



H.323 RAS Support in Cisco IOS Firewall

First Published: November 17, 2006

Last Updated: June 19, 2009

This feature introduces support for H.225 Registration, Admission, and Status (RAS) signaling in Cisco IOS firewalls. RAS is a signaling protocol that is used between endpoints (such as gateways) and gatekeepers.

The H.225 standard is used by H.323 for call setup. H.255 includes RAS control, which is used to communicate with the gatekeeper. A RAS signaling channel enables connections between the gatekeeper and H.323 endpoints.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for H.323 RAS Support in Cisco IOS Firewall](#)” section on page 8.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Restrictions for H.323 RAS Support in Cisco IOS Firewall](#), page 2
- [How to Configure a Firewall Policy for H.323 RAS Protocol Inspection](#), page 2
- [Configuration Examples for H.225 RAS Protocol Inspection](#), page 5
- [Additional References](#), page 6
- [Feature Information for H.323 RAS Support in Cisco IOS Firewall](#), page 8



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for H.323 RAS Support in Cisco IOS Firewall

H.225 RAS inspection is supported only with zone-based policy firewall inspection.

How to Configure a Firewall Policy for H.323 RAS Protocol Inspection

- [Configuring a Class Map for H.323 RAS Protocol Inspection, page 2](#)
- [Creating a Policy Map for H.323 RAS Protocol Inspection, page 3](#)

Configuring a Class Map for H.323 RAS Protocol Inspection

Use this task to configure a class map for classifying network traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect [match any | match all] class-map-name**
4. **match access-group {access-group | name access-group-name}**
5. **match protocol protocol-name [signature]**
6. **match protocol protocol-name [signature]**
7. **match class-map class-map-name**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	class-map type inspect [match-any match-all] class-map-name Example: Router(config)# class-map type inspect match-all c1	Creates a Layer 3 or Layer 4 inspect type class map and enters class-map configuration mode.

	Command or Action	Purpose
Step 4	match access-group { <i>access-group</i> name <i>access-group-name</i> } Example: Router(config-cmap)# match access-group 101	(Optional) Configures the match criterion for a class map based on the access control list (ACL) name or number.
Step 5	match protocol <i>protocol-name</i> [signature] Example: Router(config-cmap)# match protocol h225ras	Configures the match criterion for a class map on the basis of a specified protocol. Note You should specify the h225ras keyword to create a class-map for H.225 RAS protocol classification. For a list of supported protocols, use the command-line interface (CLI) help option (?) on your platform.
Step 6	match protocol <i>protocol-name</i> [signature] Example: Router(config-cmap)# match protocol h323	Configures the match criterion for a class map on the basis of a specified protocol. Note You should specify the h323 keyword to create a class-map for H.323 protocol classification.
Step 7	match class-map <i>class-map-name</i> Example: Router(config-cmap)# match class-map c1	(Optional) Specifies a previously defined class as the match criterion for a class map.
Step 8	exit Example: Router(config-cmap)# exit	Returns to global configuration mode.

Creating a Policy Map for H.323 RAS Protocol Inspection

Use this task to create a policy map for a firewall policy that will be attached to zone pairs.



Note

If you are creating an inspect type policy map, only the following actions are allowed: drop, inspect, police, and pass.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-name*
5. **inspect** [*parameter-map-name*]
6. **police rate** *bps* **burst** *size*

7. **drop** [log]
8. **pass**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	policy-map type inspect <i>policy-map-name</i> Example: Router(config)# policy-map type inspect p1	Creates a Layer 3 and Layer 4 inspect type policy map and enters policy-map configuration mode.
Step 4	class type inspect <i>class-name</i> Example: Router(config-pmap)# class type inspect c1	Specifies the traffic (class) on which an action is to be performed and enters policy-map class configuration mode.
Step 5	inspect [<i>parameter-map-name</i>] Example: Router(config-pmap-c)# inspect inspect-params	Enables Cisco IOS stateful packet inspection.
Step 6	police rate <i>bps</i> <i>burst</i> <i>size</i> Example: Router(config-pmap-c)# police rate 2000 burst 3000	(Optional) Limits traffic matching within a firewall (inspect) policy.
Step 7	drop [log] Example: Router(config-pmap-c)# drop	(Optional) Drops packets that are matched with the defined class. Note The actions drop and pass are exclusive, and the actions inspect and drop are exclusive; that is, you cannot specify both of them.
Step 8	pass Example: Router(config-pmap-c)# pass	(Optional) Allows packets that are matched with the defined class.
Step 9	exit Example: Router(config-pmap-c)# exit	Returns to policy-map configuration mode.

What to Do Next

After configuring an H.323 RAS protocol firewall policy, you want to attach the policy to a zone pair. For information on completing this task, see the [“Zone-Based Policy Firewall”](#) module.

Configuration Examples for H.225 RAS Protocol Inspection

- [Example: H.323 RAS Protocol Inspection Configuration, page 5](#)
- [Example: H.225 RAS Firewall Policy Configuration, page 5](#)

Example: H.323 RAS Protocol Inspection Configuration

The following example shows how to configure an H.323 RAS protocol inspection policy:

```
class-map type inspect match-any c1
  match protocol h323
  match protocol h225ras
class-map type inspect match-all c2
  match protocol icmp
!
policy-map type inspect p1
  class type inspect c1
  inspect
  class class-default
  drop
policy-map type inspect p2
  class type inspect c2
  inspect
  class class-default
  drop
!
zone security z1
  description One-Network zone
zone security z2
  description Two-Network zone
zone-pair security zp source z1 destination z2
  service-policy type inspect p1
zone-pair security zp-rev source z2 destination z1
  service-policy type inspect p2
!
interface FastEthernet1/0
  ip address 10.0.0.0 255.255.0.0
  zone-member security z1
  duplex auto
  speed auto
!
interface FastEthernet1/1
  ip address 10.0.1.1 255.255.0.0
  zone-member security z2
  duplex auto
  speed auto
```

Example: H.225 RAS Firewall Policy Configuration

The following example shows how to configure the firewall policy to inspect H.225 RAS messages:

```

interface GigabitEthernet 0/1/5
 ip address 172.16.0.0 255.255.0.0
 zone-member security private
 no shut
!
interface GigabitEthernet 0/1/6
 ip address 192.168.0.0 255.255.0.0
 zone-member security internet
 no shut
!
zone security private
zone security internet
!
class-map type inspect match-any internet-traffic-class
 match protocol h225ras
 match protocol h323
!
policy-map type inspect private-internet-policy
 class type inspect internet-traffic-class
 inspect
 class class-default
!
zone-pair security private-internet source private destination internet
 service-policy type inspect private-internet-policy

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Zone-based policy configuration commands	Cisco IOS Security Command Reference
Zone-based policy information: configurations, examples, descriptions	Zone-Based Policy Firewall Zone-Based Policy Firewall Design Guide

MIBs

MIB	MIBs Link
No new or modified MIBs are supported.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/cisco/web/support/index.html</p>

Feature Information for H.323 RAS Support in Cisco IOS Firewall

Table 1 lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.


Note

Table 1 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1 Feature Information for H.323 RAS Support

Feature Name	Releases	Feature Information
H.323 RAS Support in Cisco IOS Firewall	12.4(11)T	This feature introduces support for H.255 Registration, Admission, and Status (RAS) signaling in Cisco IOS firewalls. The following commands were introduced or modified: match protocol (zone).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2006–2009 Cisco Systems, Inc. All rights reserved.