H.323 RAS Support in Cisco IOS Firewall

First Published: November 17, 2006
Last Updated: November 17, 2006

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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for H.323 RAS Support in Cisco IOS Firewall" section on page 9.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS 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

Corporate 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

This section contains the following configuration tasks:

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 class-map** *class-map-name*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • 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** {*access-group* | **name** *access-group-name*} **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** *protocol-name* [**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 class-map** *class-map-name* **Example:** `Router(config-cmap)# match class-map c1`	(Optional) Specifies a previously defined class as the match criterion for a class map.
Step 7	**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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map type inspect** *policy-map-name* **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** *class-name* **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** [*parameter-map-name*] **Example:** `Router(config-pmap-c)# inspect inspect-params`	Enables Cisco IOS stateful packet inspection.
Step 6	**police rate** *bps* **burst** *size* **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

This section contains the following configuration example:

H.323 RAS Protocol Inspection Configuration: Example

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
```

Additional References

The following sections provide references related to the H.323 RAS Support in Cisco IOS Firewall feature.

Related Documents

Related Topic	Document Title
Zone-based policy information: configurations, examples, descriptions	*Zone-Based Policy Firewall*, Cisco IOS Release 12.4(9)T *Zone-Based Policy Firewall Design Guide*
Zone-based policy configuration commands	*Cisco IOS Security Command Reference*

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
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents the following modified command only:

- **match protocol (zone)**

match protocol (zone)

To configure the match criterion for a class map on the basis of the specified protocol, use the **match protocol** (zone) command in class-map configuration mode. To remove the protocol-based match criterion from a class map, use the **no** form of this command.

match protocol *protocol-name* [*parameter-map*] [**signature**]

no match protocol *protocol-name* [*parameter-map*] [**signature**]

Syntax Description

protocol-name	Name of the protocol used as a matching criterion. For a list of supported protocols, use the command-line interface (CLI) help option (**?**) on your platform.
parameter-map	(Optional) Specify a protocol-specific parameter map, if applicable.
signature	(Optional) Signature-based classification for peer-to-peer (P2P) packets is enabled. **Note** This option is available only for P2P traffic.

Command Default

None

Command Modes

Class-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced for Zone-Based Policy Firewall.
12.4(9)T	Support for the following protocols was added: • P2P protocols: **bittorrent**, **kazaa2**, **fasttrack**, **edonkey**, **gnutella**, **directconnect**, and **winmx** • Instant Messenger (IM) protocols: **aol**, **msnmsgr**, and **ymsgr** Also, the **signature** keyword was added to be used only with P2P protocols.
12.4(11)T	Support for the H.225 RAS protocol and the **h225ras** keyword were added.

Usage Guidelines

Use the **match protocol** (zone) command to specify traffic based on a particular protocol. You can use this command in conjunction with the **match access-group** and **match class-map** commands to build sophisticated traffic classes.

The **match protocol** (zone) command is available under the **class-map type inspect** command.

If you enter the **match protocol** (zone) command under the **class-map type inspect** command, the Port to Application Mapping (PAM) mappings are honored when the protocol field in the packet is matched against this command. All the port mappings configured in PAM appear under the class map.

Examples

The following example specifies a class map called c1 and configures the HTTP protocol as a match criterion:

```
class-map type inspect c1
 match protocol http
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 or Layer 4 inspect type class map.
match access-group	Configures the match criteria for a class map based on the specified ACL.

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

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS 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 Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS 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.