ret - rz

retries

To specify the number of times to retry the list of DNS servers when the ASA does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

retries *number*
no retries [*number*]

Syntax Description

number	Specifies the number of retries, from 0 through 10. The default is 2.

Command Default

The default number of retries is 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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Add DNS servers using the **name-server** command.

This command replaces the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The ASA tries each server only once.

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# retries 0
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters the dns server-group mode.
show running-config dns server-group	Shows one or all the existing dns-server-group configurations.

retry-count

To set the value for the number of consecutive polling failures to the Cloud Web Security proxy server before determining the server is unreachable, enter the **retry-count** command in scansafe general-options configuration mode. To restore the default, use the **no** form of this command.

retry-count *value*
no retry-count [*value*]

Syntax Description

value Enters the retry counter value, from 2 to 100. The default is 5.

Command Default

The default value is 5.

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
Scansafe general-options configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server.

If any client is unable to reach the primary server, then the ASA starts polling the tower to determine availability. (If there is no client activity, the ASA polls every 15 minutes.) If the proxy server is unavailable after a configured number of retries (the default is 5; this setting is configurable), the server is declared unreachable, and the backup proxy server becomes active.

If a client or the ASA can reach the server at least twice consecutively before the retry count is reached, the polling stops and the tower is determined to be reachable.

The retry count also applies to application health checking if you enable it.

After a failover to the backup server, the ASA continues to poll the primary server. If the primary server becomes reachable, then the ASA returns to using the primary server.

Examples

The following example configures a retry value of 7:

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
```

```
health-check application
retry-count 7
license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
health-check application	Enables Cloud Web Security application health checking for failover.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the waits before polling the proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

retry-interval

To configure the amount of time between retry attempts for a particular AAA server designated in a previous **aaa-server host** command, use the **retry-interval** command in aaa-server host mode. To reset the retry interval to the default value, use the **no** form of this command.

retry-interval *seconds*
no retry-interval

Syntax Description

seconds	Specify the retry interval (1-10 seconds) for the request. This is the time the ASA waits before retrying a connection request.

Command Default

The default retry interval is 10 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
AAA-server host	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was modified to conform to CLI guidelines.

Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the ASA waits between connection attempts. Use the **timeout** command to specify the length of time during which the ASA attempts to make a connection to a AAA server.

This command does not apply to servers in an RSA SecurID REST API server group.

Note For the RADIUS protocol, if the server responds with an ICMP Port Unreachable message, the retry-interval setting is ignored and the AAA server is immediately moved to the failed state. If this is the only server in the AAA group, it is reactivated and another request is sent to it. This is the intended behavior.

Examples

The following examples show the **retry-interval** command in context.

```
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 7
```

```
ciscoasa
(config-aaa-server-host)# retry-interval 9
```

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
timeout	Specifies the length of time during which the ASA attempts to make a connection to a AAA server.

reval-period

To specify the interval between each successful posture validation in a NAC Framework session, use the **reval-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC Framework policy, use the **no** form of this command.

reval-period *seconds*
no reval-period [*seconds*]

Syntax Description

seconds	Number of seconds between each successful posture validation. The range is 300 to 86400.

Command Default

The default value is 36000.

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
nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.3(0)	"nac-" was removed from the command name. The command was moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.

Usage Guidelines

The ASA starts the revalidation timer after each successful posture validation. The expiration of this timer triggers the next unconditional posture validation. The ASA maintains posture validation during revalidation. The default group policy becomes effective if the Access Control Server is unavailable during posture validation or revalidation.

Examples

The following example changes the revalidation timer to 86400 seconds:

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes the revalidation timer from the NAC policy:

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

Command	Description

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
debug nac	Enables logging of NAC Framework events.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.

revert webvpn all

To remove all web-related data (customization, plug-in, translation table, URL list, and web content) from the ASA flash memory, enter the **revert webvpn all** command in privileged EXEC mode.

revert webvpn all

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn all** command to disable and remove all web-related information (customization, plug-in, translation table, URL list, and web content) from the flash memory of the ASA. Removal of all web-related data returns default settings when applicable.

Examples

The following command removes all of the web-related configuration data from the ASA:

```
ciscoasa# revert webvpn all
ciscoasa
```

Related Commands

Command	Description
show import webvpn (option)	Displays various imported WebVPN data and plug-ins. currently present in flash memory on the ASA.

revert webvpn AnyConnect-customization

To remove a file from the ASA that *customizes the Secure client GUI*, use the **revert webvpn AnyConnect-customization** command in privileged EXEC mode.

revert webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

Syntax Description

type	The type of customizing file: • binary—An executable that replaces the AnyConnect GUI. • resource—A resource file, such as the corporate logo. • transform—A transform that customizes the MSI.
platform	The OS of the endpoint device running the Secure Client. Specify one of the following: linux, mac-intel, mac-powerpc, win, or win-mobile.
name	The name that identifies the file to remove (maximum 64 characters).

Command Default

There is no default behavior for this command.

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	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

For detailed procedures for customizing the Secure Client GUI, see the AnyConnect VPN Client Administrator Guide.

Examples

The following example removes the Cisco logo that was previously imported as a resource file to customize the AnyConnect GUI:

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

Related Commands

Command	Description
customization	Specifies the customization object to use for a tunnel-group, group, or user.

Command	Description
export customization	Exports a customization object.
import customization	Installs a customization object.
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn customization	Displays the current customization objects present on the flash device of the ASA.

revert webvpn customization

To remove a customization object from the ASA cache memory, enter the **revert webvpn customization** command in privileged EXEC mode.

revert webvpn customization *name*

Syntax Description

name	Specifies the name of the customization object to be deleted.

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn customization** command to remove Clientless SSL VPN support for the specified customization and to remove it from the cache memory on the ASA. Removal of a customization object returns default settings when applicable. A customization object contains the configuration parameters for a specific, named portal page.

Version 8.0 software extends the functionality for configuring customization, and the new process is incompatible with previous versions. During the upgrade to 8.0 software, the security appliance preserves a current configuration by using old settings to generate new customization objects. This process occurs only once, and is more than a simple transformation from the old format to the new one because the old values are only a partial subset of the new ones.

Note Version 7.2 portal customizations and URL lists work in the Beta 8.0 configuration only if clientless SSL VPN (WebVPN) is enabled on the appropriate interface in the Version 7.2(x) configuration file before you upgrade to Version 8.0.

Examples

The following command removes the customization object named GroupB:

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

Related Commands

Command	Description
customization	Specifies the customization object to use for a tunnel-group, group, or user.
export customization	Exports a customization object.
import customization	Installs a customization object.
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn customization	Displays the current customization objects present on the flash device of the ASA.

revert webvpn plug-in protocol

To remove a plug-in from the flash device of the ASA, enter the **revert webvpn plug-in protocol** command in privileged EXEC mode.

revert plug-in protocol *protocol*

Syntax Description

protocol Enter one of the following strings:

- rdp

The Remote Desktop Protocol plug-in lets the remote user connect to a computer running Microsoft Terminal Services.

- **ssh**

The Secure Shell plug-in lets the remote user establish a secure channel to a remote computer, or lets the remote user use Telnet to connect to a remote computer.

- **vnc**

The Virtual Network Computing plug-in lets the remote user use a monitor, keyboard, and mouse to view and control a computer with remote desktop sharing turned on.

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn plug-in protocol** command to disable and remove Clientless SSL VPN support for the specified Java-based client application, as well as to remove it from the flash drive of the ASA.

Examples

The following command removes support for RDP:

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

Related Commands

Command	Description
import webvpn plug-in protocol	Copies the specified plug-in from a URL to the flash device of the ASA. Clientless SSL VPN automatically supports the use of the Java-based client application for future sessions when you issue this command.
show import webvpn plug-in	Lists the plug-ins present on the flash device of the ASA.

revert webvpn translation-table

To remove a translation table from the ASA flash memory, enter the **revert webvpn translation-table** command in privileged EXEC mode.

revert webvpn translation-table *translationdomain* **language** *language*

Syntax Description

translationdomain	Available translation domains: • **AnyConnect** • **PortForwarder** • **banners** • **csd** • **customization** • **url-list** • **webvpn** • If available, translations of messages from Citrix, RPC, Telnet-SSH, and VNC plug-ins.)
language *language*	Specifies the language to be deleted. Specify the language using the 2-character code. Enter ? to see which languages are installed. Use the **show import webvpn translation-table** command to see which languages in each domain have been 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
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn translation-table** command to disable and remove an imported translation table and to remove it from the flash memory. Removal of a translation table returns default settings when applicable.

Examples

The following command removes the AnyConnect translation table for French:

```
ciscoasa# revert webvpn translation-table anyconnect language fr

ciscoasa#
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL-list, and web content) .
show import webvpn translation-table	Displays the current translation tables currently present on the flash device.

revert webvpn url-list

To remove a URL list from the ASA, enter the **revert webvpn url-list** command in privileged EXEC mode.

revert webvpn url-list template *name*

Syntax Description

template *name*	Specifies the name of a URL list.

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn url-list** command to disable and remove a current URL list from the flash drive of the ASA. Removal of a url-list returns default settings when applicable.

The template argument used with the **revert webvpn url-list** command specifies the name of a previously configured list of URLs. To configure such a list, use the **url-list** command in global configuration mode.

Examples

The following command removes the URL list, servers2:

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show running-configuration url-list	Displays the current set of configured URL list commands.
url-list (WebVPN mode)	Applies a list of WebVPN servers and URLs to a particular user or group policy.

revert webvpn webcontent

To remove a specified web object from a location in the ASA flash memory, enter the **revert webvpn webcontent** command in privileged EXEC mode.

revert webvpn webcontent *filename*

Syntax Description

filename	Specifies the name of the flash memory file with the web content to be deleted.

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 mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the **revert webvpn content** command to disable and remove a file containing the web content and to remove it from the flash memory of the ASA. Removal of web content returns default settings when applicable.

Examples

The following command removes the web content file, ABCLogo, from the ASA flash memory:

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

Related Commands

Command	Description
revert webvpn all	Removes all webvpn-related data (customization, plug-in, translation table, URL list, and web content).
show webvpn webcontent	Displays the web content currently present in flash memory on the ASA.

revocation-check

To define whether revocation checking is needed for the trustpool policy, use the **revocation-check** command in crypto ca trustpool configuration mode. To restore the default revocation checking method, which is *none*, use the **no** form of this command.

revocation-check { [**crl**] [**ocsp**] [**none**] }
no revocation-check { [**crl**] [**ocsp**] [**none**] }

Syntax Description

crl	Specifies that the ASA should use CRL as the revocation checking method.
none	Specifies that the ASA should interpret the certificate status as valid, even if all methods return an error.
ocsp	Specifies that the ASA should use OCSP as the revocation checking method.

Command Default

The default value is *none*.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpool configuration mode	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(1)	Interface keyword to revocation checking using OCSP URL was added.
9.13(1)	The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.
9.15(1)	The option to bypass revocation checking, which was removed in 9.13(1), was restored.

Usage Guidelines

The signer of the OCSP response is usually the OCSP server (responder) certificate. After receiving the response, devices try to verify the responder certificate.

Normally a CA sets the lifetime of its OCSP responder certificate to a relatively short period to minimize the chance of compromising its security. The CA includes an ocsp-no-check extension in the responder certificate that indicates it does not need revocation status checking. But if this extension is not present, the device tries to check the certificate revocation status using the revocation methods you configure for the trustpoint with this **revocation-check** command. The OCSP responder certificate must be verifiable if it does not have an

ocsp-no-check extension since the OCSP revocation check fails unless you also set the *none* option to ignore the status check.

Note With any permutation of the optional arguments, *none* must be the last keyword used.

The ASA tries the methods in the order in which you configure them, trying the second and third methods only if the previous method returns an error (for example, server down), instead of finding the status as revoked.

You can set a revocation checking method in the client certificate validating trustpoint and also configure no revocation checking (**revocation-check none)** in the responder certificate validating trustpoint. See the **match certificate** command for a configuration example.

If you have configured the ASA with the **revocation-check crl none** command, when a client connects to the ASA, it automatically starts downloading the CRL because it has not been cached, then validates the certificate, and finishes downloading the CRL. In this case, if the CRL is not cached, the ASA validates the certificate before downloading the CRL.

The following options for bypassing revocation checking, which was removed in ASA 9.13(1), was later restored:

Option	Action
revocation-check crl none	If CRLs cannot be accessed, bypass revocation checking
revocation-check ocsp none	If OCSP checking cannot be performed, bypass revocation checking
revocation-check crl ocsp none	If CRLs cannot be accessed, try OCSP. If OCSP cannot be performed, bypass revocation checking
revocation-check ocsp crl none	If OCSP cannot be performed, try CRLs, else, bypass revocation checking

When you are assigning OCSP URL for revocation checking, you can specify the management interface from where the OCSP is reachable. This interface value determines the routing decision.

Examples

```
ciscoasa(config-ca-trustpoint)# revocation-chec
k ?
crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)# ocsp
ocsp interface mgmt url http://1.1.1.1:8888
```

Here, mgmt is the name of the management interface

Related Commands

Command	Description
crypto ca trustpool policy	Enters a submode that provides the commands that define the trustpool policy.
match certificate allow expired-certificate	Allows the administrator to exempt certain certificates from expiration checking.

Command	Description
match certificate skip revocation-check	Allows the administrator to exempt certain certificates from revocation checking.

rewrite(Deprecated)

To disable content rewriting a particular application or type of traffic over a WebVPN connection, use the **rewrite** command in webvpn mode. To eliminate a rewrite rule, use the **no** form of this command with the rule number, which uniquely identifies the rule. To eliminate all rewriting rules, use the **no** form of the command without the rule number.

By default, the ASA rewrites, or transforms, all WebVPN traffic.

rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]
no rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]

Syntax Description

disable	Defines this rewrite rule as a rule that disables content rewriting for the specified traffic. When you disable content rewriting, traffic does not go through the security appliance.
enable	Defines this rewrite rule as a rule that enables content rewriting for the specified traffic.
integer	Sets the order of the rule among all of the configured rules. The range is 1-65534.
name	(Optional) Identifies the name of the application or resource to which the rule applies.
order	Defines the order in which the ASA applies the rule.
resource-mask	Identifies the application or resource for the rule.
resource name	(Optional) Specifies the application or resource to which the rule applies. Maximum 128 bytes.
string	Specifies the name of the application or resource to match that can contain a regular expression. You can use the following wildcards: Specifies a pattern to match that can contain a regular expression. You can use the following wildcards: * — Matches everything. You cannot use this wildcard by itself. It must accompany an alphanumeric string. ? —Matches any single character. [!seq] — Matches any character not in sequence. [seq] — Matches any character in sequence. Maximum 300 bytes.

Command Default

The default is to rewrite everything.

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.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The ASA performs content rewriting for applications to insure that they render correctly over WebVPN connections. Some applications do not require this processing, such as external public websites. For these applications, you might choose to turn off content rewriting.

You can turn off content rewriting selectively by using the rewrite command with the disable option to let users browse specific sites directly without going through the ASA. This is similar to split-tunneling in IPsec VPN connections.

You can use this command multiple times. The order in which you configure entries is important because the ASA searches rewrite rules by order number and applies the first rule that matches.

Examples

The following example shows how to configure a rewrite rule, order number of 1, that turns off content rewriting for URLS from cisco.com domains:

```
ciscoasa
(config-webpn)#
 rewrite order 2 disable resource-mask *cisco.com/*
```

Related Commands

Command	Description
apcf	Specifies nonstandard rules to use for a particular application.
proxy-bypass	Configures minimal content rewriting for a particular application.

re-xauth

To require that IPsec users reauthenticate on IKE rekey, issue the **re-xauth enable** command in group-policy configuration mode. To disable user reauthentication on IKE rekey, use the **re-xauth disable** command.

To remove the re-xauth attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for reauthentication on IKE rekey from another group policy.

re-xauth { **enable** [**extended**] | **disable** }
no re-xauth

Syntax Description

disable	Disables reauthentication on IKE rekey
enable	Enables reauthentication on IKE rekey
extended	Extends the time allowed for reentering authentication credentials until the maximum lifetime of the configured SA.

Command Default

Reauthentication on IKE rekey 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
Group policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0.4	The **extended** keyword was added.

Usage Guidelines

Reauthentication on IKE rekey applies only to IPsec connections.

If you enable reauthentication on IKE rekey, the ASA prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

The user has 30 seconds to enter credentials, and up to three attempts before the SA expires at approximately two minutes and the tunnel terminates. Use the **extended** keyword to allow users to reenter authentication credentials until the maximum lifetime of the configured SA.

To check the configured rekey interval, in monitoring mode, issue the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data.

Note The reauthentication fails if there is no user at the other end of the connection.

Examples

The following example shows how to enable reauthentication on rekey for the group policy named FirstGroup:

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip authentication mode

To specify the type of authentication used in RIP Version 2 packets, use the **rip authentication mode** command in interface configuration mode. To restore the default authentication method, use the **no** form of this command.

rip authentication mode { **text** | **md5** }
no rip authentication mode

Syntax Description

md5	Uses MD5 for RIP message authentication.
text	Uses clear text for RIP message authentication (not recommended).

Command Default

Clear text authentication is used 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
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

Related Commands

Command	Description
rip authentication key	Enables RIP Version 2 authentication and specifies the authentication key.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.

Command	Description
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip authentication key

To enable authentication of RIP Version 2 packets and specify the authentication key, use the **rip authentication key** command in interface configuration mode. To disable RIP Version 2 authentication, use the **no** form of this command.

rip authentication key [**0**|**8**] *string* **key_id** *id*
no rip authentication key

Syntax Description

0	Specifies an unencrypted password will follow.
8	Specifies an encrypted password will follow.
id	Specifies the key identification value; valid values range from 1 to 255.
key	Specifies the shared key to be used for the authentication key string. The key can contain up to 16 characters.
string	Specifies the unencrypted (cleartext) user password.

Command Default

RIP authentication 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
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates. When you enable neighbor authentication, you must ensure that the *key* and *key_id* arguments are the same as those used by neighbor devices that provide RIP version 2 updates. The key is a text string of up to 16 characters.

Use the **show interface** command to view the **rip authentication** commands on an interface.

Examples

The following examples shows RIP authentication configured on interface GigabitEthernet 0/3:

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

Related Commands

Command	Description
rip authentication mode	Specifies the type of authentication used in RIP Version 2 packets.
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
show running-config interface	Displays the configuration commands for the specified interface.
version	Specifies the version of RIP used globally by the ASA.

rip receive version

To specify the version of RIP accepted on an interface, use the **rip receive version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

version { [**1**] [**2**] }
no version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Command Default

The ASA accepts Version 1 and Version 2 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
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can override the global setting on a per-interface basis by entering the **rip receive version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to receive RIP Versions 1 and 2 packets the specified interface:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip send version	Specifies the RIP version to use when sending update out of a specific interface.
router rip	Enables the RIP routing process and enters router configuration mode for that process.

Command	Description
version	Specifies the version of RIP used globally by the ASA.

rip send version

To specify the RIP version used to send RIP updates on an interface, use the **rip send version** command in interface configuration mode. To restore the defaults, use the **no** form of this command.

rip send version { [**1**] [**2**] }
no rip send version

Syntax Description

1	Specifies RIP Version 1.
2	Specifies RIP Version 2.

Command Default

The ASA sends RIP Version 1 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
Interface configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You can override the global RIP send version setting on a per-interface basis by entering the **rip send version** command on an interface.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates.

Examples

The following example configures the ASA to send and receive RIP Versions 1 and 2 packets on the specified interface:

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

Related Commands

Command	Description
rip receive version	Specifies the RIP version to accept when receiving updates on a specific interface.
router rip	Enables the RIP routing process and enter router configuration mode for that process.

Command	Description
version	Specifies the version of RIP used globally by the ASA.

rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

rmdir [/ **no confirm**] [**disk0:| disk1:| flash:**] *path*

Syntax Description

/noconfirm	(Optional) Suppresses the confirmation prompt.
disk0*:*	(Optional) Specifies the nonremovable internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the removable external Flash memory card, followed by a colon.
flash:	(Optional) Specifies the nonremovable internal flash, followed by a colon. In the ASA 5500 series adaptive security appliances, the **flash** keyword is aliased to **disk0**.
path	(Optional) The absolute or relative path of the directory to remove.

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

If the directory is not empty, the **rmdir** command fails.

Examples

The following example shows how to remove an existing directory named “test”:

```
ciscoasa# rmdir test
```

Related Commands

Command	Description
dir	Displays the directory contents.
mkdir	Creates a new directory.
pwd	Displays the current working directory.
show file	Displays information about the file system.

route

To enter a static or default route for the specified interface, use the **route** command in global configuration mode. To remove routes from the specified interface, use the **no** form of this command.

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]
no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] **tunneled**]

Syntax Description

gateway_ip	Specifies the IP address of the gateway router (the next-hop address for this route). **Note** The *gateway_ip* argument is optional in transparent mode.
interface_name	Specifies the interface name through which the traffic is routed. For transparent mode, specify a bridge group member interface name. For routed mode with bridge groups, specify the BVI name. In routed mode, to "black hole" unwanted traffic, enter the **null0** interface.
ip_address	Specifies the internal or external network IP address.
metric	(Optional) Specifies the administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
netmask	Specifies a network mask to apply to *ip_address*.
track*number*	(Optional) Associates a tracking entry with this route. Valid values are from 1 to 500. **Note** The **track** option is only available in single, routed mode.
tunneled	Specifies the route as the default tunnel gateway for VPN traffic. **Note** The tunneled static route is also included in the **show route management-only** output, though the interface is non-management only.

Command Default

The *metric* default is 1.

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
7.0(1)	This command was added.
7.2(1)	The **track** *number* value was added.
9.2(1)	The **null0** interface option was added.

Release	Modification
9.7(1)	Support was added for BVI interfaces in routed mode when using Integrated Routing and Bridging.

Usage Guidelines

Use the **route** command to enter a default or static route for an interface. To enter a default route, set *ip_address* and *netmask* to **0.0.0.0,** or use the shortened form of **0**. All routes that are entered using the **route** command are stored in the configuration when it is saved.

You can define a separate default route for tunneled traffic along with the standard default route. When you create a default route with the **tunneled** option, all traffic from a tunnel terminating on the ASA that cannot be routed using learned or static routes, is sent to this route. For traffic emerging from a tunnel, this route overrides over any other configured or learned default routes.

The following restrictions apply to default routes with the **tunneled** option:

- Do not enable unicast RPF (**ip verify reverse-path**) on the egress interface of a tunneled route. Enabling uRPF on the egress interface of a tunneled route causes the session to fail.
- Do not enable TCP intercept on the egress interface of the tunneled route, because the session will fail.
- Do not use the VoIP inspection engines (CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), the DNS inspect engine, or the DCE RPC inspection engine with vlan mapping options or tunneled routes. These inspection engines ignore the vlan-mapping setting which could result in packets being incorrectly routed.

You cannot define more than one default route with the **tunneled** option; ECMP for tunneled traffic is not supported.

Create static routes to access networks that are connected outside a router on any interface. For example, the ASA sends all packets that are destined to the 192.168.42.0 network through the 192.168.1.5 router with the following static route command.

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

After you enter the IP address for each interface, the ASA creates a CONNECT route in the route table. This entry is not deleted when you use the **clear route** or **clear configure route** commands.

Unlike with ACLs, static **null0** routes do not cause any performance degradation. The **null0** configuration is used to prevent routing loops. BGP leverages the **null0** configuration for Remotely Triggered Black Hole routing.

Examples

The following example shows how to specify one default route command for an outside interface:

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

The following example shows how to add these static route commands to provide access to the networks:

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

The following example uses an SLA operation to install a default route to the 10.1.1.1 gateway on the outside interface. The SLA operation monitors the availability of that gateway. If the SLA operation fails, then the backup route on the DMZ interface is used.

```
ciscoasa(config)# sla monitor 123
```

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

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

The following example shows how to configure a static null0 route:

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

Related Commands

Command	Description
clear configure route	Removes statically configured **route** commands.
clear route	Removes routes learned through dynamic routing protocols such as RIP.
show route	Displays route information.
show running-config route	Displays configured routes.

route-map

To define the conditions for redistributing routes from one routing protocol into another, or to enable policy routing, use the route-map command in global configuration mode and the match and set command in route-map configuration modes. To delete an entry, use the no form of this command.

route-map *name* [**permit | deny**] [*sequence number*]
no route-map *name* [**permit | deny**] [*sequence number*]

Syntax Description

name	Defines a meaningful name for the route map. The redistribute router configuration command uses this name to reference this route map. Multiple route maps may share the same name.
permit	If the match criteria are met for this route map, and the permit keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed. If the match criteria are not met, and the permit keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set. The permit keyword is the default.
deny	If the match criteria are met for the route map and the deny keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.
sequence-number	Number that indicates the position a new route map will have in the list of route maps already configured with the same name. If given with the no form of this command, the position of the route map should be deleted.

Command Default

By default, the route-map is configured with permit and sequence number 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
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.21(1)	This command was enhanced to display warning messeges on incomplete command.

Usage Guidelines

Use route maps to redistribute routes

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

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

Use route maps when you want detailed control over how routes are redistributed between routing processes. The destination routing protocol is the one you specify with the router global configuration command. The source routing protocol is the one you specify with the redistribute router configuration command. See the "Examples" section for an illustration of how route maps are configured.

When you are passing routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a route-map command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route map section with an explicit match specified.

The sequence-number argument works as follows:

1. If no entry is defined with the route-map name, an entry is created with the sequence-number argument set to 10.

2. If only one entry is defined with the route-map name, that entry becomes the default entry for the following route-map command. The sequence-number argument of this entry is unchanged.

3. If more than one entry is defined with the route-map name, an error message is printed to indicate that the sequence-number argument is required.

4. If the no route-map name command is specified (with no sequence-number argument), the whole route map is deleted.

Examples

The following example shows how to redistribute routes with a hop count equal to 1 into OSPF. The ASA redistributes these routes as external LSAs with a metric of 5 and a metric type of Type 1:

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

The following example shows how to redistribute the 10.1.1.0 static route into eigrp process 1 with the configured metric value:

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

The following example shows the default-behavior when the action and sequence number are not specified:

```
ciscoasa(config)#route-map test ?
 <0-65535>     Sequence to insert to/delete from existing route-map entry
 deny          Route map denies set operations
 ordering-seq  Named ordering sequence
 permit        Route map permits set operations

ciscoasa(config)#route-map test
%Warning:Incomplete command: Operation Missing.The CLI will be deprecated soon
%Warning:lncomplete command: Sequence Number Missing.The CLI will be deprecated soon

ciscoasa#sh run | sec route-map
route-map test permit 10
```

Note When you do not specify the action and the sequence-number, a warning message on incomplete CLI command is displayed, though the route-map is configured with the default values.

Related Commands

Command	Description
redistribute	Redistributes routes from one routing domain into another routing domain.
route	Creates a static or default route for an interface.
router	Enters the router configuration mode for a specified protocol.

route priority high

To assign a high priority to an IS-IS IP prefix, use the **route priority high** command in router isis configuration mode. To remove the IP prefix priority, use the **no** form of this command

route priority high *tag-value*
no route priority high *tag-value*

Syntax Description

tag-value Assigns a high priority to IS-IS IP prefixes with a specific route tag. The range is 1 to 4294967295.

Command Default

No IP prefix priority is set.

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 configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

When you use the **route priority high** command to tag higher priority IS-IS IP prefixes for faster processing and installation in the global routing table, you can achieve faster convergence. For example, you can help Voice over IP (VoIP) gateway addresses get processed first to help VoIP traffic get updated faster than other types of packets.

Examples

The following example uses the **route priority high** command to assign a tag value of 100 to the IS-IS IP prefix:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# route priority high tag 100
```

Related Commands

router-alert

To define an action when the Router Alert IP option occurs in a packet header with IP Options inspection, use the **router-alert** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

router-alert action { **allow | clear** }
no router-alert action { **allow | clear** }

Syntax Description

allow	Allow packets containing the Router Alert IP option.
clear	Remove the Router Alert option from packet headers and then allow the packets.

Command Default

By default, IP Options inspection allows packets containing the Router Alert 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
8.2(2)	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.

The Router Alert (RTRALT) or IP Option 20 notifies transit routers to inspect the contents of the packet even when the packet is not destined for that router. This inspection is valuable when implementing RSVP and similar protocols require relatively complex processing from the routers along the packets delivery path.

Examples

The following example shows how to set up an action for protocol violation in a policy map:

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

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.

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the router bgp command in global configuration mode. To remove a BGP routing process, use the no form of this command.

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

Syntax Description

autonomous-system-number	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535.

Command Default

No BGP routing process is enabled 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
Global configuration	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octetnumbers in the range from 1 to 65535 as described in RFC 4271, A Border Gateway Protocol 4 (BGP-4).

Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) allocates four-octet autonomous system numbers in the range from 65536 to 4294967295.

RFC 5396, Textual Representation of Autonomous System (AS) Numbers, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

Examples

The following example shows how to configure a BGP process for autonomous system number 100:

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

Related Commands

Command	Description
show route bgp	Displays the routing table.
show bgp summary	Display the status of all Border Gateway Protocol (BGP) connections

router eigrp

To start an EIGRP routing process and configure parameters for that process, use the **router eigrp** command in global configuration mode. To disable EIGRP routing, use the **no** form of this command.

router eigrp *as-number*
no router eigrp *as-number*

Syntax Description

as-number	Autonomous system number that identifies the routes to the other EIGRP routers. It is also used to tag the routing information. Valid values are from 1 to 65535.

Command Default

EIGRP routing 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
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **router eigrp** command creates an EIGRP routing process or enters router configuration mode for an existing EIGRP routing process. You can only create a single EIGRP routing process on the ASA.

Use the following router configuration mode commands to configure the EIGRP routing processes:

- **auto-summary**—Enable/disable automatic route summarization.
- **default-information**—Enable/disable the reception and sending of default route information.
- **default-metric**—Define the default metrics for routes redistributed into the EIGRP routing process.
- **distance eigrp**—Configure the administrative distance for internal and external EIGRP routes.
- **distribute-list**—Filter the networks received and sent in routing updates.
- **eigrp log-neighbor-changes**—Enable/disable the logging of neighbor state changes.
- **eigrp log-neighbor-warnings**—Enable/disable the logging of neighbor warning messages.
- **eigrp router-id**—Creates a fixed router ID.
- **eigrp stub**—Configures the ASA for stub EIGRP routing.

- **neighbor**—Statically define an EIGRP neighbor.
- **network**—Configure the networks that participate in the EIGRP routing process.
- **passive-interface**—Configure an interface to act as a passive interface.
- **redistribute**—Redistribute routes from other routing processes into EIGRP.

Use the following interface configuration mode commands to configure interface-specific EIGRP parameters:

- **authentication key eigrp**—Define the authentication key used for EIGRP message authentication.
- **authentication mode eigrp**—Define the authentication algorithm used for EIGRP message authentication.
- **delay**—Configure the delay metric for an interface.
- **hello-interval eigrp**—Change the interval at which EIGRP hello packets are sent out of an interface.
- **hold-time eigrp**—Change the hold time advertised by the ASA.
- **split-horizon eigrp**—Enable/disable EIGRP split-horizon on an interface.
- **summary-address eigrp**—Manually define a summary address.

Examples

The following example shows how to enter the configuration mode for the EIGRP routing process with the autonomous system number 100:

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
clear configure eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

router-id

To use a fixed router ID, use the **router-id** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3. To reset OSPF to use the previous router ID behavior, use the **no** form of this command.

router-id *id*
no router-id [*id*]

Syntax Description

id Specifies the router ID in IP address format.

Command Default

If not specified, the highest-level IP address on the ASA is used as the router ID.

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 configuration	• Yes	—	• Yes	• Yes	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The processing order for this command was changed. The command is now processed before the **network** commands in an OSPFv2 configuration.
9.0(1)	Multiple context mode and OSPFv3 are supported.

Usage Guidelines

By default, the ASA uses the highest-level IP address on an interface that is covered by a **network** command in the OSPF configuration. If the highest-level IP address is a private address, then that address is sent in hello packets and database definitions. To use a specific router ID, use the **router-id** command to specify a global address for the router ID.

Router IDs must be unique within an OSPF routing domain. If two routers in the same OSPF domain are using the same router ID, routing may not work correctly.

You should enter the **router-id** command before entering **network** commands in an OSPF configuration. This prevents possible conflicts with the default router ID generated by the ASA. If you do have a conflict, you will receive the message:

```
ERROR: router-id id in use by ospf process pid
```

To enter the conflicting ID, remove the **network** command that contains the IP address causing the conflict, enter the **router-id** command, and then re-enter the **network** command.

Clustering

In Layer 2 clustering, you either need to configure the **router-id** *id* command or leave the router ID blank, provided all units receive the same router ID.

Examples

The following example sets the router ID to 192.168.1.1:

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show ospf	Displays general information about the OSPFv2 routing processes.

router-id cluster-pool

To specify the router ID cluster pool for a Layer 3 clustering deployment, use the **router-id cluster-pool** command in router configuration mode for OSPFv2 or IPv6 router configuration mode for OSPFv3.

router-id cluster-pool hostname | A.B.C.D *ip_pool*

Syntax Description

cluster-pool	Enables configuration of an IP address pool when Layer 3 clustering is configured.
hostname | **A.B.C.D**	Specifies the OSPF router ID for this OSPF process.
ip_pool	Specifies the name of the IP address pool.

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
Router configuration	• Yes	—	• Yes	—	—
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Router IDs must be unique within an OSPFv2 or OSPFv3 routing domain in clustering. If two routers in the same OSPFv2 or OSPFv3 domain are using the same router ID, routing in clustering may not work correctly.

In Layer 2 clustering, you either need to configure the **router-id** *id* command or leave the router ID blank, provided all units receive the same router ID.

When a Layer 3 cluster interface is configured, each unit must have a unique interface IP address. To make sure that each unit has a unique interface IP address, you can configure a local pool of IP addresses for OSPFv2 or OSPFv3 with the **router-id cluster-pool** command.

Examples

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv2:

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
```

```
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

The following example shows how to configure an IP address pool when Layer 3 clustering is configured for OSPFv3:

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

Related Commands

Command	Description
ipv6 router ospf	Enters IPv6 router configuration mode.
router ospf	Enters router configuration mode.
show ipv6 ospf	Displays general information about the OSPFv3 routing processes.
show ospf	Displays general information about the OSPFv2 routing processes.

router isis

To enable the IS-IS routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

router isis
no router isis

Syntax Description

This command has no arguments or keywords.

Command Default

This command 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(1)	This command was added.

Usage Guidelines

This command is used to enable IS-IS routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the ASA. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible. See the Related Commands table for a list of commands used to configure IS-IS.

Examples

In the following example IS-IS routing is enabled:

```
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

Related Commands

router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

router ospf *pid*
no router ospf *pid*

Syntax Description

pid	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The *pid* does not need to match the ID of OSPF processes on other routers.

Command Default

OSPF routing 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
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the ASA. Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in router configuration mode.

When using the **no router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no router ospf** command terminates the OSPF routing process specified by its *pid.* You assign the *pid* locally on the ASA. You must assign a unique value for each OSPF routing process.

The **router ospf** command is used with the following OSPF-specific commands to configure OSPF routing processes:

- **area**—Configures a regular OSPF area.
- **compatible rfc1583**—Restores the method used to calculate summary route costs per RFC 1583.
- **default-information originate**—Generates a default external route into an OSPF routing domain.
- **distance**—Defines the OSPF route administrative distances based on the route type.
- **ignore**—Suppresses the sending of syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets.

- **log-adj-changes**—Configures the router to send a syslog message when an OSPF neighbor goes up or down.
- **neighbor**—Specifies a neighbor router. Used to allow adjacency to be established over VPN tunnels.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain to another according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timer lsa arrival**— Defines the minimum interval (in msec) between accepting the same link-state advertisement (LSA) from OSPF neighbors.
- **timer pacing flood**— Defines the minimum interval (in msec) at which LSAs in the flooding queue are paced between updates.
- **timer pacing lsa-group**— Defines the interval (in sec) between groups of LSA being refreshed or managed.
- **timer pacing retransmission**— Defines the minimum interval (in msec) between neighbor retransmissions.
- **timer throttle lsa**— Defines the delay to generate the first occurrence of LSA (in milliseconds).
- **timer throttle spf**— Defines the delay between receiving a change to SPF calculation (in milliseconds).
- **timer nsf wait**—Defines the interface wait interval during NSF restart. The default value is 20 seconds. The permissible range is 1 to 65535 seconds.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

Related Commands

Command	Description
clear configure router	Clears the OSPF router commands from the running configuration.
show running-config router ospf	Displays the OSPF router commands in the running configuration.

router rip

To start a RIP routing process and configure parameters for that process, use the **router rip** command in global configuration mode. To disable the RIP routing process, use the **no** form of this command.

router rip
no router rip

Syntax Description

This command has no arguments or keywords.

Command Default

RIP routing 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
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **router rip** command is the global configuration command for configuring the RIP routing processes on the ASA. You can only configure one RIP process on the ASA. The **no router rip** command terminates the RIP routing process and removes all router configuration for that process.

When you enter the **router rip** command, the command prompt changes to ciscoasa(config-router)#, indicating that you are in router configuration mode.

The **router rip** command is used with the following router configuration commands to configure RIP routing processes:

- **auto-summary**—Enable/disable automatic summarization of routes.
- **default-information originate**—Distribute a default route.
- **distribute-list in**—Filter networks in incoming routing updates.
- **distribute-list out**—Filter networks in outgoing routing updates.
- **network**—Add/remove interfaces from the routing process.
- **passive-interface**—Set specific interfaces to passive mode.
- **redistribute**—Redistribute routes from other routing processes into the RIP routing process.
- **version**—Set the RIP protocol version used by the ASA.

Additionally, you can use the following commands in interface configuration mode to configure RIP properties on a per-interface basis:

- **rip authentication key**—Set an authentication key.
- **rip authentication mode**—Set the type of authentication used by RIP Version 2.
- **rip send version**—Set the version of RIP used to send updates out of the interface. This overrides the version set in global router configuration mode, if any.
- **rip receive version**—Set the version of RIP accepted by the interface. This overrides the version set in global router configuration mode, if any.

RIP is not supported in transparent mode. By default, the ASA denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through an ASA operating in transparent mode you must define access list entries to permit this traffic. For example, to permit RIP version 2 traffic through the ASA, create an access list entry such as the following:

ciscoasa(config)# **access-list myriplist extended permit ip any host 224.0.0.9**

To permit RIP version 1 broadcasts, create an access list entry such as the following:

ciscoasa(config)# **access-list myriplist extended permit udp any any eq rip**

Apply these access list entries to the appropriate interface using the **access-group** command.

You can enable both RIP and OSPF routing on the ASA at the same time.

Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

Related Commands

Command	Description
clear configure router rip	Clears the RIP router commands from the running configuration.
show running-config router rip	Displays the RIP router commands in the running configuration.

rtp-conformance

To check RTP packets flowing on the pinholes for protocol conformance in H.323 and SIP, use the **rtp-conformance** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

rtp-conformance [**enforce-payloadtype**]
no rtp-conformance [**enforce-payloadtype**]

Syntax Description

enforce-payloadtype	Enforces payload type to be audio/video based on the signaling exchange.

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
7.2(1)	This command was added.

Examples

The following example shows how to check RTP packets flowing on the pinholes for protocol conformance on an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

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.
debug rtp	Displays debug information and error messages for RTP packets associated with H.323 and SIP inspection.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

rtp-min-port rtp-max-port (Deprecated)

To configure the rtp-min-port and rtp-max-port limits for the phone proxy feature, use the **rtp-min-port rtp-max-port** command in phone-proxy configuration mode. To remove the limits from the phone proxy configuration, use the **no** form of this command.

rtp-min-port *port1* **rtp-maxport** *port2*
no rtp-min-port *port1* **rtp-maxport** *port2*

Syntax Description

port1	Specifies the minimum value for the RTP port range for the media termination point, where *port1* can be a value from 1024 to 16384.
port2	Specifies the maximum value for the RTP port range for the media termination point, where *port2* can be a value from 32767 to 65535.

Command Default

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

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Phone-proxy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	The command was added.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Usage Guidelines

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

Examples

The following example shows the use of the **rtp-min-port** command to specify the ports to use for media connections:

```
ciscoasa
(config-phone-proxy)#
rtp-min-port 2001 rtp-maxport 32770
```

Related Commands

Command	Description
phone-proxy	Configures the Phone Proxy instance.