



Firewall Support for SIP

The Firewall Support for SIP feature integrates Cisco IOS firewalls, Voice over IP (VoIP) protocol, and Session Initiation Protocol (SIP) within a Cisco IOS-based platform, enabling better network convergence.



Note

Some Cisco IOS versions earlier than 12.2(11)YU and 12.2(15)T may accept the configuration commands for SIP that are shown in this document; however, those earlier versions will not function properly.

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 Firewall SIP Support”](#) section on page 13.

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 Firewall Support for SIP, page 2](#)
- [Information About Firewall Support for SIP, page 2](#)
- [How to Configure Your Firewall for SIP, page 8](#)
- [Configuration Examples for Firewall SIP Support, page 11](#)
- [Additional References, page 11](#)
- [Feature Information for Firewall SIP Support, page 13](#)



Americas Headquarters:

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

Restrictions for Firewall Support for SIP

DNS Name Resolution

Although SIP methods can have Domain Name System (DNS) names instead of raw IP addresses, this feature currently does not support DNS names.

SIP UDP Support Only

This feature supports only the SIP User Datagram Protocol (UDP) format for signaling; the TCP format is not supported.

SIP Abbreviated Header

This feature does not support the compact form of SIP header fields.

Earlier Versions of Cisco IOS

Some Cisco IOS versions earlier than 12.2(11)YU and 12.2(15)T may accept the configuration commands for SIP that are shown in this document; however, those earlier versions will not function properly.

Information About Firewall Support for SIP

- [Cisco IOS Firewall, page 2](#)
- [SIP \(Session Initiation Protocol\), page 3](#)
- [SIP Messages, page 3](#)
- [Firewall for SIP Functionality Description, page 5](#)
- [SIP Message Treatment by the Firewall, page 6](#)
- [Call Database, page 7](#)
- [Cisco IOS Firewall, page 2](#)
- [SIP \(Session Initiation Protocol\), page 3](#)

Cisco IOS Firewall

The Cisco IOS firewall extends the concept of static access control lists (ACLs) by introducing dynamic ACL entries that open on the basis of the necessary application ports on a specific application and close these ports at the end of the application session. The Cisco IOS firewall achieves this functionality by inspecting the application data, checking for conformance of the application protocol, extracting the relevant port information to create the dynamic ACL entries, and closing these ports at the end of the session. The Cisco IOS firewall is designed to easily allow a new application inspection whenever support is needed.

SIP (Session Initiation Protocol)

SIP is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints. Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP Messages

SIP has two types of messages—requests and responses—that have the following generic structure:

```
generic-message = Request-Line | Status-Line
                  * ( general-header | request-header
                    | response-header | entity-header )
                  CRLF
                  [ message-body]
```

**Note**

Any of these message components may contain embedded IP addresses.

[Table 1](#) identifies the six available SIP request messages.

Table 1 *SIP Request Messages*

SIP Message	Purpose
ACK	Confirms receipt of a final response to INVITE
BYE	Is sent by either side to end the call
CANCEL	Is sent to end a call that has not yet been connected
INVITE	Is a request from a User Agent Client (UAC) to initiate a session
OPTIONS	Are sent to query capabilities of the user agents and network servers
REGISTER	Is sent by the client to register the address with a SIP proxy

[Table 2](#) identifies the available SIP response methods.

Table 2 **SIP Response Messages**

SIP Message	Purpose
1xx Informational	• 100 = Trying • 180 = Ringing • 181 = Call Is Being Forwarded • 182 = Queued • 183 = Session Progress
2xx Successful	• 200 = OK
3xx Redirection	• 300 = Multiple Choices • 301 = Moved Permanently • 302 = Moved Temporarily • 303 = See Other • 305 = Use Proxy • 380 = Alternative Service
4xx Request Failure	• 400 = Bad Request • 401 = Unauthorized • 402 = Payment Required • 403 = Forbidden • 404 = Not Found • 405 = Method Not Allowed • 406 = Not Acceptable • 407 = Proxy Authentication Required • 408 = Request Timeout • 409 = Conflict • 410 = Gone • 411 = Length Required • 413 = Request Entity Too Large • 414 = Request URI Too Large • 415 = Unsupported Media Type • 420 = Bad Extension • 480 = Temporarily Not Available • 481 = Call Leg/Transaction Does Not Exist
4xx Request Failure (continued)	• 482 = Loop Detected • 483 = Too Many Hops • 484 = Address Incomplete • 485 = Ambiguous • 486 = Busy Here

Table 2 ***SIP Response Messages (continued)***

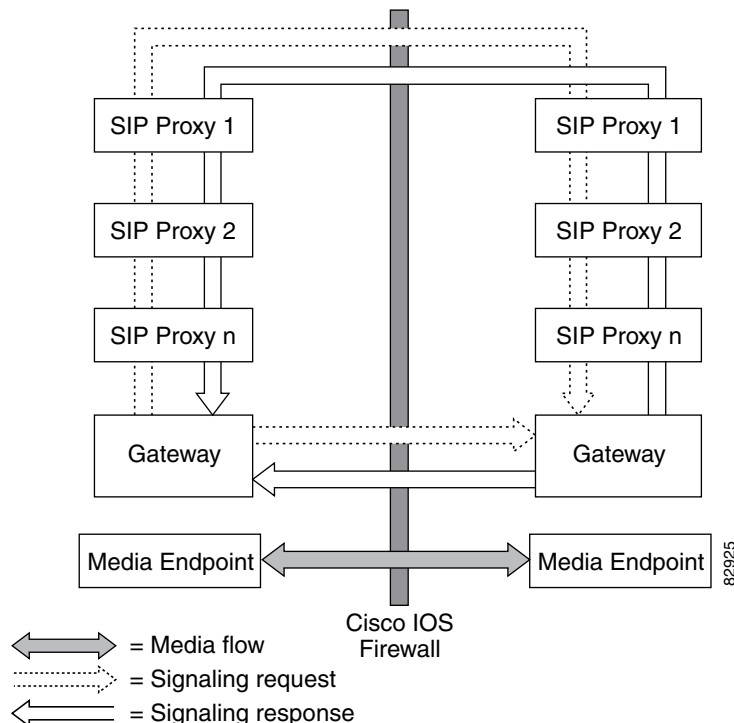
SIP Message	Purpose
5xx Server Failure	• 500 = Internal Server Error • 501 = Not Implemented • 502 = Bad Gateway • 503 = Service Unavailable • 504 = Gateway Timeout • 505 = SIP Version Not Supported
6xx Global Failure	• 600 = Busy Anywhere • 603 = Decline • 604 = Does Not Exist Anywhere • 606 = Not Acceptable

Firewall for SIP Functionality Description

The Firewall for SIP Support feature allows SIP signaling requests to traverse directly between gateways or through a series of proxies to the destination gateway or phone. After the initial request, if the Record-Route header field is not used, subsequent requests can traverse directly to the destination gateway address as specified in the Contact header field. Thus, the Cisco IOS firewall is aware of all surrounding proxies and gateways and allows the following functionality:

- SIP signaling responses can travel the same path as SIP signaling requests.
- Subsequent signaling requests can travel directly to the endpoint (destination gateway).
- Media endpoints can exchange data between each other.

See [Figure 1](#) for a sample topology that displays these functionalities.

Figure 1 Cisco IOS Firewall for SIP Awareness Sample Topology

SIP Message Treatment by the Firewall

See [Table 3](#) for information on the treatment of SIP methods by the Cisco IOS firewall.

Table 3 Treatment of SIP Methods by the Cisco IOS Firewall

SIP Message	Purpose
200 OK	Signifies the end of the call creation phase. The packet is checked for validity against the call database, and the contact information of the server is taken from it. Temporary call-flow-based openings in the firewall are created for allowing the BYE message, which can be initiated from the inside or outside.
200 OK for BYE	Signifies the graceful termination of the call and is in response to the BYE message. The same action as the CANCEL message is taken.
ACK	Signifies that the message is passed after checking for validity.
BYE	Signifies the intent to terminate the call. The database state is updated and temporary openings in the firewall are created for response to the BYE message.
CANCEL	Signifies abnormal data termination. The signaling sessions, media sessions, pregenerated temporary openings in the firewall, and the call database entry for the call are removed.

Table 3 *Treatment of SIP Methods by the Cisco IOS Firewall (continued)*

SIP Message	Purpose
INVITE	Occurs typically at the start of the call. The firewall will create a database entry upon receipt of this method and fill the database with relevant information extracted from this message. Temporary openings in the firewall will allow for a series of responses to the INVITE request. The temporary openings will be call-flow sensitive and will allow for responses for a fixed amount of time (t = 30 secs).
NO MATCH	Signifies a signaling message that is not present in the database.
Other Methods	Signifies that the message is passed if the call ID is present in the call database.
REGISTER	Results in the creation of an entry in the call database. Time-based, flow-control ACL firewall openings will allow for the response to the REGISTER and subsequent INVITE messages.
SESSION PROGRESS	Contains a response to the INVITE message, and it is a packet during the call creation phase. The packet is checked against the call database for validity of call ID and the media ports; the server proxy information is gathered from the packet. Media channels should be created in this phase.

Call Database

A call database, which contains the details of a call leg, is maintained for all call flows. A call database is created and maintained because there can be numerous signaling sessions for each call. [Table 4](#) identifies the information available in the call database.

Table 4 *Call Database Information*

Type	Purpose
call_int_over	Checks to see whether or not call initialization is over, and if so, checks to see if the call is in the teardown phase
C con ip & C con port	Signifies the IP address and port in the contact field of the initiator; for example, "Contact:<sip:1111@172.16.0.3:5060;user=phone>"
C media ip & C media port	Signifies the IP address in the media field of the initiator; for example, "c=IN IP4 172.16.0.3"
C media port	Signifies the port in the media field of the initiator; for example, "m=audio 20758 RTP/AVP 0"
C src ip & C src port	Signifies the actual IP address and port of the initiator
C via ip & C via port	Signifies the IP address and port in the via field of the initiator (the first via line); for example, "Via: SIP/2.0/UDP 172.16.0.3:5060"
current sip state	Is the current state of the call (which helps to avoid retransmission)
from/to/callid	Is extracted from the "INVITE" SIP request message to identify the call
media header	Keeps the list of media sessions for the call

Table 4 **Call Database Information (continued)**

Type	Purpose
media opened	Signifies multiple messages that may have media information, so you need to check to see whether or not the media has been opened for the call
prev sip state	Signifies the previous state of the call (which helps to avoid retransmission)
S con ip & S con port	Signifies the IP address and port in the contact field for the responder
S media ip	Signifies the IP address in the media field for the responder
S media port	Signifies the port in the media field for the responder
S src ip & S src port	Signifies the actual IP address and port of the responder
S via ip & S via port	Signifies the IP address and port in the via field for the responder
signal header	Keeps the list of signaling sessions for the call
sip_proxy_traversed	Makes the firewall topologically aware of whether the call has traversed through proxies

How to Configure Your Firewall for SIP

- [Configuring Firewall for SIP Support, page 8](#) (required)
- [Verifying Firewall for SIP Support, page 9](#) (optional)
- [Monitoring Firewall for SIP Support, page 10](#) (optional)

Configuring Firewall for SIP Support

To enable a firewall to support SIP, use the following commands.

Prerequisite

Before you configure Cisco IOS firewall support for SIP on your router, you first need to configure access lists, whose purpose normally is to block SIP traffic from unprotected networks for which the firewall will create temporary openings for specific traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name *inspection-name* sip [alert {on | off}] [audit-trail {on | off}] [timeout *seconds*]**
4. **interface *type number***
5. **ip inspect *inspection-name* {in | out}**
6. Repeat Steps 3 through 5 (Optional)

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	ip inspect name inspection-name sip [alert {on off}] [audit-trail {on off}] [timeout seconds] Example: Router(config)# ip inspect name voip sip	Turns on inspection for SIP. alert—Alert messages are generated. This function is on by default. audit-trail—Audit trail messages are generated. This function is off by default. timeout—Overrides the global channel inactivity timeout value.
Step 4	interface type number Example: Router(config)# interface FastEthernet 0/0	Configures an interface type and enters interface configuration mode.
Step 5	ip inspect inspection-name {in out} Example: Router(config-if)# ip inspect voip in	Applies inspection configurations to an interface and for a particular traffic direction.
Step 6	If SIP calls are coming from other interfaces, repeat Steps 3 through 5 and apply SIP inspections for the calls that are coming from those interfaces.	Note The inspection of protocols other than SIP may not be desirable for traffic that comes from external networks, so it may be necessary to configure an additional inspection rule specifying only SIP.

Verifying Firewall for SIP Support

To verify Cisco IOS firewall session information, perform the following optional steps:

SUMMARY STEPS

1. **enable**
2. **show ip inspect name inspection-name**
3. **show ip inspect session [detail]**
4. **show ip access-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	show ip inspect name <i>inspection-name</i> Example: Router# show ip inspect name voip	(Optional) Displays the configured inspection rule.
Step 3	show ip inspect session [detail] Example: Router# show ip inspect session	(Optional) Displays existing sessions that are currently being tracked and inspected by the Cisco IOS firewall. The optional detail keyword causes additional details about these sessions to be shown.
Step 4	show ip access-list Example: Router# show ip access-list	(Optional) Displays the contents of all current IP access lists.

Monitoring Firewall for SIP Support

To monitor firewall events, perform the following optional steps:



Note

Effective with Cisco IOS Release 12.4(20)T, the **debug ip inspect** command is replaced by the **debug policy-firewall** command. See the *Cisco IOS Debug Command Reference* for more information.

SUMMARY STEPS

1. enable
2. debug ip inspect sip

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	debug ip inspect sip Example: Router# debug ip inspect sip	(Optional) Displays the operations of the SIP inspection engine for debugging purposes.

Configuration Examples for Firewall SIP Support

- [Example: Firewall and SIP Configuration, page 11](#)

Example: Firewall and SIP Configuration

The following example shows how to allow outside initiated calls and internal calls. For outside initiated calls, an ACL needs to be punched to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
  ip inspect voip in
!
!
interface FastEthernet0/1
  ip inspect voip in
  ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS firewall information and configuration tasks	“Configuring Context-Based Access Control”
Cisco IOS firewall commands	Cisco IOS Security Command Reference

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	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

RFCs

RFCs ¹	Title
RFC 2543	SIP: Session Initiation Protocol

1. Not all supported RFCs are listed.

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 SIP Support

Table 5 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 5 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 5 Feature Information for Firewall SIP Support

Feature Name	Releases	Feature Information
Firewall SIP Support	12.2(11)YU 12.2(15)T	The Firewall Support for SIP feature integrates Cisco IOS firewalls, Voice over IP (VoIP) protocol, and Session Initiation Protocol (SIP) within a Cisco IOS-based platform, enabling better network convergence. The following commands were introduced or modified: debug ip inspect, ip inspect name.

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.

© 2007 Cisco Systems, Inc. All rights reserved.

