

q - res

- queue-limit (priority-queue), on page 3
- queue-limit (tcp-map), on page 5
- quick-start, on page 7
- quit, on page 9
- quota management-session, on page 10
- radius-common-pw, on page 12
- radius-reject-message, on page 14
- radius-with-expiry (Deprecated), on page 15
- raid, on page 17
- range, on page 19
- ras-rcf-pinholes, on page 21
- rate-limit, on page 22
- reactivation-mode, on page 24
- record-entry, on page 26
- record-route, on page 28
- redirect-fqdn, on page 30
- redistribute (ipv6 router ospf), on page 32
- redistribute (router eigrp), on page 35
- redistribute (router ospf), on page 37
- redistribute (router rip), on page 40
- redistribute isis, on page 42
- redundant-interface, on page 44
- regex, on page 46
- reload, on page 51
- remote-access threshold session-threshold-exceeded, on page 54
- rename (class-map), on page 55
- rename (privileged EXEC), on page 56
- renewal-reminder, on page 58
- replication http, on page 60
- request-command deny, on page 62
- request-data-size, on page 64
- request-queue, on page 66
- request-timeout (Deprecated), on page 68

- reserved-bits, on page 70
- reserve-port-protect, on page 72
- reset, on page 73
- resolver, on page 75
- responder-only, on page 76
- rest-api (Deprecated), on page 78
- restore, on page 80

queue-limit (priority-queue)

To specify the depth of the priority queues, use the **queue-limit** command in priority-queue configuration mode. To remove this specification, use the **no** form of this command.



Note This command is not supported on ASA 5580 Ten Gigabit Ethernet interfaces. (Ten Gigabit Ethernet interfaces are supported for priority queues on the ASA 5585-X.) This command is also not supported for the ASA 5512-X through ASA 5555-X Management interface.This command is not supported on the ASA Services Module.

queue-limit *number-of-packets*
no queue-limit *number-of-packets*

Syntax Description

number-of-packets	Specifies the maximum number of low-latency or normal priority packets that can be queued (that is, buffered) before the interface begins dropping packets. The upper limit of the range of values is determined dynamically at run time. To view this limit, enter **help** or **?** on the command line. The key determinant is the memory needed to support the queues and the memory available on the device. The queues must not exceed the available memory. The theoretical maximum number of packets is 2147483647.

Command Default

The default queue limit is 1024 packets.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Priority-queue configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA allows two classes of traffic: low-latency queuing (LLQ) for higher priority, latency sensitive traffic (such as voice and video) and best-effort, the default, for all other traffic. The ASA recognizes priority traffic and enforces appropriate quality of service (QoS) policies. You can configure the size and depth of the priority queue to fine-tune the traffic flow.



Note You *must* configure the **priority-queue** command in order to enable priority queueing for the interface.

You can apply one **priority-queue** command to any interface that can be defined by the **nameif** command.

The **priority-queue** command enters priority-queue configuration mode, as shown by the prompt. In priority-queue configuration mode, you can configure the maximum number of packets allowed in the transmit queue at any given time (**tx-ring-limit** command) and the number of packets of either type (priority or best -effort) allowed to be buffered before dropping packets (**queue-limit** command).

The tx-ring-limit and the queue-limit that you specify affect both the higher priority low-latency queue and the best-effort queue. The tx-ring-limit is the number of either type of packets allowed into the driver before the driver pushes back to the queues sitting in front of the interface to let them buffer packets until the congestion clears. In general, you can adjust these two parameters to optimize the flow of low-latency traffic.

Because queues are not of infinite size, they can fill and overflow. When a queue is full, any additional packets cannot get into the queue and are dropped. This is *tail drop* . To avoid having the queue fill up, you can use the **queue-limit** command to increase the queue buffer size.

Examples

The following example configures a priority queue for the interface named test, specifying a queue limit of 234 packets and a transmit queue limit of 3 packets.

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

Related Commands

Command	Description
clear configure priority-queue	Removes the current priority queue configuration on the named interface.
priority-queue	Configures priority queuing on an interface.
show priority-queue statistics	Shows the priority-queue statistics for the named interface.
show running-config [all] priority-queue	Shows the current priority queue configuration. If you specify the **all** keyword, this command displays all the current priority queue, queue-limit, and tx-ring-limit configuration values.
tx-ring-limit	Sets the maximum number of packets that can be queued at any given time in the Ethernet transmit driver.

queue-limit (tcp-map)

To configure the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, use the **queue-limit** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

queue-limit *pkt_num* **timeout** *seconds*
no queue-limit

Syntax Description

pkt_num	Specifies the maximum number of out-of-order packets that can be buffered and put in order for a TCP connection, between 1 and 250. The default is 0, which means this setting is disabled and the default system queue limit is used depending on the type of traffic. See the "Usage Guidelines" section for more information.
timeout *seconds*	(Optional) Sets the maximum amount of time that out-of-order packets can remain in the buffer, between 1 and 20 seconds. The default is 4 seconds. If packets are not put in order and passed on within the timeout period, then they are dropped. You cannot change the timeout for any traffic if the *pkt_num* argument is set to 0; you need to set the limit to be 1 or above for the **timeout** keyword to take effect.

Command Default

The default setting is 0, which means this command is disabled.

The default timeout is 4 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)/8.0(4)	The **timeout** keyword was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1.tcp-map—Identifies the TCP normalization actions.

- **a.queue-limit**—In tcp-map configuration mode, you can enter the **queue-limit** command and many others.

2.class-map—Identify the traffic on which you want to perform TCP normalization.

3.policy-map—Identify the actions associated with each class map.

- **a.class**—Identify the class map on which you want to perform actions.
- **b.set connection advanced-options**—Identify the tcp-map you created.

4.service-policy—Assigns the policy map to an interface or globally.

If you do not enable TCP normalization, or if the **queue-limit** command is set to the default of 0, which means it is disabled, then the default system queue limit is used depending on the type of traffic:

- Connections for application inspection (the **inspect** command), IPS (the **ips** command), and TCP check-retransmission (the TCP map **check-retransmission** command) have a queue limit of 3 packets. If the ASA receives a TCP packet with a different window size, then the queue limit is dynamically changed to match the advertised setting.
- For other TCP connections, out-of-order packets are passed through untouched.

If you set the **queue-limit** command to be 1 or above, then the number of out-of-order packets allowed for all TCP traffic matches this setting. For example, for application inspection, IPS, and TCP check-retransmission traffic, any advertised settings from TCP packets are ignored in favor of the **queue-limit** setting. For other TCP traffic, out-of-order packets are now buffered and put in order instead of passed through untouched.

Examples

The following example sets the queue limit to 8 packets and the buffer timeout to 6 seconds for all Telnet connections:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	Identifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

quick-start

To define an action when the Quick-Start (QS) option occurs in a packet header with IP Options inspection, use the **quick-start** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

quick-start action { **allow** | **clear** }
no quick-start action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Quick-Start IP option.
clear	Remove the Quick-Start option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Quick-Start IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

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

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# quick-start action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

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

quit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **quit** command.

quit

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **quit** command in privileged or user EXEC modes, you log out from the ASA. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **quit** command to exit global configuration mode, and then logout from the session:

```
ciscoasa(config)# quit
ciscoasa# quit
Logoff
```

The following example shows how to use the **quit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
ciscoasa(config)# quit
ciscoasa# disable
ciscoasa>
```

Related Commands

Command	Description
exit	Exits a configuration mode or logs out from privileged or user EXEC modes.

quota management-session

To set the maximum number of aggregate, per user, and per-protocol administrative sessions that are allowed on the ASA, use the **quota management-session** command in global configuration mode. To set the quota to the default value, use the **no** form of this command.

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*
no quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

Syntax Description

number	Specifies the maximum number of simultaneous ASDM, SSH, and Telnet sessions that are allowed. (9.12 and later) When entered without any other keywords, this argument sets the aggregate number of sessions between 1 and 15. The default is 15. (9.10 and earlier) Valid values are from 0 (unlimited) to 10,000.
ssh	Sets the maximum SSH sessions, between 1 and 5. The default is 5.
telnet	Sets the maximum Telnet sessions, between 1 and 5. The default is 5.
http	Sets the maximum HTTPS (ASDM) sessions, between 1 and 5. The default is 5.
user	Sets the maximum sessions per user, between 1 and 5. The default is 5.

Command Default

(9.12 and later) The aggregate default is 15.

The SSH, Telnet, HTTP, and user defaults are 5.

(9.10 and earlier) The default is 0, which means there is no session limit.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.
9.12(1)	You can now enter this command within a context instead of in the system. You can also now set the per user and per-protocol limits, in addition to the aggregate limit. The maximum aggregate sessions is now 15; if you configured 0 (unlimited) or 16+, then when you upgrade, the value is changed to 15.

Usage Guidelines

When the quota is reached, subsequent management session requests are denied, and a syslog message is generated. The console session is never blocked by the management session quota mechanism to prevent device lockout.

Note In multiple context mode, you cannot configure the number of ASDM sessions, where the maximum is fixed at 5 sessions.

Note If you also set a resource limit per context for the maximum administrative sessions (SSH, etc.) using the **limit-resource** command, then the lower value will be used.

Examples

The following example configures the aggregate management session quota to 8, and the individual session limits to various quantities:

```
ciscoasa
(config)#
quota management-session 8
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

Related Commands

Command	Description
show run quota management-session	Displays the current value of the management-session quota.
show quota management-session	Displays statistics for management sessions.

radius-common-pw

To specify a common password to be used for all users who are accessing a RADIUS authorization server through the ASA, use the **radius-common-pw** command in aaa-server host configuration mode. To remove this specification, use the **no** form of this command.

radius-common-pw *string*
no radius-common-pw

Syntax Description

string	A case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server.

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server host	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is valid only for RADIUS authorization servers.

The RADIUS authorization server requires a password and username for each connecting user. The ASA provides the username automatically. You enter the password here. The RADIUS server administrator must configure the RADIUS server to associate this password with each user authorizing to the server via this ASA. Be sure to provide this information to your RADIUS server administrator.

If you do not specify a common user password, each user password is the username. If you are using usernames for common user passwords, as a security precaution, do not use the RADIUS server for authorization anywhere else on your network.

13-125

Note The *string* argument is essentially a space-filler. The RADIUS server expects and requires it, but does not use it. Users do not need to know it.

Examples

The following example configures a RADIUS AAA server group named "svrgrp1" on host "1.2.3.4," sets the timeout interval to 9 seconds, sets the retry interval to 7 seconds, and configures the RADIUS commnon password as "allauthpw."

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)#
radius-common-pw allauthpw
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

Related Commands

Command	Description
aaa-server host	Enters aaa-server host configuration mode, so that you can configure AAA server parameters that are host-specific.
clear configure aaa-server	Removes all AAA command statements from the configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

radius-reject-message

To enable the display of a RADIUS reject message on the login screen when authentication is rejected, use the **radius-eject-message** command from tunnel-group webvpn attributes configuration mode. To remove the command from the configuration, use the **no** form of the command:

radius-reject-message
no radius-reject-message

Command Default

The default is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Enable this command if you want to display to remote users a RADIUS message about an authentication failure.

Examples

The following example enables the display of a RADIUS rejection message for the connection profile named engineering:

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (Deprecated)

Note The last supported release of this command was Version 8.0(1).

To have the ASA use MS-CHAPv2 to negotiate a password update with the user during authentication, use the **radius-with-expiry** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

radius-with-expiry
no radius-with-expiry

Syntax Description

This command has no arguments or keywords.

Command Default

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		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was deprecated. The **password-management** command replaces it. The **no** form of the **radius-with-expiry** command is no longer supported.
8.0(2)	This command was deprecated.

Usage Guidelines

You can apply this attribute only to the IPSec remote-access tunnel-group type. The ASA ignores this command if RADIUS authentication has not been configured.

Examples

The following example entered in config-ipsec configuration mode, configures Radius with Expiry for the remote-access tunnel group named remotegrp:

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# radius-with-expiry
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
password-management	Enables password management. This command, in the tunnel-group general-attributes configuration mode, replaces the **radius-with-expiry** command.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

raid

To manage the SSDs in a RAID, use the **raid** command in privileged EXEC mode.



Note This command is only supported on the Secure Firewall 3100.

raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

Syntax Description

add	Adds an SSD to the RAID. It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up.
psid	If you add an SSD that was previously used on another system, and is still locked, enter the *psid*. The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.
remove	Removes the SSD from the RAID and keeps the data intact.
remove-secure	Removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD.
local-disk {**1** | **2**}	Specifies the SSD, disk1 or disk2.

Command Default

If you have two SSDs, they form a RAID when you boot up.

Command Modes

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

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

Command History

Release	Modification
9.17(1)	This command was introduced for the Secure Firewall 3100.

Usage Guidelines

You can perform the following tasks while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.

- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.



Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Examples

The following example removes disk2 from the RAID and performs a secure erase.

```
ciscoasa# raid remove-secure local-disk 2
```

Related Commands

Command	Description
show raid	Shows the RAID status.
show ssd	Shows the SSD status.

range

To configure a range of addresses for a network object, use the **range** command in object configuration mode. Use the **no** form of this command to remove the object from the configuration.

range *ip_addr_1 ip_addr2*
no range *ip_addr_1 ip_addr2*

Syntax Description

ip_addr_1	Identifies the first IP address in the range, either IPv4 or IPv6.
ip_addr_2	Identifies the last IP address in the range.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was added.
9.0(1)	We added support for IPv6 addresses.

Usage Guidelines

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a range network object:

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully-qualified domain name network object.
host	Specifies a host network object.

Command	Description
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

ras-rcf-pinholes

To enable call setup between H.323 endpoints when the Gatekeeper is inside the network, use the **ras-rcf-pinholes** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

ras-rcf-pinholes enable
no ras-rcf-pinholes enable

Syntax Description

enable	Enables call setup between H.323 endpoints.

Command Default

By default, this option is disabled.

Command Modes

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

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

Command History

Release	Modification
8.0(5)	This command was added.

Usage Guidelines

The ASA includes options to open pinholes for calls based on the RegistrationRequest/RegistrationConfirm (RRQ/RCF) messages. Because these RRQ/RCF messages are sent to and from the Gatekeeper, the calling endpoint's IP address is unknown and the ASA opens a pinhole through source IP address/port 0/0.

Examples

The following example shows how to set up an action in a policy map to open pinholes for these calls:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

Related Commands

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

rate-limit

When using the Modular Policy Framework, limit the rate of messages for packets that match a **match** command or class map by using the **rate-limit** command in match or class configuration mode. This rate limit action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the no form of this command.

rate-limit *rate*
no rate-limit *rate*

Syntax Description

rate	Applies a rate limit to the traffic, 1 - 4294967295. For ESMTP, GTP, RTSP, and SIP, the rate is in packets per second. For SCTP, the rate is in kilobits per second (kbps).

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.5(2)	This command was extended to SCTP inspection, where the rate is in kbps rather than packets per second.

Usage Guidelines

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

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

Examples

The following example limits the invite requests to 100 messages per second:

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(config-pmap-c)# rate-limit 100
```

Related Commands

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

reactivation-mode

To specify the method by which failed servers in a group are reactivated, use the **reactivation-mode** command in aaa-server protocol mode. To remove this specification, use the **no** form of this command.

reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }
no reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }

Syntax Description

deadtime *minutes*	(Optional) Specifies the amount of time in minutes, between 0 and 1440, that elapses between the disabling of the last server in the group and the subsequent re-enabling of all servers. Deadtime applies only if you configure fallback to the local database; authentication is attempted locally until the deadtime elapses. The default is 10 minutes.
depletion	Reactivates failed servers only after all of the servers in the group are inactive.
timed	Reactivates failed servers after 30 seconds of down time.

Command Default

The default reactivation mode is depletion, and the default deadtime value is 10.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Each server group has an attribute that specifies the reactivation policy for its servers.

In **depletion** mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers. When **depletion** mode is in use, you can also specify the **deadtime** parameter. The **deadtime** parameter specifies the amount of time (in minutes) that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. This parameter is meaningful only when the server group is being used in conjunction with the local fallback feature. Additionally, if you also use the group for accounting, where local fallback isn't used, then the deadtime will be canceled. You can avoid this problem by creating a different group (with the same servers) for accounting.

In **timed** mode, failed servers are reactivated after 30 seconds of down time. This is useful when customers use the first server in a server list as the primary server and prefer that it is online whenever possible. This policy breaks down in the case of UDP servers. Since a connection to a UDP server will not fail, even if the

server is not present, UDP servers are put back on line blindly. This could lead to slowed connection times or connection failures if a server list contains multiple servers that are not reachable.

Accounting server groups that have simultaneous accounting enabled are forced to use the **timed** mode. This implies that all servers in a given list are equivalent.

Note This command is ignored for SDI server groups, because SDI server groups contain a single server.

Examples

The following example configures a TACACS+ AAA server named "srvgrp1" to use the depletion reactivation mode, with a deadtime of 15 minutes:

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
ciscoasa
(config-aaa-server)#
exit
ciscoasa
(config)#
```

The following example configures a TACACS+ AAA server named "srvgrp1" to use timed reactivation mode:

```
ciscoasa
(config)# aaa-server svrgrp2 protocol tacacs+
ciscoasa
(config-aaa-server)# reactivation-mode timed
ciscoasa
(config-aaa-server)#
```

Related Commands

accounting-mode	Indicates whether accounting messages are sent to a single server or sent to all servers in the group.
aaa-server protocol	Enters aaa-server group configuration mode so you can configure AAA server parameters that are group-specific and common to all hosts in the group.
max-failed-attempts	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
clear configure aaa-server	Removes all AAA server configuration.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

record-entry

To specify the trustpoints to be used for the creation of the CTL file, use the record-entry command in ctl-file configuration mode. To remove a record entry from a CTL, use the **no** form of this command.

record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]
no record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

Syntax Description

capf	Specifies the role of this trustpoint to be CAPF. Only one CAPF trustpoint can be configured.
cucm	Specifies the role of this trustpoint to be CCM. Multiple CCM trustpoints can be configured.
cucm-tftp	Specifies the role of this trustpoint to be CCM+TFTP. Multiple CCM+TFTP trustpoints can be configured.
domain-name *domain_name*	(Optional) Specifies the domain name of the trustpoint used to create the DNS field for the trustpoint. This is appended to the Common Name field of the Subject DN to create the DNS Name. The domain name should be configured when the FQDN is not configured for the trustpoint.
address *ip_address*	Specifies the IP address of the trustpoint.
tftp	Specifies the role of this trustpoint to be TFTP. Multiple TFTP trustpoints can be configured.
trustpoint *trust_point*	Sets the name of the trustpoint installed.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
CTL-file configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.

Usage Guidelines

Only one domain-name can be specified. If the CTL file does not exist, manually export this certificate from CUCM to the ASA.

Use this command only when you have not configured a CTL file for the Phone Proxy. Do not use this command when you have already configured a CTL file.

The IP address you specify in the *ip_address* argument must be the global address or address as seen by the IP phones because it will be the IP address used for the CTL record for the trustpoint.

Add additional record-entry configurations for each entity that is required in the CTL file.

Examples

The following example shows the use of the **record-entry** command to specify the trustpoints to be used for the creation of the CTL file:

```
ciscoasa(config-ctl-file)# record-entry
 cucm-tftp
 trustpoint cucm1 address 192.168.1.2
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

record-route

To define an action when the Record Route (RR) option occurs in a packet header with IP Options inspection, use the **record-route** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

record-route action { **allow** | **clear** }
no record-route action { **allow** | **clear** }

Syntax Description

allow	Allow packets containing the Record Route IP option.
clear	Remove the Record Route option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection drops packets containing the Record Route IP option.

You can change the default using the **default** command in the IP Options inspection policy map.

Command Modes

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

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

Command History

Release	Modification
9.5(1)	This command was added.

Usage Guidelines

This command can be configured in an IP Options inspection policy map.

You can configure IP Options inspection to control which IP packets with specific IP options are allowed through the ASA. You can allow a packet to pass without change or clear the specified IP options and then allow the packet to pass.

Examples

The following example shows how to set up an action for IP Options inspection in a policy map:

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# record-route action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.

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

redirect-fqdn

To enable or disable redirection using a fully qualified domain name in vpn load-balancing mode, use the **redirect-fqdn enable** command in global configuration mode.

redirect-fqdn { **enable** | **disable** }
no redirect-fqdn { **enable** | **disable** }

Note To use VPN load balancing, you must have an ASA Model 5510 with a Plus license or an ASA Model 5520 or higher. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description

disable	Disables redirection with fully qualified domain names.
enable	Enables redirection with fully qualified domain names.

Command Default

This behavior is disabled by default.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Vpn load-balancing mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

By default, the ASA sends only IP addresses in load-balancing redirection to a client. If certificates are in use that are based on DNS names, the certificates will be invalid when redirected to a secondary device.

As a VPN cluster master, this ASA can send a fully qualified domain name (FQDN), using reverse DNS lookup, of a cluster device (another ASA in the cluster), instead of its outside IP address, when redirecting VPN client connections to that cluster device.

All of the outside and inside network interfaces on the load-balancing devices in a cluster must be on the same IP network.

To do WebVPN load Balancing using FQDNs rather than IP addresses, you must do the following configuration steps:

1. Enable the use of FQDNs for Load Balancing with the **redirect-fqdn enable** command.
2. Add an entry for each of your ASA outside interfaces into your DNS server, if such entries are not already present. Each ASA outside IP address should have a DNS entry associated with it for lookups. These DNS entries must also be enabled for Reverse Lookup.
3. Enable DNS lookups on your ASA with the command - “dns domain-lookup inside” (or whichever interface has a route to your DNS server).
4. Define your DNS server IP address on the ASA; for example: dns name-server 10.2.3.4 (IP address of your DNS server)

Examples

The following is an example of the **redirect-fqdn** command that disables redirection:

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that enables redirection for a fully qualified domain name, specifies the public interface of the cluster as “test” and the private interface of the cluster as “foo”:

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.
vpn load-balancing	Enters vpn load-balancing mode.

redistribute (ipv6 router ospf)

To redistribute IPv6 routes from one OSPFv3 routing domain into OSPFv3 routing domain, use the **redistribute** command in ipv6 router ospf configuration mode. To disable the redistribution, use the **no** form of this command.

redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

Syntax Description

as-number	Specifies the autonomous system number of the routing process. Valid values range from 1 to 65535.
external	Specifies the OSPFv3 metric routes that are external to a specified autonomous system, but are imported into OSPFv3 as type 1 or type 2 external routes. Valid values are 1 or 2.
include-connected	(Optional) Allows the target protocol to redistribute routes that have been learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.
internal	Specifies OSPFv3 metric routes that are internal to a specified autonomous system.
level-1	Specifies that for Intermediate System-to-Intermediate System (IS-IS), the level 1 routes are redistributed into other IP routing protocols independently.
level-1-2	Specifies that for IS-IS, both level 1 and level 2 routes are redistributed into other IP routing protocols independently.
level-2	Specifies that for IS-IS, level 2 routes are redistributed into other IP routing protocols independently.
map-tag	Specifies the identifier of a configured route map.
match	(Optional) Redistributes routes into other routing domains.
metric *metric_value*	(Optional) Specifies the OSPFv3 default metric value, which ranges from 0 to 16777214.
metric-type *metric_type*	(Optional) Specifies the external link type that is associated with the default route advertised into the OSPFv3 routing domain. It can be either of the following two values: 1 for type 1 external routes or 2 for type 2 external routes.
nssa-external	Specifies routes that are external to the autonomous system, but are imported into OSPFv3 in a not so stubby area (NSSA) for IPv6 as type 1 or type 2 external routes.
process-id	(Optional) Specifies the number that is assigned administratively when the OSPFv3 routing process is enabled.

route-map *map_name*	(Optional) Specifies the name of the route map that is used to filter the routes that are imported from the source routing protocol to the current OSPFv3 routing protocol. If specified but no route maps tags are listed, no routes are imported. If not specified, all routes are redistributed.
source-protocol	Specifies the source protocol from which routes are being redistributed. Valid values can be one of the following: connected, ospf, or static.
tag *tag_value*	(Optional) Specifies the 32-bit decimal value that is attached to each external route. This value is not used by OSPFv3 itself, but may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero is used. Valid values range from 0 to 4294967295.
transparent	(Optional) Causes RIP to use the routing table metric for redistributed routes as the RIP metric.

Command Default

The following are the command defaults:

- **metric** *metric-value*: **0**
- **metric-type** *type-value*: **2**
- **match**: **internal**, **external 1**, **external 2**
- **tag** *tag-value*: **0**

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 router ospf configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows how to redistribute static routes into the current OSPFv3 process:

```
ciscoasa(config-if)# ipv6
 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.

Command	Description
show running-config ipv6 router	Displays the commands in the router configuration for OSPFv3.

redistribute (router eigrp)

To redistribute routes from one routing domain into the EIGRP routing process, use the **redistribute** command in router eigrp configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*
no redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*

Syntax Description

bandwidth	EIGRP bandwidth metric in Kilobits per second. Valid values are from 1 to 4294967295.
connected	Specifies redistributing a network connected to an interface into the EIGRP routing process.
delay	EIGRP delay metric, in 10 microsecond units. Valid values are from 0 to 4294967295.
external *type*	Specifies the EIGRP metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies EIGRP metric routes that are internal to a specified autonomous system.
load	EIGRP effective bandwidth (loading) metric. Valid values are from 1 to 255, where 255 indicates 100% loaded.
match	(Optional) Specifies the conditions for redistributing routes from OSPF into EIGRP.
metric	(Optional) Specifies the values for the EIGRP metrics of routes redistributed into the EIGRP routing process. **Note** Not applicable for redistribution of static routes. Use prefix-list or access-list instead.
mtu	The MTU of the path. Valid values are from 1 to 65535.
nssa-external *type*	Specifies the EIGRP metric type for routes that are external to an NSSA; valid values are **1** or **2**.
eigrp *pid*	Used to redistribute an EIGRP routing process into the EIGRP routing process. The *pid* specifies the internally used identification parameter for an EIGRP routing process; valid values are from 1 to 65535.
reliability	EIGRP reliability metric. Valid values are from 0 to 255, where 255 indicates 100% reliability.
rip	Specifies redistributing a network from the RIP routing process into the EIGRP routing process.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the EIGRP routing process. If not specified, all routes are redistributed.

static	Used to redistribute a static route into the EIGRP routing process. **Note** Redistribution of static routes with a route-map matching a metric is not supported.

Command Default

The following are the command defaults:

- **match**: **Internal**, **external 1**, **external 2**

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.20(1)	Redistribute for EIGRP IPv6 route was added.

Usage Guidelines

You must specify the **metric** with the redistribute command if you do not have a **default-metric** command in your EIGRP configuration.

Examples

The following example redistributes static and connected routes into the EIGRP routing process:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redistribute (router ospf)

To redistribute routes from one routing domain into an OSPF routing process, use the **redistribute** command in router ospf configuration mode. To remove the redistribution when no options are included, use the **no** form of this command. The **no** form of the command with an option removes only the configuration for that option.

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

Syntax Description

connected	Specifies redistributing a network connected to an interface into an OSPF routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the OSPF routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214. **Note** Not applicable for redistribution of static routes. Use prefix-list or access-list instead.
metric-type *metric_type*	(Optional) The external link type associated with the default route advertised into the OSPF routing domain. It can be either of the following two values: **1** (Type 1 external route) or **2** (Type 2 external route).
nssa-external *type*	Specifies the OSPF metric type for routes that are external to an NSSA; valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the current OSPF routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
rip	Specifies redistributing a network from the RIP routing process into the current OSPF routing process.

route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the current OSPF routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into an OSPF process. **Note** Redistribution of static routes with a route-map matching a metric is not supported.
subnets	(Optional) For redistributing routes into OSPF, scopes the redistribution for the specified protocol. If not used, only classful routes are redistributed.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Command Default

The following are the command defaults:

- **metric** *metric-value*: 0
- **metric-type** *type-value*: **2**
- **match**: **Internal**, **external 1**, **external 2**
- **tag** *tag-value*: 0

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command was modified to include the **rip** keyword.
8.0(2)	This command was modified to include the **eigrp** keyword.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows how to redistribute static routes into the current OSPF process:

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

Related Commands

Command	Description
redistribute (RIP)	Redistributes routes into the RIP routing process.
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

redistribute (router rip)

To redistribute routes from another routing domain into the RIP routing process, use the **redistribute** command in router rip configuration mode. To remove the redistribution, use the **no** form of this command.

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]

Syntax Description

connected	Specifies redistributing a network connected to an interface into the RIP routing process.
eigrp *as-number*	Used to redistribute EIGRP routes into the RIP routing process. The *as-number* specifies the autonomous system number of the EIGRP routing process. Valid values are from 1 to 65535.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system.
match	(Optional) Specifies the conditions for redistributing routes from OSPF to RIP.
metric {*metric_value* | **transparent**}	(Optional) Specifies the RIP metric value for the route being redistributed. Valid values for *metric_value* are from 0 to 16. Setting the metric to **transparent** causes the current route metric to be used. **Note** Not applicable for redistribution of static routes. Use prefix-list or access-list instead.
nssa-external *type*	Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are **1** or **2**.
ospf *pid*	Used to redistribute an OSPF routing process into the RIP routing process. The *pid* specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
route-map *map_name*	(Optional) Name of the route map used to filter the imported routes from the source routing protocol to the RIP routing process. If not specified, all routes are redistributed.
static	Used to redistribute a static route into an OSPF process. **Note** Redistribution of static routes with a route-map matching a metric is not supported.

Command Default

The following are the command defaults:

- **metric** *metric-value*: 0
- **match**: **Internal**, **external 1**, **external 2**

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	This command was modified to include the **eigrp** keyword.
9.0(1)	Multiple context mode is supported.

Examples

The following example shows how to redistribute static routes into the current RIP process:

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# redistribute static metric 2
```

Related Commands

Command	Description
redistribute (router eigrp)	Redistributes routes from other routing domains into EIGRP.
redistribute (router ospf)	Redistributes routes from other routing domains into OSPF.
router rip	Enables the RIP routing process and enters router configuration mode for that process.
show running-config router	Displays the commands in the global router configuration.

redistribute isis

To redistribute IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1, use the **redistribute isis** command in router isis configuration mode. To disable the redistribution, use the **no** form of this command.

redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]
no redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]

Syntax Description

level-1 | level-2	The level from which and to which you are redistributing IS-IS routes.
into	The keyword that separates the level of routes being redistributed from the level into which you are redistributing routes.
distribute-list *list-number*	(Optional) The number of a distribute list that controls the IS-IS redistribution. You may specify either a distribute list or a route map, but not both.
route-map *map-tag*	(Optional) The name of a route map that controls the IS-IS redistribution. You can specify either a distribute list or a route map, but not both.

Command Default

This command has no default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

In IS-IS, all areas are stub areas, which means that no routing information is leaked from the backbone (Level 2) into areas (Level 1). Level 1-only routers use default routing to the closest Level 1-Level 2 router in their area. This command lets you redistribute Level 2 IP routes into Level 1 areas. This redistribution enables Level 1-only routers to pick the best path for an IP prefix to get out of the area. This is an IP-only feature, CLNS routing is still stub routing.

For more control and stability you can configure a distribute list or route map to control which Level 2 IP routes can be redistributed into Level 1. This allows large IS-IS-IP networks to use area for better scalability.

Note You must specify the **metric-style wide** command for the **redistribute isis** command to work.

Examples

In the following example, access list 100 controls the redistribution of IS-IS from Level 1 into Level 2:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 distribute-list 100
ciscoasa(config-router)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

In the following example, the route map named match-tag controls the redistribution of IS-IS from Level 1 into Level 2 so that only routes tagged with 110 are redistributed:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
ciscoasa(config-router)# route-map match-tag permit 10
ciscoasa(config-router)# match tag 11
```

Related Commands

redundant-interface

To set which member interface of a redundant interface is active, use the **redundant-interface** command in privileged EXEC mode.

redundant-interface redundant *number* **active-member** *physical_interface*

Syntax Description

active-member *physical_interface*	Sets the active member. See the **interface** command for accepted values. Both member interfaces must be the same physical type.
redundant *number*	Specifies the redundant interface ID, such as **redundant1**.

Command Default

By default, the active interface is the first member interface listed in the configuration, if it is available.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

To view which interface is active, enter the following command:

```
ciscoasa# show interface redundant
number
 detail
 | grep Member
```

For example:

```
ciscoasa# show interface redundant1
 detail
 | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

Examples

The following example creates a redundant interface. By default, gigabitethernet 0/0 is active because it is first in the configuration. The redundant-interface command sets gigabitethernet 0/1 as the active interface.

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
```

```
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

Related Commands

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

regex

To create a regular expression to match text, use the **regex** command in global configuration mode. To delete a regular expression, use the **no** form of this command.

regex *name regular_expression*
regex *name* [*regular_expression*]

Syntax Description

name	Specifies the regular expression name, up to 40 characters in length.
regular_expression	Specifies the regular expression up to 100 characters in length. See the "Usage Guidelines" section for a list of metacharacters you can use in the regular expression.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **regex** command can be used for various features that require text matching. For example, you can configure special actions for application inspection using Modular Policy Framework using 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 (see the **class-map type regex** command).

A regular expression matches text strings either literally as an exact string, or by using *metacharacters* so you can match multiple variants of a text string. You can use a regular expression to match the content of certain application traffic; for example, you can match body text inside an HTTP packet.



Note As an optimization, the ASA searches on the deobfuscated URL. Deobfuscation compresses multiple forward slashes (/) into a single slash. For strings that commonly use double slashes, like "http://", be sure to search for "http:/" instead.

Table 18-1 lists the metacharacters that have special meanings.

Table 1: regex Metacharacters

Character	Description	Notes
.	Dot	Matches any single character. For example, **d.g** matches dog, dag, dtg, and any word that contains those characters, such as doggonnit.
(*exp***)**	Subexpression	A subexpression segregates characters from surrounding characters, so that you can use other metacharacters on the subexpression. For example, **d(o|a)g** matches dog and dag, but **do|ag** matches do and ag. A subexpression can also be used with repeat quantifiers to differentiate the characters meant for repetition. For example, **ab(xy){3}z** matches abxyxyxyz.
|	Alternation	Matches either expression it separates. For example, **dog|cat** matches dog or cat.
?	Question mark	A quantifier that indicates that there are 0 or 1 of the previous expression. For example, **lo?se** matches lse or lose. **Note** You must enter **Ctrl+V** and then the question mark or else the help function is invoked.
*	Asterisk	A quantifier that indicates that there are 0, 1 or any number of the previous expression. For example, **lo*se** matches lse, lose, loose, and so on.
+	Plus	A quantifier that indicates that there is at least 1 of the previous expression. For example, **lo+se** matches lose and loose, but not lse.
{*x***}** or **{***x***,}**	Minimum repeat quantifier	Repeat at least *x* times. For example, **ab(xy){2,}z** matches abxyxyz, abxyxyxyz, and so on.
[*abc***]**	Character class	Matches any character in the brackets. For example, **[abc]** matches a, b, or c.
[^*abc***]**	Negated character class	Matches a single character that is not contained within the brackets. For example, **[^abc]** matches any character other than a, b, or c. **[^A-Z]** matches any single character that is not an uppercase letter.
[*a-c***]**	Character range class	Matches any character in the range. **[a-z]** matches any lowercase letter. You can mix characters and ranges: **[abcq-z]** matches a, b, c, q, r, s, t, u, v, w, x, y, z, and so does [**a-cq-z]**. The dash (-) character is literal only if it is the last or the first character within the brackets: **[abc-]** or **[-abc]**.
""	Quotation marks	Preserves trailing or leading spaces in the string. For example, **"test"** preserves the leading space when it looks for a match.
^	Caret	Specifies the beginning of a line.
\	Escape character	When used with a metacharacter, matches a literal character. For example, **\[** matches the left square bracket.

Character	Description	Notes
char	Character	When character is not a metacharacter, matches the literal character.
\r	Carriage return	Matches a carriage return 0x0d.
\n	Newline	Matches a new line 0x0a.
\t	Tab	Matches a tab 0x09.
\f	Formfeed	Matches a form feed 0x0c.
\x*NN*	Escaped hexadecimal number	Matches an ASCII character using hexadecimal (exactly two digits).
\NNN	Escaped octal number	Matches an ASCII character as octal (exactly three digits). For example, the character 040 represents a space.

Usage Guidelines

To test a regular expression to make sure it matches what you think it will match, enter the **test regex** command.

The regular expression performance impact is determined by two main factors:

- The length of text that needs to be searched for a regular expression match.

The regular expression engine has only a small impact to the ASA performance when the search length is small.

- The number of regular expression chained tables that need to be searched for a regular expression match.

How the Search Length Impacts Performance

When you configure a regular expression search, every byte of the searched text is usually examined against a regular expression database to find a match. The longer the searched text is, the longer the search time will be. Below is a performance test case which illustrates this phenomenon.

- An HTTP transaction includes one 300-byte long GET request and one 3250-byte long response.
- 445 regular expressions for URI search and 34 regular expressions for request body search.
- 55 regular expressions for response body search.

When a policy is configured to search the URI and the body in the HTTP GET request only, the throughput is:

- 420 Mbps when the corresponding regular expression database is not searched.
- 413 Mbps when the corresponding regular expression database is searched (this demonstrates a relatively small overhead of using regular expression).

But when a policy is configured to also search the whole HTTP response body, the throughput drops down to 145 Mbps because of the long response body (3250 bytes) search.

Following is a list of factors that will increase the length of text for a regular expression search:

- A regular expression search is configured on multiple, different protocol fields. For example, in HTTP inspection, if only URI is configured for a regular expression match, then only the URI field is searched for a regular expression match, and the search length is then limited to the URI length. But if additional

protocol fields are also configured for a regular expression match, such as Headers, Body, and so on, then the search length will increase to include the header length and body length.

- The field to be searched is long. For example, if the URI is configured for a regular expression search, then a long URI in a GET request will have a long search length. Also, currently the HTTP body search length is limited by default to 200 bytes. If, however, a policy is configured to search the body, and the body search length is changed to 5000 bytes, then there will be severe impact on the performance because of the long body search.

How the Number of Chained Regular Expression Tables Impact Performance

Currently, all regular expressions that are configured for the same protocol field, such as all regular expressions for URI, are built into a database consisting of one or more regular expression chained tables. The number of tables is determined by the total memory required and the availability of memory at the time the tables are built. A regular expression database will be split into multiple tables under any of the following conditions:

- When the total memory required is greater than 32 MB since the maximum table size is limited to 32 MB.
- When the size of the largest contiguous memory is not sufficient to build a complete regular expression database, then smaller but multiple tables will be built to accommodate all the regular expressions. Note that the degree of memory fragmentation varies depending on many factors that are interrelated and are almost impossible to predict the level of fragmentation.

With multiple chained tables, each table must be searched for regular expression matches and hence the search time increases in proportion to the number of tables that are searched.

Certain types of regular expressions tend to increase the table size significantly. It is prudent to design regular expressions in a way to avoid wildcard and repeating factors if possible. See Table 18-1 for a description of the following metacharacters:

- Regular expressions with wildcard type of specifications:
- Dot (.)
- Various character classes that match any character in a class:
- [^a-z]
- [a-z]
- [abc]]
- Regular expressions with repeating type of specifications:
- *
- +
- {n,}
- Combination of the wild-card and repeating types of regular expressions can increase the table size dramatically, for examples:
- 123.*xyz
- 123.+xyz
- [^a-z]+

- [^a-z]*
- .*123.* (This should not be done because this is equivalent to matching "123").

The following examples illustrate how memory consumptions are different for regular expressions with and without wildcards and repetition.

- Database size for the following 4 regular expressions is 958,464 bytes.

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- Database size for the following 4 regular expressions is only 10240 bytes.

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

A large number of regular expressions will increase the total memory that is needed for the regular expression database and hence increases the probabilities of more tables if memory is fragmented. Following are examples of memory consumptions for different numbers of regular expressions:

- 100 sample URIs: 3,079,168 bytes
- 200 sample URIs: 7,156,224 bytes
- 500 sample URIs: 11,198,971 bytes



Note The maximum number of regular expressions per context is 2048.The **debug menu regex 40 10** command can be used to display how many chained tables there are in each regex database.

Examples

The following example creates two regular expressions for use in an inspection policy map:

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
```

Related Commands

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

reload

To reboot and reload the configuration, use the **reload** command in privileged EXEC mode.

reload [**at** *hh* **:** *mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh* **:**] *mm*] [**max-hold-time** [*hh* **:**] *mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

Syntax Description

at *hh*:*mm*	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 hours.
cancel	(Optional) Cancels a scheduled reload.
day	(Optional) Number of the day in the range from 1 to 31.
in [*hh***:**]*mm*]	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must occur within 24 hours.
max-hold-time [*hh***:***mm*	(Optional) Specifies the maximum hold time the ASA waits to notify other subsystems before a shutdown or reboot. After this time elapses, a quick (forced) shutdown/reboot occurs.
month	(Optional) Specifies the name of the month. Enter enough characters to create a unique string for the name of the month. For example, "Ju" is not unique because it could represent June or July, but "Jul" is unique because no other month beginning with those exact three letters.
noconfirm	(Optional) Permits the ASA to reload without user confirmation.
quick	(Optional) Forces a quick reload, without notifying or correctly shutting down all the subsystems.
reason *text*	(Optional) Specifies the reason for the reload, 1 to 255 characters. The reason text is sent to all open IPsec VPN client, terminal, console, Telnet, SSH, and ASDM connections/sessions. **Note** Some applications, like ISAKMP, require additional configuration to send the reason text to IPsec VPN clients. See the VPN CLI Configuration Guide for more information.
save-config	(Optional) Saves the running configuration to memory before shutting down. If you do not enter the **save-config** keyword, any configuration changes that have not been saved will be lost after the reload.
save-show-tech	(Optional) Saves the output of the **show tech** command to a file before the reload occurs.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to add the following new arguments and keywords: *day*, *hh*, *mm*, *month*, **quick**, **save-config**, and *text*.
9.1(3)	The **save-show-tech** keyword was added.

Usage Guidelines

The command lets you reboot the ASA and reload the configuration from flash memory.

By default, the **reload** command is interactive. The ASA first checks whether the configuration has been modified but not saved. If so, the ASA prompts you to save the configuration. In multiple context mode, the ASA prompts for each context with an unsaved configuration. If you specify the **save-config** keyword, the configuration is saved without prompting you. The ASA then prompts you to confirm that you really want to reload the system. Only a response of **y** or pressing the **Enter** key causes a reload. After confirmation, the ASA starts or schedules the reload process, depending on whether you have specified a delay keyword (**in** or **at**).

By default, the reload process operates in "graceful" mode. All registered subsystems are notified when a reboot is about to occur, allowing these subsystems to shut down properly before the reboot. To avoid waiting until for such a shutdown to occur, specify the **max-hold-time** keyword to specify a maximum time to wait. Alternatively, you can use the **quick** keyword to force the reload process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

You can force the **reload** command to operate noninteractively by specifying the **noconfirm** keyword. In this case, the ASA does not check for an unsaved configuration unless you have specified the **save-config** keyword. The ASA does not prompt you for confirmation before rebooting the system. It starts or schedules the reload process immediately, unless you have specified a delay keyword, although you can specify the **max-hold-time** or **quick** keyword to control the behavior or the reload process.

Use the **reload cancel** command to cancel a scheduled reload. You cannot cancel a reload that is already in progress.

Note Configuration changes that are not written to the flash partition are lost after a reload. Before rebooting, enter the **write memory** command to store the current configuration in the flash partition.

Examples

The following example shows how to reboot and reload a configuration:

```
ciscoasa#
reload
```

```
Proceed with ?  [confirm]
 y
Rebooting...
XXX
Bios VX.X
...
```

Related Commands

Command	Description
show reload	Displays the reload status of the ASA.

remote-access threshold session-threshold-exceeded

To set threshold values, use the **remote-access threshold** command in global configuration mode. To remove threshold values, use the **no** version of this command. This command specifies the number of active remote access sessions, at which point the ASA sends traps.

remote-access threshold session-threshold-exceeded *threshold-value*
no **remote-access threshold session-threshold-exceeded**

Syntax Description

threshold-value	Specifies an integer less than or equal to the session limit the ASA supports.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0 (1)	This command was added.

Examples

The following example shows how to set a threshold value of 1500:

```
ciscoasa# remote-access threshold session-threshold-exceeded 1500
```

Related Commands

Command	Description
snmp-server enable trap remote-access	Enables threshold trapping.

rename (class-map)

To rename a class map, enter the **rename** command in class-map configuration mode.

rename *new_name*

Syntax Description

new_name	Specifies the new name of the class map, up to 40 characters in length. The name "class-default" is reserved.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to rename a class map from test to test2:

```
ciscoasa(config)# class-map test
ciscoasa(config-cmap)# rename test2
```

Related Commands

Command	Description
class-map	Creates a class map.

rename (privileged EXEC)

To rename a file or a directory from the source filename to the destination filename, use the **rename** command in privileged EXEC mode.

rename [**/noconfirm**] [**disk0 :** | **disk1 :** | **flash:**] *source-path* [**disk0 :** | **disk1 :** | **flash:**] *destination-path*

Syntax Description

/**noconfirm**	(Optional) Suppresses the confirmation prompt.
destination-path	Specifies the path of the destination file.
disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon.
source-path	Specifies the path of the source file.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **rename flash: flash:** command prompts you to enter a source and destination filename.

You cannot rename a file or directory across file systems.

For example:

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

Examples

The following example shows how to rename a file named “test” to “test1”:

```
ciscoasa# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

Related Commands

Command	Description
mkdir	Creates a new directory.
rmdir	Removes a directory.
show file	Displays information about the file system.

renewal-reminder

To specify the number of days before user certificate expiration that an initial reminder to re-enroll is sent to certificate owners, use the **renewal-reminder** command in ca server configuration mode. To reset the time to the default of 14 days, use the **no** form of this command.

renewal-reminder *days*
no renewal-reminder

Syntax Description

days	Specifies the time in days before the expiration of an issued certificate that the certificate owner is first reminded to re-enroll. Valid values range from 1 to 90 days.

Command Default

The default value is 14 days.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

There are three reminders in all. An e-mail is sent automatically to the certificate owner for each of the three reminders if an e-mail address is specified in the user database. If no e-mail address exists, a syslog message is generated to alert the administrator of the renewal.

By default, the CA server sends the following three e-mail messages in the specified order before certificate expiration:

1. Certification Enrollment Invitation

2. Reminder: Certification Enrollment Invitation

3. Last Reminder: Certification Enrollment Invitation

The first e-mail is the invitation, the second e-mail is a reminder, and the third e-mail is a final reminder. The default setting for this notification is 14 days, which means that the initial invitation goes out 14 days before certificate expiration, the reminder e-mail goes out 7 days before certificate expiration, and the final reminder e-mail goes out 3 days before certificate expiration.

You can customize the renewal-reminder interval using the **renewal-reminder** *days* command.

Examples

The following example specifies that the ASA send an expiration notice to users 7 days before certificate expiration:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# renewal-reminder 7
ciscoasa
(config-ca-server)
#
```

The following example resets the expiration notice time to the default of 14 days before certificate expiration:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no renewal-reminder
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode command set, which allows you to configure and manage the local CA.
lifetime	Specifies the lifetimes of the CA certificate, all issued certificates, and the CRL.
show crypto ca server	Displays the configuration details of the local CA server.

replication http

To enable HTTP connection replication for the failover group, use the **replication http** command in failover group configuration mode. To disable HTTP connection replication, use the **no** form of this command.

replication http
no replication http

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

By default, the ASA does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

This command is available for Active/Active failover only. It provides the same functionality as the **failover replication http** command for Active/Standby failover, except for failover groups in Active/Active failover configurations.

Examples

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

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.

Command	Description
failover replication http	Configures stateful failover to replicate HTTP connections.

request-command deny

To disallow specific commands within FTP requests, use the **request-command deny** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the no form of this command.

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }
no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

Syntax Description

appe	Disallows the command that appends to a file.
cdup	Disallows the command that changes to the parent directory of the current working directory.
dele	Disallows the command that deletes a file on the server.
get	Disallows the client command for retrieving a file from the server.
help	Disallows the command that provides help information.
mkd	Disallows the command that makes a directory on the server.
put	Disallows the client command for sending a file to the server.
rmd	Disallows the command that deletes a directory on the server.
rnfr	Disallows the command that specifies rename-from filename.
rnto	Disallows the command that specifies rename-to filename.
site	Disallows the command that is specific to the server system. Usually used for remote administration.
stou	Disallows the command that stores a file using a unique file name.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is used for controlling the commands allowed within FTP requests traversing the ASA when using strict FTP inspection.

Examples

The following example causes the ASA to drop FTP requests containing **stor**, **stou**, or **appe** commands:

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# request-command deny put stou appe
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ftp-map	Defines an FTP map and enables FTP map configuration mode.
inspect ftp	Applies a specific FTP map to use for application inspection.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.

request-data-size

To set the size of the payload in the SLA operation request packets, use the **request-data-size** command in sla monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

request-data-size *bytes*
no request-data-size

Syntax Description

bytes The size, in bytes, of the request packet payload. Valid values are from 0 to 16384. The minimum value depends upon the protocol used. For echo types, the minimum value is 28 bytes. Do not set this value higher than the maximum allowed by the protocol or the PMTU.

Note
The ASA adds an 8-byte timestamp to the payload, so the actual payload is *bytes* + 8.

Command Default

The default *bytes* is 28.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
sla monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

For reachability, it may be necessary to increase the default data size to detect PMTU changes between the source and the target. Low PMTU will likely affect session performance and, if detected, may indicate that the secondary path be used.

Examples

The following example configures an SLA operation with an ID of 123 that uses an ICMP echo request/response time probe operation. It sets the payload size of the echo request packets to 48 bytes and the number of echo requests sent during an SLA operation to 5.

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
```

```
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
num-packets	Specifies the number of request packets to send during an SLA operation.
sla monitor	Defines an SLA monitoring operation.
type echo	Configures the SLA operation as an echo response time probe operation.

request-queue

To specify the maximum number of GTP requests that will be queued waiting for a response, use the request-queue command in policy map parameters configuration mode. Use the **no** form of this command to return this number to the default of 200.

request-queue *max_requests*
no request-queue *max_requests*

Syntax Description

max_requests	The maximum number of GTP requests that will be queued waiting for a response, from 1 to 4294967295.

Command Default

The default is 200.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **request-queue** command specifies the maximum number of GTP requests that are queued waiting for a response. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

Examples

The following example specifies a maximum request queue size of 300:

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# request-queue 300
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
inspect gtp	Applies a specific GTP map to use for application inspection.

Commands	Description
show service-policy inspect gtp	Displays the GTP configuration.

request-timeout (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To configure the number of seconds before a failed SSO authentication attempt times out, use the **request-timeout** command in webvpn configuration mode.

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

request-timeout *seconds*
no request-timeout

Syntax Description

seconds	The number of seconds before a failed SSO authentication attempt times out. The range is 1 to 30 seconds. Fractions are not supported.

Command Default

The default value for this command is 5 seconds.

Command Modes

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

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

Command History

Release	Modification
7.1.1	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

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

This command applies to both types of SSO Servers.

Once you have configured the ASA to support SSO authentication, you have the option to adjust two timeout parameters:

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

Examples

The following example, entered in webvpn-config-sso-siteminder mode, configures an authentication timeout at ten seconds for the SiteMinder type SSO server, “example”:

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# request-timeout 10
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

reserved-bits

To clear reserved bits in the TCP header, or drop packets with reserved bits set, use the **reserved-bits** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

reserved-bits { **allow** | **clear** | **drop** }
no reserved-bits { **allow** | **clear** | **drop** }

Syntax Description

allow	Allows packet with the reserved bits in the TCP header.
clear	Clears the reserved bits in the TCP header and allows the packet.
drop	Drops the packet with the reserved bits in the TCP header.

Command Default

The reserved bits are allowed by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 **reserved-bits** command in tcp-map configuration mode to remove ambiguity as to how packets with reserved bits are handled by the end host, which may lead to desynchronizing the ASA. You can choose to clear the reserved bits in the TCP header or even drop packets with the reserved bits set.

Examples

The following example shows how to clear packets on all TCP flows with the reserved bit set:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# reserved-bits clear
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
```

```
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
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.

reserve-port-protect

To restrict usage on the reserve port during media negotiation, use the **reserve-port-protect** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

reserve-port-protect
no reserve-port-protect

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:

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

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows how to protect the reserve port in an RTSP inspection policy map:

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

Related Commands

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

reset

When using the Modular Policy Framework, drop packets, close the connection, and send a TCP reset for traffic that matches a **match** command or class map by using the **reset** command in match or class configuration mode. This reset action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the no form of this command.

reset [**log**]
no reset [**log**]

Syntax Description

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

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

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

If you reset a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to reset the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as resetting the connection, can occur. You can configure both the **reset** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is reset for a given match.

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

Examples

The following example resets the connection and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

Related Commands

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

resolver

To configure the addresses of the Cisco Umbrella DNS servers, which resolve DNS requests, use the **resolver** command in Umbrella configuration mode. Use the **no** form of this command to return to the default setting.

resolver { **ipv4** | **ipv6** } *ip_address*
no resolver { **ipv4** | **ipv6** } *ip_address*

Syntax Description

ipv4 *ip_address*	The IPv4 address of the Umbrella DNS server to use.
ipv6 *ip_address*	The IPv6 address of the Umbrella DNS server to use.

Command Default

The default DNS resolvers are 208.67.220.220 and 2620:119:53::53.

Command Modes

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

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

Command History

Release	Modification
9.12(1)	This command was added.

Usage Guidelines

You can configure both IPv4 and IPv6 addresses by entering the command twice. You can specify valid Umbrella DNS servers only.

Examples

The following example defines non-default DNS resolvers for Cisco Umbrella. The servers are 208.67.222.222 and 2620:119:35::35.

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222

ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

Related Commands

Commands	Description
umbrella-global	Configures the Cisco Umbrella global parameters.

responder-only

To configure one end of the VTI tunnel to act only as a responder, use the responder-only command in the IPsec profile configuration mode. Use the no form of this command to remove the responder-only mode.

responder-only
no responder-only

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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

Using this command, one end of the VTI tunnel can be configured to act as a responder only.

The responder-only end will not initiate the tunnel or rekeying.

This option is useful when collision handling is not available, or when both ends of a tunnel try to initiate the tunnel simultaneously in instances when IKEv1 is used. All the rekey configurations for the IKE or IPsec tunnels on the responder-only end would be ignored even if configured.

Examples

The following example adds the responder-only mode to the IPsec profile:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# responder-only
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.

Command	Description
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

rest-api (Deprecated)

Use the **agent** keyword to enable an installed REST API Agent from flash. Use the no form of this command to disable the Agent.

Use the image keyword after downloading a REST API package to this ASA (using the **copy** command) to verify and install the package. The version of the REST API Agent must match the ASA version. To uninstall this package, use the no form of this command.]

rest-api [**agent** | **image disk0 :** / *package*]
no rest-api [**agent** | **image disk0 :** / *package*]

Syntax Description

agent	Enable the installed REST API Agent.
image disk0:/*package*	Install the previously downloaded REST API image, identified by *package* .

Command Default

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Enable/disable REST API Agent	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.
9.17(1)	This command was deprecated.

Usage Guidelines

Issue this command with the **image** keyword to perform compatibility and validation checks on the specified REST API package. If the package passes all checks pass, it will be installed to internal flash.

The REST API configuration is saved in the startup configuration file. Use the **clear configure** command to clear this configuration.

Installing or updating the REST API package will not trigger a reboot of the ASA.

Use this command with the **agent** keyword to enable the installed REST API Agent.

Examples

This example downloads the REST API package from cisco.com, and then installs it:

```
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-9.3.2-32.pkg  disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
```

This example upgrades the existing REST API Agent by disabling the running REST API Agent, and then downloading, installing and starting the new REST API Agent:

```
ciscoasa(config)# no rest-api agent
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-121-lfbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
ciscoasa(config)# rest-api agent
```

Related Commands

Commands	Description
copy	Copy a specified REST API package from a TFTP server to the internal flash memory.
show rest-api agent	Determine if the REST API Agent is running.
clear configure	Clear the running configuration, including the REST API configuration.

restore

To restore an ASA configuration, certificates, keys, and images from a backup file, use the **restore** command in privileged EXEC mode.

restore [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**cert-passphrase** *value*] [**location** *path*]

Syntax Description

cert-passphrase *value*	During the restoration of VPN certificates and preshared keys, a secret key identified by the **cert-passphrase** keyword is required to decode the certificates. You must provide a passphrase to be used for decoding the certificates in PKCS12 format.
context *ctx-name*	In multiple context mode from the system execution space, enter the **context** keyword to restore the specified context. Each backed up context file must be restored individually; that is, re-enter the **restore** command for each.
interface *name*	(Optional) Specifies the interface name through which the backup will be copied. If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table.
location *path*	The restore **location** can be a local disk or a remote URL. If you do not provide a location, the following default names are used: • Single mode—disk0:*hostname* .backup.*timestamp* .tar.gz • Multiple mode—disk0:*hostname* .context-*ctx-name* .backup.*timestamp* .tar.gz
/noconfirm	Specifies not to prompt for the **location** and **cert-passphrase** parameters. Allows you to bypass warning and error messages to continue the backup.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.
9.5(1)	The **interface** *name* argument was added.

Usage Guidelines

See the following guidelines:

- You should have at least 300 MB of disk space available at the restore location before you start a restore.
- If you make any configuration changes during or after a backup, those changes will not be included in the backup. If you change a configuration after making the backup, then perform a restore, this configuration change will be overwritten. As a result, the ASA might behave differently.
- You can start only one restore at a time.
- You can only restore a configuration to the same ASA version as when you performed the original backup. You cannot use the restore tool to migrate a configuration from one ASA version to another. If a configuration migration is required, the ASA automatically upgrades the resident startup configuration when it loads the new ASA OS.
- If you use clustering, you can only restore the startup-configuration, running-configuration, and identity certificates. You must create and restore a backup separately for each unit.
- If you use failover, you must create and restore a backup separately for the active and standby units.
- If you set a master passphrase for the ASA, then you need that master passphrase to restore the backup configuration that you create with this procedure. If you do not know the master passphrase for the ASA, see the CLI configuration guide to learn how to reset it before continuing with the backup.
- If you import PKCS12 data (with the **crypto ca trustpoint** command) and the trustpoint uses RSA keys, the imported key pair is assigned the same name as the trustpoint. Because of this limitation, if you specify a different name for the trustpoint and its key pair after you have restored an ASDM configuration, the startup configuration will be the same as the original configuration, but the running configuration will include a different key pair name. This means that if you use different names for the key pair and trustpoint, you cannot restore the original configuration. To work around this issue, make sure that you use the same name for the trustpoint and its key pair.
- If you do not specify the interface, the ASA checks the management-only routing table; if there are no matches, it then checks the data routing table. Note that if you have a default route through a management-only interface, all **restore** traffic will match that route and never check the data routing table. In this scenario, always specify the interface if you need to restore through a data interface.
- You cannot back up using the CLI and restore using ASDM, or vice versa.
- Each backup file includes the following content:
- Running-configuration
- Startup-configuration
- All security images

Cisco Secure Desktop and Host Scan images

Cisco Secure Desktop and Host Scan settings

AnyConnect (SVC) client images and profiles

AnyConnect (SVC) customizations and transforms

- Identity certificates (includes RSA key pairs tied to identity certificates; excludes standalone keys)
- VPN pre-shared keys
- SSL VPN configurations

- Application Profile Custom Framework (APCF)
- Bookmarks
- Customizations
- Dynamic Access Policy (DAP)
- Plug-ins
- Pre-fill scripts for connection profiles
- Proxy Auto-config
- Translation table
- Web content
- Version information

Examples

The following example shows how to restore a backup:

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
is required to restore running configuration, startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
device, please note them for future reference.
ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the IP
is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the IP
is already used as media-termination address on interface inside.
```

```
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
 configuration file if you want to preserve the old http- and https-proxy configurations.
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
cisco. If the passphrase is not correct, certificates will not be restored.
No passphrase was provided for identity certificates. Using the default value: cisco. If
the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

Related Commands

Command	Description
backup	Backs up an ASA configuration, keys, certificates, and images from a backup file.