snapshot periodic** {**interval minutes** | **hourly** [**mm**] | **daily** | **monthly day_of_month** |**weekly day_of_week** [**hh:mm**]}—Subscribes to snapshot periodic events.
  minutes: The interval in minutes.
  day_of_month: Day of the month, 1-31.
  day_of_week: Day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday).
  hh, mm: Hours and minutes of a day, in 24-hour time.

Note Call-home HTTPS messages can only be sent over a specified source interface on the VRF using the **ip http client source-interface** command, independent of the **vrf** command described here.

Examples

The following example show how to configure contact information:

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

The following example shows how to configure the Call Home message rate-limit threshold:

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

The following example shows how to set the Call Home message rate-limit threshold to the default setting:

```
hostname(config)# call-home
hostname(cfg-call-home)# default rate-limit
```

The following example shows how to create a new destination profile with the same configuration settings as an existing profile:

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

The following example shows how to configure the general e-mail parameters, including a primary and secondary e-mail server:

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

Related Commands

Command	Description
alert-group	Enables an alert group.
profile	Enters call-home profile configuration mode.
show call-home	Displays Call Home configuration information.

call-home send

To execute a CLI command and e-mail the command output to a specified address, use the **call-home send** command in privileged EXEC mode.

call-home send cli command [**email** *email*] [**service-number** *service number*]

Syntax Description

cli-command	Specifies the CLI command to be executed. The command output is sent by e-mail.
email *email*	Specifies the e-mail address to which the CLI command output is sent. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com.
service-number *service number*	Specifies an active TAC case number to which the command output pertains. This number is required only if no e-mail address (or a TAC e-mail address) is specified, and will appear in the e-mail subject line.

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
8.2(2)	This command was introduced.

Usage Guidelines

This command causes the specified CLI command to be executed on the system. The specified CLI command must be enclosed in quotes (“”), and can be any **run** or **show** command, including commands for all modules.

The command output is then sent by e-mail to the specified e-mail address. If no e-mail address is specified, the command output is sent to the Cisco TAC at attach@cisco.com. The e-mail is sent in long text format with the service number, if specified, in the subject line.

Examples

The following example shows how to send a CLI command and have the command output e-mailed:

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

Related Commands

call-home	Enters call home configuration mode.
call-home test	Sends a Call Home test message that you define.

service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home send alert-group

To send a specific alert group message, use the **call-home send alert-group** command in privileged EXEC mode.

call-home send alert-group {**configuration** | **telemetry** | **inventory** | **group snapshot**} [**profile** *profile-name*]

Syntax Description

configuration	Sends the configuration alert-group message to the destination profile.
group snapshot	Sends the snapshot group.
inventory	Sends the inventory call-home message.
profile *profile-name*	(Optional) Specifies the name of the destination profile.
telemetry	Sends the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay 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
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
8.2(2)	This command was introduced.

Usage Guidelines

If you do not specify the **profile** *profile-name*, the message is sent to all subscribed destination profiles.

Only the configuration, diagnostic, and inventory alert groups can be manually sent. The destination profile need not be subscribed to the alert group.

Examples

The following example shows how to send the configuration alert-group message to the destination profile:

```
hostname# call-home send alert-group configuration
```

The following example shows how to send the diagnostic alert-group message to the destination profile for a specific module, slot/subslot, or slot/bay number:

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

The following example shows how to send the diagnostic alert-group message to all destination profiles for a specific module, slot/subslot, or slot/bay number:

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

This example shows how to send the inventory call-home message:

```
hostname# call-home send alert-group inventory
```

Related Commands

call-home	Enters call home configuration mode.
call-home test	Sends a Call Home test message that you define.
service call-home	Enables or disables Call Home.
show call-home	Displays call-home configuration information.

call-home test

To manually send a Call Home test message using the configuration of a profile, use the **call-home test** command in privileged EXEC mode.

call-home test [“*test-message*”] **profile** *profile-nam*e

Syntax Description

profile *profile-name*	Specifies the name of the destination profile.
“*test-message*”	(Optional) Test message text.

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
8.2(2)	This command was introduced.

Usage Guidelines

This command sends a test message to the specified destination profile. If you enter test message text, you must enclose the text in quotes (“”) if it contains spaces. If you do not enter a message, a default message is sent.

Examples

The following example shows how to manually send a Call Home test message:

```
hostname# call-home test “test of the day” profile Ciscotac1
```

Related Commands

call-home	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.
show call-home	Displays Call Home configuration 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.

[**cluster exec**] **capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**interface asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**} {**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

[**cluster exec**] **no capture** *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy** | **raw-data** | **lacp** | **isakmp** [**ikev1** | **ikev2**] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] [**asa_dataplane**] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**reinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**} {**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

Syntax Description

access-list *access_list_name*	(Optional) Captures traffic that matches an access list. In multiple context mode, this is only available within a context.
any	Specifies any IP address instead of a single IP address and mask.
all	Captures all the packets that the ASA drops
asa_dataplane	Captures packets on the ASA backplane that pass between the ASA and the ASA CX module.
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 the **packet-length**, **circular-buffer**, and **buffer** keywords, but not with the **interface** or **ethernet-type** keyword. In a cluster, dropped forwarded data packets from one unit to another are also captured. In multiple context mode, when this option is issued in system context, all dropped data packets are captured; when this option is issued in a user context, only dropped data packets that enter from interfaces belonging to the user context are captured.
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes. Once the byte buffer is full, packet capture stops. When used in a cluster, this is the per-unit size, not the sum of all units.
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.
cluster exec	(Optional) Used only in a clustering deployment as a wrapper CLI prefix and can be used with the **capture** and **show capture** commands. Enables you to issue the **capture** command in one unit and run the command in all the other units at the same time.

ethernet-type *type*	(Optional) Selects an Ethernet type to capture. Supported Ethernet types include 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, and VLAN. An exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner Ethernet type is used for matching.
host *ip*	Specifies the single IP address of the host to which the packet is being sent.
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. To capture packets on the dataplane of an ASA, you can use the **interface** keyword with "asa_dataplane" as the interface name.You can specify "cluster" as the interface name to capture the traffic on the cluster control link interface. The interface names "cluster" and "asa-dataplane" are fixed and not configurable. If the type **lacp** capture is configured, the interface name is the physical name.
ikev1/ikev2	Captures only IKEv1 or IKEv2 protocol information.
isakmp	(Optional) Captures ISAKMP traffic for VPN connections. The ISAKMP subsystem does not have access to the upper layer protocols. The capture is a pseudo capture, with the physical, IP, and UDP layers combined together to satisfy a PCAP parser. The peer addresses are obtained from the SA exchange and are stored in the IP layer.
lacp	(Optional) Captures LACP traffic. If configured, the interface name is the physical interface name. The **trace**, **match**, and **access-list** keywords cannot be used together with the **lacp** keyword.
mask	The subnet mask for the IP address. When you specify a network mask, the method is different from the Cisco IOS software **access-list** command. The ASA uses a network mask (for example, 255.255.255.0 for a Class C mask). The Cisco IOS mask uses wildcard bits (for example, 0.0.0.255).
match *prot*	Specifies the packets that match the five-tuple to allow filtering of those packets to be captured. You can use this keyword up to three times on one line.
operator	(Optional) Matches the port numbers used by the source or destination. The permitted operators are as follows: • **lt—**less than • **gt—**greater than • **eq—**equal to • **neq**—not equal to • **range**—range
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
port	(Optional) If you set the protocol to **tcp** or **udp**, specifies the integer or name of a TCP or UDP port.
raw-data	(Optional) Captures inbound and outbound packets on one or more interfaces.
real-time	Displays the captured packets continuously in real-time. To terminate real-time packet capture, enter **Ctrl + c.** To permanently remove the capture, use the **no** form of this command. This option applies only to **raw-data** and **asp-drop** captures. This option is not supported when you use the **cluster exec capture** command.
reinject-hide	(Optional) Specifies that no reinjected packets will be captured. Applies only in a clustering environment.

tls-proxy	(Optional) Captures decrypted inbound and outbound data from TLS proxy on one or more interfaces.
trace *trace_count*	(Optional) Captures packet trace information, and the number of packets to capture. This option is used with an access list to insert trace packets into the data path to determine whether or not the packet has been processed as expected.
type	(Optional) Specifies the type of data captured.
user *webvpn-user*	(Optional) Specifies a username for a WebVPN capture.
webvpn	(Optional) Captures WebVPN data for a specific WebVPN connection.

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 packets.
- The default **packet-length** is 1518 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
6.2(1)	This command was introduced.
7.0(1)	This command was modified to include the following keywords: **type asp-drop**, **type isakmp**, **type raw-data**, and **type webvpn**.
7.0(8)	Added the **all** option to capture all packets that the ASA drops.
7.2(1)	This command was modified to include the following options: **trace** *trace_count,* **match** *prot,* **real-time, host** *ip,* **any**, *mask,* and *operator.*
8.0(2)	This command was modified to update the path to capture contents.
8.4(1)	The new **type** keywords **ikev1** and **ikev2** were added.
8.4(2)	Additional detail was added to the output for IDS.
8.4(4.1)	The **asa_dataplane** option was added to support traffic over the backplane to the ASA CX module.
9.0(1)	The **cluster, cluster exec,** and **reinject-hide** keywords were added. The new **type** option **lacp** was added. Support for multiple-context mode was added for ISAKMP.
9.1(3)	Supports filtering of packets captured on the ASA CX backplane with the **asa_dataplane** option.

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. Use the **https://***ASA-ip-address***/***admin***/capture/***capture_name*[**/pcap**] command to see the packet capture information with a web browser. If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

If you copy the buffer contents to a TFTP server in ASCII format, you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and read it with TCPDUMP or Ethereal.

Note Enabling WebVPN capture affects the performance of the ASA. Be sure to disable the capture after you generate the capture files that you need for troubleshooting.

Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** keyword is specified, the capture is detached from the specified interface and the capture is preserved. Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself.

You cannot perform any operations on a capture while the real-time display is in progress. Using the **real-time** keyword with a slow console connection may result in an excessive number of non-displayed packets because of performance considerations. The fixed limit of the buffer is 1000 packets. If the buffer fills up, a counter is maintained of the captured packets. If you open another session, you can disable the real-time display be entering the **no capture real-time** command.

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

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

The ASA architecture consists of three different sets of processors for packet processing; this architecture poses certain restrictions on the capability of the capture feature. Typically most of the packet forwarding functionality in the ASA is handled by the two front-end network processors, and packets are sent to the control-plane general-purpose processor only if they need application inspection. The packets are sent to the session management path network processor only if there is a session miss in the accelerated path processor.

Because all the packets that are forwarded or dropped by the ASA hits the two front-end network processors, the packet capture feature is implemented in these network processors. So all the packets that hit the ASA can be captured by these front end processors, if an appropriate capture is configured for those traffic interfaces. On the ingress side, the packets are captured the moment the packet hits the ASA interfaces, and on the egress side the packets are captured just before they are sent out on the wire.

After you have performed cluster-wide capture, to copy the same capture file from all units in the cluster at the same time to a TFTP server, enter the following command on the master unit:

```
hostname# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

Multiple PCAP files, one from each unit, are copied to the TFTP server. The destination capture file name is automatically attached with the unit name, such as filename_A.pcap, filename_B.pcap, and so on. In this example, A and B are cluster unit names.

Note A different destination name is generated if you add the unit name at the end of the filename.

The following are some of the limitations of the capture feature. Most of the limitations are caused by the distributed nature of the ASA architecture and by the hardware accelerators that are being used in the ASA.

- You can only capture IP traffic; you cannot capture non-IP packets such as ARPs.
- For cluster control link capture in multiple context mode, only the packet that is associated with the context sent in the cluster control link is captured.
- In multicontext mode, the **copy capture** command is available only in the system space. The syntax is as follows:

  copy /pcap capture:*Context-name*/*in-cap* **tftp**:

  Where *in-cap* is the capture configured in the context *context-name*
- The **cluster exec capture realtime** command is not supported. The following error message appears:

  ```
  Error: Real-time capture can not be run in cluster exec mode.
  ```
- For a shared VLAN, the following guidelines apply:
  - You can only configure one capture for the VLAN; if you configure a capture in multiple contexts on the shared VLAN, then only the last capture that was configured is used.
  - If you remove the last-configured (active) capture, no captures become active, even if you have previously configured a capture in another context; you must remove and readd the capture to make it active.
  - All traffic that enters the interface to which the capture is attached (and that matches the capture access list) is captured, including traffic to other contexts on the shared VLAN.
  - Therefore, if you enable a capture in Context A for a VLAN that is also used by Context B, both Context A and Context B ingress traffic are captured.
- For egress traffic, only the traffic of the context with the active capture is captured. The only exception is when you do not enable the ICMP inspection (therefore the ICMP traffic does not have a session in the accelerated path). In this case, both ingress and egress ICMP traffic for all contexts on the shared VLAN is captured.
- Configuring a capture typically involves configuring an access list that matches the traffic that needs to be captured. After an access list that matches the traffic pattern is configured, then you need to define a capture and associate this access list to the capture, along with the interface on which the capture needs to be configured. Note that a capture only works if an access list and an interface are associated with a capture for capturing IPv4 traffic. The access list is not required for IPv6 traffic.
- For the ASA CX module traffic, captured packets contain an additional AFBP header that your PCAP viewer might not understand; be sure to use the appropriate plugin to view these packets.
- If there is no ingress interface and therefore no global interface, packets sent on the ASA CX backplane are treated as control packets in the system context. These packets bypass the access list check and are always captured. This behavior applies in both single mode and multiple context mode.

Examples

To capture a packet, enter the following command:

```
hostname# capture captest interface inside
```

```
hostname# capture captest interface outside
```

On a web browser, you can view the content of the **capture** command that was issued, named "captest," at the following location:

```
https://171.69.38.95/admin/capture/captest
```

To download a libpcap file (that web browsers use) to a local machine, enter the following command:

```
https://171.69.38.95/capture/http/pcap
```

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

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

The following example shows how to capture ARP packets:

```
hostname# capture arp ethernet-type arp interface outside
```

The following example inserts five tracer packets into the data stream, where *access-list 101* defines traffic that matches TCP protocol FTP:

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

To view the traced packets and information about packet processing in an easily readable manner, use the **show capture ftptrace** command.

The following example shows how to display captured packets in real-time:

```
hostname# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

The following example shows how to configure an extended access list that matches the IPv4 traffic that needs to be captured:

```
hostname (config)# access-list capture extended permit ip any any
```

The following examples shows how to configure the capture:

```
hostname (config)# capture name access-list acl_name interface interface_name
```

By default, configuring a capture creates a linear capture buffer of size 512 KB. You can optionally configure a circular buffer. By default, only 68 bytes of the packets are captured in the buffer. You can optionally change this value.

The following example creates a capture called "ip-capture" using the capture access list previously configured that is applied to the outside interface:

```
hostname (config)# capture ip-capture access-list capture interface outside
```

The following example shows how to view the capture:

```
hostname (config)# show capture name
```

The following example shows how to end the capture, but retain the buffer:

```
hostname (config)# no capture name access-list acl_name interface interface_name
```

The following example shows how to end the capture and delete the buffer:

```
hostname (config)# no capture name
```

The following example shows how to filter traffic captured on the ASA CX backplane in single mode:

```
hostname# capture x interface asa_dataplane access-list any4
hostname# capture y interface asa_dataplane match ip any any
```

Note Control packets are captured in the single mode even though you have specified the access list.

The following examples show how to filter traffic captured on the ASA CX backplane in multiple context mode:

Usage in user context:

```
hostname (contextA)# capture x interface asa_dataplane access-list any4
hostname (contextA)# capture y interface asa_dataplane match ip any any
```

Usage in system context:

```
hostname# capture z interface asa_dataplane
```

Note In multiple context mode, the **access-list** and **match** options are not available in the system context.

Capture for Clustering

To enable capture on all units in the cluster, you can add the **cluster exec** keywords in front of each of these commands.

The following example shows how to create an LACP capture for the clustering environment:

```
hostname (config)# capture lacp type lacp interface gigabitEthernet0/0
```

The following example shows how to create a capture for control path packets in the clustering link:

```
hostname (config)# cap cp interface cluster match udp any eq 49495 any
hostname (config)# cap cp interface cluster match udp any any eq 49495
```

The following example shows how to create a capture for data path packets in the clustering link:

```
hostname (config)# access-list cc1 extended permit udp any any eq 4193
hostname (config)# access-list cc1 extended permit udp any eq 4193 any
hostname (config)# capture dp interface cluster access-list ccl
```

The following example shows how to capture data path traffic through the cluster:

```
hostname (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
hostname (config)# capture abc interface inside match dup host 1.1.1.1 any
hostname (config)# capture abc interface inside access-list xxx
```

The following example shows how to capture logical update messages for flows that match the real source to the real destination, and capture packets forwarded over CCL that match the real source to the real destination:

```
hostname (config)# access-list dp permit real src real dst
```

The following example shows how to capture a certain type of data plane message, such as icmp echo request/response, that is forwarded from one ASA to another ASA using the **match** keyword or the access list for the message type:

```
hostname (config)# capture capture_name interface cluster access-list match icmp any any
```

The following example shows how to create a capture by using access list 103 on a cluster control link in a clustering environment:

```
hostname (config)# access-list 103 permit ip A B
hostname (config)# capture example1 interface cluster
```

In the previous example, if A and B are IP addresses for the CCL interface, only the packets that are sent between these two units are captured.

If A and B are IP addresses for through-device traffic, then the following is true:

- Forwarded packets are captured as usual, provided the source and destination IP addresses are matched with the access list.
- The data path logic update message is captured provided it is for the flow between A and B or for an access list (for example, access-list 103). The capture matches the five-tuple of the embedded flow.
- Although the source and destination addresses in the UDP packet are CCL addresses, if this packet is to update a flow that is associated with addresses A and B, it is also captured. That is, as long as addresses A and B that are embedded in the packet are matched, it is also captured.

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 [**disk0:** | **disk1:** | **flash:**] [*path*]

Syntax Description

disk0:	Specifies the internal flash memory, followed by a colon.
disk1:	Specifies the removable, external flash memory card, followed by a colon.
flash:	Specifies the internal flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.
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
7.0(1)	This command was introduced.

Examples

The following example shows how to change to the “config” directory:

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

Related Commands

Command	Description
pwd	Displays the current working directory.

cdp-url

To specify the CDP to be included in certificates issued by the local CA, use the **cdp-url** command in ca server configuration mode. To revert to the default CDP, use the **no** form of this command.

[no] cdp-url *url*

Syntax Description

url	Specifies the URL where a validating party obtains revocation status for certificates issued by the local CA. The URL must be less than 500 alphanumeric characters.

Defaults

The default CDP URL is that of the ASA that includes the local CA. The default URL is in the format: http://hostname.domain/+CSCOCA+/asa_ca.crl.

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 server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The CDP is an extension that can be included in issued certificates to specify the location where a validating party can obtain revocation status for the certificate. Only one CDP can be configured at a time.

Note If a CDP URL is specified, it is the responsibility of the administrator to maintain access to the current CRL from that location.

Examples

The following example configures a CDP at 10.10.10.12 for certificates issued by the local CA server:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to ca server configuration mode CLI command set, which allows you to configure and manage a local CA.
crypto ca server crl issue	Forces the issuance of a CRL.
crypto ca server revoke	Marks a certificate issued by a local CA server as revoked in the certificate database and CRL.
crypto ca server unrevoke	Unrevokes a previously revoked certificate issued by a local CA server.
lifetime crl	Specifies the lifetime of the certificate revocation list.

certificate

To add the indicated certificate, use the **certificate** command in crypto ca certificate chain configuration mode. 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 CA 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 an RA key encipherment certificate used in SCEP.
ra-general	Indicates that the certificate is an RA certificate used for digital signing and key encipherment in SCEP messaging.
ra-sign	Indicates that the certificate is an RA 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
7.0(1)	This command was introduced.

Usage Guidelines

When this command is issued, the ASA interprets the data included with it as the certificate in hexadecimal format. A **quit** string indicates the end of the certificate.

A CA 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 RA to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor information, the CA can then issue a certificate.

Examples

The following example adds a CA certificate with the 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 mode.
crypto ca trustpoint	Enters ca trustpoint mode.
show running-config crypto map	Displays all configuration for all the crypto maps.

certificate-group-map

To associate a rule entry from a certificate map with a tunnel group, use the **certificate-group-map** command in webvpn configuration mode. To clear current tunnel-group map associations, use the **no** form of this command.

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

Syntax Description

certificate_map_name	The name of a certificate map.
index	The numeric identifier for a map entry in the certificate map. The index value can be in the range of 1-65535.
tunnel_group_name	The name of the tunnel group chosen if the map entry matches the certificate. The *tunnel-group name* must already exist.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

With the **certificate-group-map** command in effect, if a certificate received from a WebVPN client corresponds to a map entry, the resulting tunnel group is associated with the connection, overriding any tunnel group choice made by the user.

Multiple instances of the **certificate-group-map** command allow multiple mappings.

Examples

The following example shows how to associate rule 6 for a tunnel group named tgl:

```
hostname(config)# webvpn
hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters ca certificate map configuration mode for configuring rules based on the certificate issuer and subject distinguished names (DNs).
tunnel-group-map	Configures the policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

chain

To enable sending a certificate chain, use the **chain** command in tunnel-group ipsec-attributes configuration mode. 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:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	Routed	Transparent	Single	Context	System
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Entering this command includes the root certificate and any subordinate CA certificates in the transmission.

Examples

The following example entered in tunnel-group-ipsec attributes 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-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the current tunnel group configuration.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

change-password

To enable users to change their own account passwords, use the **change-password** command in privileged EXEC mode.

change-password [**/silent**] [**old-password** *old-password* [**new-password** *new-password*]]

Syntax Description

new-password *new-password*	Specifies the new password.
old-password *old-password*	Reauthenticates the user.

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	•	•	—	—	•
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.4(4.1)	This command was introduced.

Usage Guidelines

If users omit the passwords, the ASA prompts them for input. When users enter the **change-password** command, they are asked to save their running configuration. After a user has successfully changed the password, a message appears to remind the user to save configuration changes.

Examples

The following example changes a user account password:

```
hostname# change-password old-password myoldpassword000 new password mynewpassword123
```

Related Commands

Command	Description
show run password-policy	Shows the password policy for the current context.
clear configure password-policy	Resets password policy for the current context to the default value.
clear configure username	Removes a username from a user account.

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
7.0(1)	This command was introduced.

Usage Guidelines

If you log into 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.

channel-group

To assign a physical interface to an EtherChannel, use the **channel-group** command in interface configuration mode. To unassaign the interface, use the **no** form of this command.

channel-group *channel_id* **mode** {**active** | **passive** | **on**} [**vss-id** {**1** | **2**}]

no channel-group *channel_id*

Syntax Description

channel_id	Specifies the EtherChannel to which you want to assign this interface, between 1 and 48.
vss-id {**1** | **2**}	(Optional) With clustering, if you are connecting the ASA to two switches in a VSS or vPC, then configure the **vss-id** keyword to identify to which switch this interface is connected (1 or 2). You must also use the **port-channel span-cluster vss-load-balance** command for the port-channel interface.
mode {**active** | **passive** | **on**}	You can configure each physical interface in an EtherChannel to be: • Active—Sends and receives Link Aggregation Control Protocol (LACP) updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic. • Passive—Receives LACP updates. A passive EtherChannel can only establish connectivity with an active EtherChannel. • On—The EtherChannel is always on, and LACP is not used. An "on" EtherChannel can only establish a connection with another "on" EtherChannel.

Command Default

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
8.4(1)	We introduced this command.
9.0(1)	We added the **vss-id** keyword to support ASA clustering and spanned EtherChannels.

Usage Guidelines

Each channel group can have eight active interfaces. Note that you can assign up to 16 interfaces to a channel group. While only eight interfaces can be active, the remaining interfaces can act as standby links in case of interface failure.

All interfaces in the channel group must be the same type and speed. The first interface added to the channel group determines the correct type and speed.

If the port-channel interface for this channel ID does not yet exist in the configuration, one will be added:

```
interface port-channel channel_id
```

The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices. LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. "On" mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

ASA Clustering

You can include multiple interfaces per ASA in a spanned EtherChannel. Multiple interfaces per ASA are especially useful for connecting to both switches in a VSS or vPC. If you are connecting the ASA to two switches in a VSS or vPC, then you should enable VSS load balancing by using the **vss-load-balance** keyword. This feature ensures that the physical link connections between the ASAs to the VSS (or vPC) pair are balanced. You must configure the **vss-id** keyword in the **channel-group** command for each member interface before enabling load balancing.

Examples

The following example assigns interfaces to channel group 1:

```
hostname(config)# interface GigabitEthernet0/0
hostname(config-if)# channel-group 1 mode active
hostname(config-if)# interface GigabitEthernet0/1
hostname(config-if)# channel-group 1 mode active
hostname(config-if)# interface GigabitEthernet0/2
hostname(config-if)# channel-group 1 mode passive
```

Related Commands

Command	Description
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.

Command	Description
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

character-encoding

To specify the global character encoding in WebVPN portal pages, use the **character-encoding** command in webvpn configuration mode. To remove the value of the character-encoding attribute, use the **no** form of this command.

character-encoding *charset*

no character-encoding *charset*

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper case to lower case in the ASA configuration.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Character encoding, also called “character coding” and “a character set,” is the pairing of raw data (such as 0s and 1s) and characters to represent the data. The language determines the character encoding method to use. Some languages use the same method, while others do not. Usually, the geographic region determines the default encoding method used by the browser, but the user can change this. The browser can also detect the encoding specified on the page, and render the document accordingly. The character-encoding attribute lets the user specify the value of the character-encoding method into the WebVPN portal page to ensure that the browser renders it correctly, regardless of the region in which the user is using the browser, or any changes made to the browser.

The character-encoding attribute is a global setting that, by default, all WebVPN portal pages inherit. However, the user can override the file-encoding attribute for Common Internet File System (CIFS) servers that use character encoding that differs from the value of the character-encoding attribute. Use different file-encoding values for CIFS servers that require different character encodings.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character-encoding attribute. The remote user browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the correct rendering of file names or directory paths, as well as pages, is an issue.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. The user needs to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

The encoding type set on the remote browser determines the character set for WebVPN portal pages when this attribute does not have a value.

Examples

The following example sets the character-encoding attribute to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

Related Commands

Command	Description
debug webvpn cifs	Displays debugging messages about the CIFS server.
file-encoding	Specifies CIFS servers and associated character encoding to override the value of this attribute.
show running-config [all] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.

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

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
7.0(1)	This command was introduced.

Usage Guidelines

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.

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.

check-retransmission

To prevent against TCP retransmission style attacks, use the **check-retransmission** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

check-retransmission

no check-retransmission

Syntax Description

This command has no arguments or keywords.

Defaults

The default 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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. To prevent against TCP retransmission style attacks that arise from end-system interpretation of inconsistent retransmissions, use the **check-retransmission** command in tcp-map configuration mode.

The ASA will make efforts to verify if the data in retransmits are the same as the original. If the data does not match, then the connection is dropped by the ASA. When this feature is enabled, packets on the TCP connection are only allowed in order. For more details, see the **queue-limit** command.

Examples

The following example enables the TCP check-retransmission feature on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

checksum-verification

To enable or disable TCP checksum verification, use the **checksum-verification** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

checksum-verification

no checksum-verification

Syntax Description

This command has no arguments or keywords.

Defaults

Checksum verification 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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **checksum-verification** command in tcp-map configuration mode to enable TCP checksum verification. If the check fails, the packet is dropped.

Examples

The following example enables TCP checksum verification on TCP connections from 10.0.0.0 to 20.0.0.0:

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap

hostname(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

cipc security-mode authenticated

To force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario, use the **cipc security-mode authenticated** command in phone-proxy configuration mode. To turn off this command when CIPC softphones support encryption, use the **no** form of this command.

cipc security-mode authenticated

no cipc security-mode authenticated

Syntax Description

This command has no arguments or keywords.

Defaults

Be default, this command is disabled via the no form of the command.

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

Separating voice and data traffic by using VLANs is a security best practice to hide voice streams from security threats that attempt to penetrate the data VLAN. However, Cisco IP Communicator (CIPC) softphone applications must connect to their respective IP phones, which reside on the voice VLAN. This requirement makes segregating voice and data VLANs an issue because the SIP and SCCP protocols dynamically negotiate the RTP/RTCP ports on a wide range of ports. This dynamic negotiation requires that a range of ports be open between the two VLANs.

Note Earlier versions of CIPC that do not support Authenticated mode are not supported with the Phone Proxy.

To allow CIPC softphones on the data VLAN to connect to their respective IP phones on the voice VLAN without requiring access between the VLANs on a wide range of ports, you can configure the Phone Proxy with the **cipc security-mode authenticated** command.

This command allows the Phone Proxy to look for CIPC configuration files and force CIPC softphones to be in authenticated mode rather than encrypted mode, because current versions of CIPC do not support encrypted mode.

When this command is enabled, the Phone Proxy parses the phones configuration file to determine if the phone is a CIPC softphone and changes the security mode to authenticated. Additionally, CIPC softphones support authenticated mode only while the Phone Proxy, by default, forces all phones to be in encrypted mode.

Examples

The following example shows the use of the **cipc security-mode authenticated** command to force Cisco IP Communicator (CIPC) softphones to operate in authenticated mode when CIPC softphones are deployed in a voice and data VLAN scenario:

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)#cipc security-mode authenticated
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.

clacp system-mac

To manually configure the cLACP system ID on the master unit in an ASA cluster, use the **clacp system-mac** command in cluster group configuration mode. To retsore the default setting, use the **no** form of this command.

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

no clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

Syntax Description

mac_address	Manually sets the system ID in the form *H.H.H*, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0A-00-00-AA-AA is entered as 000A.0000.AAAA.
auto	Auto-generates the system ID.
system-priority *number*	Sets the system priority, between 1 and 65535. The priority is used to decide which unit is in charge of making a bundling decision. By default, the ASA uses priority 1, which is the highest priority. The priority needs to be higher than the priority on the switch.

Command Default

By default, the system-mac is auto-generated (**auto**).

By default, the system-priority is 1.

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
Cluster group configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch. ASAs in a cluster collaborate in cLACP negotiation so that they appear as a single (virtual) device to the switch. One parameter in cLACP negotiation is a system ID, which is in the format of a MAC address. All ASAs use the same system ID: auto-generated by the master unit (the default) and replicated to all slaves; or manually specified in this command. You might want to manually configure the MAC address for troubleshooting purposes, for example, so you can use an easily identified MAC address. Typically, you would use the auto-generated MAC address.

This command is not part of the bootstrap configuration, and is replicated from the master unit to the slave units. However, you cannot change this value after you enable clustering.

Examples

The following example manually configures a system ID:

```
cluster group pod1
   local-unit unit1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   health-check
   clacp system-mac 000a.0000.aaaa
   enable noconfirm
```

Related Commands

Command	Description
cluster group	Configures cluster parameters.

class (global)

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	•	•	—	—	•

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

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

When you create a class, the ASA does not set aside a portion of the resources for each context assigned to the class; rather, the ASA 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 limits 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.
- 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, enter the following commands:

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
hostname(config-class)# limit-resource routes 5000
```

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** or **class-map type management** 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
7.0(1)	This command was introduced.

Usage Guidelines

To use the **class** command, use the Modular Policy Framework. To use a class in a Layer 3/4 policy map, enter the following commands:

1. **class-map**—Identify the traffic on which you want to perform actions.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features*—For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the CLI configuration guide for more details about the commands available for each feature.
3. **service-policy**—Assigns the policy map to an interface or globally.

To use a class in an inspection policy map, enter the following commands:

1. **class-map type inspect**—Identify the traffic on which you want to perform actions.

2. **policy-map type inspect**—Identify the actions associated with each class map.
   a. **class**—Identify the inspection class map on which you want to perform actions.
   b. *commands for application types*—See the CLI configuration guide for commands available for each application type. Actions supported in class configuration mode of an inspection policy map include:
   - Dropping a packet
   - Dropping a connection
   - Resetting a connection
   - Logging
   - Rate-limiting of messages
   - Masking content

   c. **parameters**—Configure parameters that affect the inspection engine. The CLI enters parameters configuration mode. See the CLI configuration guide for available commands.
3. **class-map**—Identify the traffic on which you want to perform actions.
4. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the Layer 3/4 class map on which you want to perform actions.
   b. **inspect** *application inspect_policy_map*—Enables application inspection, and calls an inspection policy map to perform special actions.
5. **service-policy**—Assigns the policy map to an interface or globally.

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. You can optionally use this class map when you want to match all traffic, and do not want to bother creating another class map. In fact, some features are only configurable for the **class-default** class map, such as the **shape** command.

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

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 ASA 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
7.0(1)	This command was introduced.

Usage Guidelines

This type of class map is for Layer 3/4 through traffic only. For management traffic destined to the ASA, see the **class-map type management** command.

A Layer 3/4 class map identifies Layer 3 and 4 traffic to which you want to apply actions. You can create multiple Layer 3/4 class maps for each Layer 3/4 policy map.

Default Class Maps

The configuration includes a default Layer 3/4 class map that the ASA 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 ASA 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. In fact, some features are only available for class-default, such as QoS traffic shaping.

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 management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration 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** or **class-map type management** 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 (with the exception of the **match tunnel-group** and **match default-inspection-traffic** commands) that identifies the traffic included in the class map.

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
class-map type management	Creates a class map for traffic to the ASA.
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** | **match-any]** *class_map_name*

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

Syntax Description

application	Specifies the type of application traffic you want to match. Available types include: • **dns** • **ftp** • **h323** • **http** • **im** • **scansafe** • **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 if you do not specify an option.
match-any	(Optional) Specifies that traffic can match one or more criteria to match the 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
7.2(1)	This command was introduced.
8.0(2)	The **match-any** keyword was added.

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 DNS traffic, you can match the domain name in a DNS query.

A class map groups multiple traffic matches (in a match-all class map), or lets you match any of a list of matches (in a match-any class map). 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 management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration 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
```

The following example creates an HTTP class map that can match any of the criteria:

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

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 management

When using the Modular Policy Framework, identify Layer 3 or 4 management traffic destined for the ASA to which you want to apply actions by using the **class-map type management** command in global configuration mode. To delete a class map, use the **no** form of this command.

class-map type management *class_map_name*

no class-map type management *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
7.2(1)	This command was introduced.
8.0(2)	The s**et connection** command is now available for a Layer 3/4 management class map, for to-the-ASA management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.

Usage Guidelines

This type of class map is for management traffic only. For through traffic, see the **class-map** command (without the **type** keyword).

For management traffic to the ASA, you might want to perform actions specific to this kind of traffic. The types of actions available for a management class map in the policy map are specialized for management traffic. For example, this type of class map lets you inspect RADIUS accounting traffic and set connection limits.

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 of all types is 255 in single mode or per context in multiple mode.

You can create multiple Layer 3/4 class maps (management or through traffic) for each Layer 3/4 policy map.

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** and **class-map type management** 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.

Use the **class-map type management** 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. You can specify a management class map that can match an access list or TCP or UDP ports. A Layer 3/4 class map contains, at most, one **match** command that identifies the traffic included in the class 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 management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration mode

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

Examples

The following example creates a Layer 3/4 management class map:

```
hostname(config)# class-map type management radius_acct
hostname(config-cmap)# match port tcp eq 10000
```

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
7.2(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 management**
- **class-map type inspection**
- **class-map type regex**
- **match** commands in policy-map type inspect configuration 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 url_example
hostname(config-cmap)# match regex url_example2
```

Related Commands

Command	Description
class-map type inspect	Creates an 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 kerberos

To clear all Kerberos ticket information on the ASA, use the **clear aaa kerberos** command in webvpn configuration mode.

[**cluster exec**] **clear aaa kerberos** [**username** *user* | **host** *ip* | *hostname*]

Syntax Description

cluster exec	(Optional) In a clustering environment, enables you to issue the **clear aaa kerberos** command in one unit and run the command in all the other units at the same time.
host	Specifies the specific host that you want to clear from the Kerberos ticket.
hostname	Specifies the hostname.
ip	Specifies the IP address for the host.
username	Specifies the specific user that you want to clear from the Kerberos ticket.

Defaults

No defaults exist for this command.

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 configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.
9.0(1)	The **cluster exec** option was added.

Usage Guidelines

Use the **clear aaa kerberos** command in webvpn configuration mode to clear all the Kerberos tickets cached on the ASA. The **username** and **host** keywords are used to clear the Kerberos tickets of a specific user or host.

Examples

The following example shows the usage of the **clear aaa kerberos** command:

```
hostname(config)# clear aaa kerberos
```

Related Commands

Command	Description
show aaa kerberos	Displays all the Kerberos tickets cached on the ASA.

clear aaa local user fail-attempts

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

[**cluster exec**] **clear aaa local user authentication fail-attempts** {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
cluster exec	(Optional) In a clustering environment, enables you to issue the **clear aaa local user authentication fail-attempts** command in one unit and run the command in all the other units at the same time.
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
7.0(1)	This command was introduced.
9.0(1)	The **cluster exec** option was added.

Usage Guidelines

Use this command if a user fails to authenticate after a few attempts.

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 ASA reboots. In addition, the system resets the counter to zero when the configuration has recently been modified.

Locking or unlocking a username results in a system log 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 the locked-out status of the user.
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.

[**cluster exec**] **clear aaa local user lockout** {**username** *name* | **all**}

Syntax Description

all	Resets the failed-attempts counter to 0 for all users.
cluster exec	(Optional) In a clustering environment, enables you to issue the **clear aaa local user lockout** command in one unit and run the command in all the other units at the same time.
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
7.0(1)	This command was introduced.
9.0(1)	The **cluster exec** option was added.

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 locked-out status of the user.
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
7.0(1)	This command was modified to adhere to CLI guidelines. In the protocol values, **nt** replaces the older **nt-domain**, and **sdi** replaces the older **rsa-ace**.

Examples

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

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

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

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

The following example 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 nondefault 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	Name or number of an access list.

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

When you enter the **clear access-list** command, you must specify the *id* of an access list to clear the counters.

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-list	Displays the access list configuration that is running on the adaptive security appliance.

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
7.0(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 (ASP) 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.

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
7.0(1)	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 asp table

To clear the hit counters in ASP ARP tables, ASP classify tables, or both, use the **clear asp table** command in privileged EXEC mode.

clear asp table [**arp** | **classify**]

Syntax Description

arp	Clears the hits counters in ASP ARP tables only.
classify	Clears the hits counters in ASP classify tables only

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
7.2(4)	This command was introduced.

Usage Guidelines

Only two options, **arp** and **classify**, have hits in the **clear asp table** command.

Examples

The following example clears all ASP table statistics:

```
hostname# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

Related Commands

Command	Description
show asp table arp	Shows the contents of the accelerated security path, which might help you troubleshoot a problem.

clear asp table filter

To clear the hit counters for the ASP filter table entries, use the **clear asp table filter** command in privileged EXEC mode.

clear asp table filter [**access-list** *acl-name*]

Syntax Description

acl-name	Clears the hit counters only for a specified access list.

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
8.2(2)	This command was introduced.

Usage Guidelines

Only the **access-list** option has hits in the **clear asp table filter** command.

Examples

The following example clears all ASP filter table statistics:

```
hostname# clear asp table filter
```

Related Commands

Command	Description
show asp table arp	Shows the contents of the accelerated security path, which might help you troubleshoot a problem.

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
7.0(1)	This command was introduced.

Usage Guidelines

Resets the low watermark counters to the current available blocks in each pool. Addtionally, this command 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-button

To customize the Clear button of the WebVPN page login field that is displayed to WebVPN users when they connect to the ASA, use the **clear-button** command in customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

Syntax Description

style	Specifies you are changing the style.
text	Specifies you are changing the text.
value	The actual text to display or Cascading Style Sheet (CSS) parameters, each with a maximum of 256 characters allowed.

Defaults

The default text is "Clear".

The default style is border:1px solid black;background-color:white;font-weight:bold;font-size:80%.

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**
Customization configuration	•	—	•	—	—

Command History

Release	**Modification**
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example changes the default background color of the Clear button from black to blue:

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# clear-button style background-color:blue
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page Login field.
login-button	Customizes the login button of the WebVPN page Login field.
login-title	Customizes the title of the WebVPN page Login field.
password-prompt	Customizes the password prompt of the WebVPN page Login field.
username-prompt	Customizes the username prompt of the WebVPN page Login field.

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command in privileged EXEC configuration 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
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

This example shows how to clear the capture buffer for the capture buffer “example”:

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

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.

clear cluster info

To clear cluster statistics, use the **clear cluster info** command in privileged EXEC mode.

clear cluster info {trace | transport}

Syntax Description

trace	Clears cluster event trace information.
transport	Clears cluster transport statistics.

Command Default

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
9.0(1)	We introduced this command.

Usage Guidelines

To view cluster statistics, use the **show cluster info** command.

Examples

The following example clears cluster event trace information:

```
hostname# clear cluster info trace
```

Related Commands

Command	Description
show cluster info	Shows cluster statistics.

clear compression

To clear compression statistics for all SVC and WebVPN connections, use the **clear compression** command in privileged EXEC mode.

clear compression {**all** | **svc** | **http-comp**}

Syntax Description

all	Clears all compressions statistics.
http-comp	Clears HTTP-COMP statistics.
svc	Clears SVC compression statistics.

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
7.1(1)	This command was introduced.

Examples

The following example, clears the compression configuration for the user:

```
hostname# clear configure compression
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.
svc compression	Enables compression of data over an SVC connection for a specific group or user.