Firewall-H.323 V3 V4 Support

The Firewall H.323 V3 V4 Support feature provides the firewall with support for the H.323 Voice over IP (VoIP) Version 3 and Version 4 protocols. With Version 3 and Version 4 support, features like call signaling (H.225) over User Datagram Protocol (UDP), multiple call signaling over a single TCP connection, T.38 Fax over TCP, and address resolution using border elements are supported. Support for a rate-limiting mechanism to monitor call attempt rate and call aggregation is also introduced and can be enabled.

H.323 is a multiprotocol and multichannel suite. Channel negotiation parameters are embedded inside encoded H.323 control messages. The Base H.323 Application Layer Gateway (ALG) Support feature provides support in firewall environments to process the H.323 control messages.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and 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 table.

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

Prerequisites for Cisco IOS Firewall-H.323 V3 V4 Support

Restrictions for Firewall-H.323 V3 V4 Support

General

- Inspection of H.323 signaling over secure (encrypted) channel is not supported.

Cisco ASR 1000 Series Aggregation Services Routers

- Support is provided for gateway terminals using the H.323v4 with H.225v4 and H.245v7 protocols only.
- Backward compatibility is provided for H.323v2 messages only. H.323v1 messages are ignored.
- Multipoint conferencing, managed by the Multipoint Control Unit (MCU), is not supported.
- The T.120 protocol is not supported.
- The firewall support is limited to H.323 Direct Call Signaling and H.225 RAS Call Signaling.

Information About Firewall-H.323 V3 V4 Support

H.323 and H.225 RAS Implementation

H.225 Registration, Admission, and Status (RAS) signaling in Cisco IOS firewalls 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.225 includes RAS control, which is used to communicate with the gatekeeper. A RAS signaling channel enables connections between the gatekeeper and H.323 endpoints.

H.323 and H.245 Protocol

During the call setup between H.323 terminals, the following protocols are used:

- H.225 Call Signaling
- H.245 Call Control

Both protocol messages contain embedded IP addresses and ports. Any message passing through a router running Cisco IOS firewall must be decoded, inspected, and encoded back to the packet.

In order for an H.323 call to take place, an H.225 connection on TCP port 1720 needs to be opened. When the H.225 connection is opened, the H.245 session is initiated and established. This connection can take place on a separate channel from the H.225 or it can be done using H.245 tunneling on the same H.225 channel whereby the H.245 messages are embedded in the H.225 messages and set on the previously established H.225 channel.

If the H.245 tunneled message is not understood the Cisco IOS firewall cannot translate the message, which causes a failure in media traffic. H.245 FastConnect procedures will not help because FastConnect is terminated as soon as an H.245 tunneled message is sent.

H.323 Version 3 and Version 4 Features Supported

The table below lists the H.323 Version 3 and Version 4 features supported by Cisco IOS firewall. For information on the H.323 standard, see the Standards section.

Note On the ASR 1000 series routers Cisco IOS firewall support is limited to H.323 Direct Call Signaling and H.225 RAS Call Signaling only.

Table 1: H.323 Standards Features Supported by Cisco IOS Firewall

Standard	Features Supported by Cisco IOS Firewall
H.323 Version 3	• Caller ID • Annex E--Protocol for Multiplexed Call Signaling Transport • Annex G--Communication Between Administrative Domains • Generic information transport • Maintaining and reusing connections using call signaling channel • Supplementary services (call hold, call park and call pickup, message waiting indication, and call waiting)

Standard	Features Supported by Cisco IOS Firewall
H.323 Version 4	• Additive registrations • Alternate gatekeepers • Endpoint capacity • Bandwidth management • Usage information reporting • Generic extensibility framework • Indicating desired protocols • Call status reporting • Enhancements to Annex D (Real-Time Fax) • QoS support for H.323 enhancements • Dual Tone Multifrequency (DTMF) digit transmission using Real-Time Protocol (RTP)

Base H.323 ALG Support

The Base H.323 ALG Support feature provides support for ALGs to perform protocol specific issues such as processing embedded IP address and port numbers and extracting connection and session information from control channels and sessions.

Encoded channel-negotiation parameters are embedded in H.323 control messages. In Cisco IOS firewall environments, the system must intercept these messages and invoke the H.323 ALG to process the messages.

The H.323 ALG performs the following tasks to process the messages:

- Intercepts the H.323 control messages on the H.225.0 TCP port 1720 and on the dynamically negotiated H.245 TCP port.
- Decodes the intercepted control messages.
- Parses the decoded control messages, identifies the embedded IP address and port-number pairs and builds action info tokens based on the IP address and port-number pairs.
- Sends the action info tokens to the Cisco IOS firewall for processing.

The Cisco IOS firewall performs the actions indicated by the action info tokens. The actions performed include session and door entry lookup, creation, and deletion, or address and port translation. When the Cisco IOS firewall completes the action, it fills the action-result field in the action-info token, with the translated IP address and port number, or with an action failure indicator. Cisco IOS firewall then adds a flag to indicate if the packet should be dropped or forwarded. Finally, it returns the action info token to the H.323 ALG.

- Receives the modified action info token from the Cisco IOS firewall and either drops or forwards the packet based on information in the action info token.

The table below lists the H.323 control messages processed by the Base H.323 ALG Support feature. For more information on the H.323 standard, see the Standards section.

Table 2: H.323 Control Messages Processed by Base H.323 ALG Support

Protocol	Messages
H.225.0 Call Signalling	• Setup • Alert • Call proceed • Connect • Facility • Progress • Empty • ReleaseComplete • SetupAcknowlege
H.245 Media Control **Note** If tunnelling mode is enabled H.245 messages may be embedded within H.225.0 messages	• OpenLogicalChannel • OpenLogicalAck • CloseLogicalChannel • CloseLogicalAck

Support of Rate Limiting Mechanism

In addition to supporting Version 3 and Version 4 of the H.323 protocol, support is introduced for a rate-limiting mechanism to monitor call attempt rate and call aggregation. Rate limiting is more important for voice applications where gateways and gatekeepers are set up in less secure arrangements such as a Demilitarized Zone (DMZ). A DMZ can be vulnerable to attack from the Internet.

Rate Limiting of H.323 Traffic Messages

Rate limiting of H.323 traffic control messages is based on actions on H.323 class maps. The messages that are to be rate limited are specified through match message statements within the class map. The rate-limit threshold value is specified by a rate limit command, as an action on the H.323 class map. The rate limit command limits the message attempt rate; it limits the number of H.323 messages being sent per second to and from an end point. Rate Limiting can be used to control call attempt rate.

Note While configuring the **rate-limit** command, do not configure the **allow** or **reset** commands. An error message is displayed if you try to configure the **allow** or **reset** commands while configuring the **rate-limit** command and vice versa.

How to Configure Firewall-H.323 V3 V4 Support

Configuring a Firewall Policy for H.323 Traffic

Configuring a Class Map for H.323 Traffic

Perform this task to define the class map that for H.323 traffic that is to be permitted between zones.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** [**match-any** | **match-all**] **class-map-name**
4. **match protocol protocol-name [parameter-map] [signature]**
5. **match protocol h225ras**
6. match protocol h323-annexe
7. match protocol h323-nxg
8. **end**

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.

	Command or Action	Purpose
Step 3	**class-map type inspect** [**match-any** | **match-all**] **class-map-name** **Example:** `Router(config)# class-map type inspect match-any h323-traffic-class`	Creates a Layer 3 and Layer 4 (Top Level) inspect type class map and enters class-map configuration mode.
Step 4	**match protocol protocol-name [parameter-map] [signature]** **Example:** `Router(config-cmap)# match protocol h323`	Configures the match criterion for a class map on the basis of the specified protocol.
Step 5	**match protocol h225ras** **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 h323-annexe **Example:** `Router(config-cmap)# match protocol h323-annexe`	Enables the inspection of H.323 Protocol Annex E traffic.
Step 7	match protocol h323-nxg **Example:** `Router(config-cmap)# match protocol h323-nxg`	Enables the inspection of H.323 Protocol Annex G traffic.
Step 8	**end** **Example:** `Router(config-cmap)# end`	Exits class-map configuration mode and enters privileged EXEC mode.

Configuring a Policy Map for H.323 Traffic

Perform this task to create a policy map for H.323 traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect policy-map-name**
4. **class type inspect** *class-map-name*
5. **inspect [parameter-map-name]**
6. **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 h323-policy`	Creates a Layer 3 or Layer inspect type policy map.
Step 4	**class type inspect** *class-map-name* **Example:** `Router(config)# class type inspect h323-traffic-class`	Specifies the traffic (class) on which an action is to be performed. **Note** The *class-map-name* value must match the appropriate class map name specified via the **class-map type inspect**command.
Step 5	**inspect [parameter-map-name]** **Example:** `Router(config)# inspect`	Enables Cisco IOS stateful packet inspection. **Note** The actions **drop** or **allow** may also be used instead of the **inspect** command here.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Configuring a Zone-Pair for H.323 Traffic and Applying an H.323 Policy Map

Perform this task to configure a zone-pair for H.323 traffic and to apply an H.323 policy map to the traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** *zone-pair-name*
4. **exit**
5. **zone security** *zone-pair-name*
6. **exit**
7. **zone security** *zone-pair-name*
8. **exit**
9. **zone-pair security zone-pair-name** {**source source-zone-name**| **self**} **destination** [**self** | **destination-zone-name**]
10. **service-policy type inspect** *policy-map-name*
11. **end**

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	**zone security** *zone-pair-name* **Example:** `Router(config) zone security in-out`	Specifies the name of the zone-pair and enters security zone configuration mode.
Step 4	**exit** **Example:** `Router(config-sec-zone) exit`	Exits security zone configuration mode and enters global configuration mode.

	Command or Action	Purpose
Step 5	**zone security** *zone-pair-name* **Example:** `Router(config) zone security inside`	Creates the source zone from which traffic originates and enters security zone configuration mode.
Step 6	**exit** **Example:** `Router(config-sec-zone) exit`	Exits security zone configuration mode and enters global configuration mode.
Step 7	**zone security** *zone-pair-name* **Example:** `Router(config) zone security outside`	Creates the destination zone to which the traffic is bound and enters security zone configuration mode.
Step 8	**exit** **Example:** `Router(config-sec-zone) exit`	Enters global configuration mode.
Step 9	**zone-pair security zone-pair-name** {**source source-zone-name**| **self**} **destination** [**self** | **destination-zone-name**] **Example:** `Router(config)# zone-pair security in-out source inside destination outside`	Associates a zone-pair and declares the names of the routers from which traffic is originating (source) and to which traffic is bound (destination).
Step 10	**service-policy type inspect** *policy-map-name* **Example:** `Router(config-sec-zone)# service-policy type inspect h323-policy`	Attaches a firewall policy map to a zone-pair and enters security zone configuration mode.
Step 11	**end** **Example:** `Router(config-sec-zone)# end`	Exits security zone configuration mode and enters privileged EXEC mode.

Configuring Rate Limiting of H.323 Traffic Control Messages

Perform this task to configure a rate limit on H.323 traffic control messages.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect protocol-name** [**match-any**| **match-all**] **class-map-name**
4. **match message message-name**
5. **exit**
6. **policy-map type inspect** *protocol-name policy-map-name*
7. **class type inspect** *protocol-name class-map-name*
8. **rate-limit** *limit-number*
9. **end**

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 protocol-name** [**match-any**| **match-all**] **class-map-name** **Example:** `Router(config)# class-map type inspect h323 match-any h323-ratelimit-class`	Creates a Layer 7 (application-specific) inspect type class map and enters class-map configuration mode.
Step 4	**match message message-name** **Example:** `Router(config-cmap)# match message setup`	Configures the match criterion for a class map on the basis of H.323 protocol messages.
Step 5	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**policy-map type inspect** *protocol-name policy-map-name* **Example:** `Router(config)# policy-map type inspect h323 h323-ratelimit-policy`	Creates a Layer 7 inspect type policy map and enters policy-map configuration mode.
Step 7	**class type inspect** *protocol-name class-map-name* **Example:** `Router(config-pmap)# class type inspect h323 h323-ratelimit-class`	Specifies the Layer 7 traffic (class) on which an action is to be performed and enters policy-map class configuration mode. **Note** The *class-map-name* value must match the appropriate class map name specified via the **class-map type inspect**command.
Step 8	**rate-limit** *limit-number* **Example:** `Router(config-pmap-c)# rate limit 1000`	Limits the number of messages that strike the Cisco IOS firewall every second.
Step 9	**end** **Example:** `Router(config-cmap-c)# end`	Exits policy-map class configuration mode and enters privileged EXEC mode.

Configuring Deep Packet Inspection on a Layer 3 Policy Map

Perform this task to configure deep packet inspection on a Layer 3 policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map type inspect policy-map-name**
4. **class type inspect class-map-name**
5. **service-policy** *protocol-name policy-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• 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 h323-policy`	Creates a Layer 3 and Layer 4 inspect type policy map.
Step 4	**class type inspect class-map-name** **Example:** `Router(config-pmap)# class type inspect h323-traffic-class`	Specifies the traffic (class) on which an action is to be performed and enters policy-map configuration mode.
Step 5	**service-policy** *protocol-name policy-map-name* **Example:** `Router(config-pmap-c)# service-policy h323 h323-ratelimit-policy`	Attaches a Layer 7 policy map to a top-level policy map.
Step 6	**end** **Example:** `Router(config-cmap-c)# end`	Exits policy-map class configuration mode and enters privileged EXEC mode.

Configuration Examples for Firewall-H.323 V3 V4 Support

Example Configuring a Voice Policy to Inspect H.323 Annex E Packets

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex E packets for the “my-voice-class” class map:

```
class-map type inspect match-all my-voice-class
 match protocol h323-annexe
```

Example Configuring a H.323 Class-Map to Match Specific Messages

The following example shows how to configure an H.323 specific class map to match H.225 setup or release-complete messages only:

```
class-map type inspect h323 match-any my_h323_rt_msgs
 match message setup
 match message release-complete
```

Example Configuring a Voice Policy to Inspect H.323 Annex G Packets

The following example shows how to configure a voice policy to inspect the H.323 protocol Annex E packets for the “my-voice-class” class map:

```
class-map type inspect match-all my-voice-class
 match protocol h323-nxg
```

Example Configuring a Voice Policy to Limit Call Attempt Rate

The following example shows how to configure a voice policy to limit the call attempt rate to 16 calls per second for the calls terminated at 192.168.2.1.

```
access-list 102 permit ip any host 192.168.2.1
!
class-map type inspect match-all my_voice_class
 match protocol h323
 match access-group 102
!
class-map type inspect h323 match-any my_h323_rt_msgs
 match message setup
 policy-map type inspect h323 my_h323_policy
!
class type inspect h323 my_h323_rt_msgs
 rate-limit 16
!
policy-map type inspect my_voice_policy
 class type inspect my_voice_class
 inspect
 service-policy h323 my_h323_policy
!
```

Additional References for Firewall—H.323 V3 V4 Support

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
Cisco security commands	• Security Command Reference: Commands A to C • Security Command Reference: Commands D to L • Security Command Reference: Commands M to R • Security Command Reference: Commands S to Z

Standards and RFCs

Standard/RFC	Title
ITU-T H.225.0	*Call signalling protocols and media stream packetization for packet-based multimedia communication systems*
ITU-T H.245	*Control protocol for multimedia communication*
ITU-T H.323 (H.323 Version 4 and earlier)	*Packet-based multimedia communications systems*
ITU-T H.450	*Supplementary services for multimedia*

Technical Assistance

Description	Link
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.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Firewall-H.323 V3 V4 Support

The following table provides release information about the feature or features described in this module. This table 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.

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

Table 3: Feature Information for Firewall - H.323 V3/V4 Support

Feature Name	Releases	Feature Information
Firewall--H.323 V3/V4 Support	12.4(20)T	This feature introduces support for a range of H.323 Version 3 and Version 4 features and support for a rate-limiting mechanism to monitor call attempt rate and call aggregation. The following commands were introduced or modified: **class-map type inspect**, **class type inspect**, **match message**, **match protocol h323-annexe**, **match protocol h323-nxg**, **match protocol (zone)**, **policy-map type inspect**, **rate-limit (firewall)**, **service-policy (policy-map)**, **service-policy type inspect**.