SIP ALG Hardening for NAT and Firewall

The SIP ALG Hardening for NAT and Firewall feature provides better memory management and RFC compliance over the existing Session Initiation Protocol (SIP) application-level gateway (ALG) support for Network Address Translation (NAT) and firewall. This feature provides the following enhancements:

- Management of the local database for all SIP Layer 7 data
- Processing of the Via header
- Support for logging additional SIP methods
- Support for Provisional Response Acknowledgment (PRACK) call flow
- Support for the Record-Route header

The above enhancements are available by default; no additional configuration is required on NAT or firewall.

This module explains the SIP ALG enhancements and describes how to enable NAT and firewall support for SIP.

- Finding Feature Information, on page 1
- Restrictions for SIP ALG Hardening for NAT and Firewall, on page 2
- Information About SIP ALG Hardening for NAT and Firewall, on page 2
- How to Configure SIP ALG Hardening for NAT and Firewall, on page 4
- Configuration Examples for SIP ALG Hardening for NAT and Firewall, on page 9
- Additional References for SIP ALG Hardening for NAT and Firewall, on page 10
- Feature Information for SIP ALG Hardening for NAT and Firewall, on page 11

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.
Restrictions for SIP ALG Hardening for NAT and Firewall

- Session Initiation Protocol (SIP) application-level gateway (ALG) does not provide any security features.
- SIP ALG manages the local database based on call IDs. There might be a corner case involving two calls coming from two different clients with the same call ID, resulting in call ID duplication.

Information About SIP ALG Hardening for NAT and Firewall

SIP Overview

Session Initiation Protocol (SIP) is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions could include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP is based on an HTTP-like request/response transaction model. Each transaction consists of a request that invokes a particular method or function on the server and at least one response.

SIP invitations that are used to create sessions carry session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements called proxy servers to help route requests to users' current locations, authenticate and authorize users for services, implement provider call-routing policies, and provide features to users. SIP also provides a registration function that allows users to upload their current locations for use by proxy servers. SIP runs on top of several different transport protocols.

Application-Level Gateways

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address information inside the payload of an application packet. An ALG is used to interpret the application-layer protocol and perform firewall and Network Address Translation (NAT) actions. These actions can be one or more of the following depending on your configuration of the firewall and NAT:

- Allow client applications to use dynamic TCP or UDP ports to communicate with the server application.
- Recognize application-specific commands and offer granular security control over them.
- Synchronize multiple streams or sessions of data between two hosts that are exchanging data.
- Translate the network-layer address information that is available in the application payload.

The firewall opens a pinhole, and NAT performs translation service on any TCP or UDP traffic that does not carry the source and destination IP addresses in the application-layer data stream. Specific protocols or applications that embed IP address information require the support of an ALG.

SIP ALG Local Database Management

A Session Initiation Protocol (SIP) trunk is a direct connection of an IP PBX to a service provider over an IP network using SIP. There can be numerous concurrent calls in a SIP trunk. During the call setup process, all calls use the same control channel for call establishment. More than one call uses the same control channel for call setup. When the same control channel is used by more than one call, the stateful information stored
in the control-channel sessions becomes unreliable. SIP stateful information consists of media channel information such as the IP address and port number used by client and server endpoints to send media data. The media channel information is used to create a firewall pinhole and a Network Address Translation (NAT) door for the data channel in firewall and NAT, respectively. Because multiple calls use the same control channel for call setup, there will be multiple sets of media data.

In a SIP trunk, more than one call shares the same firewall and NAT session. NAT and firewall identify and manage a SIP session by using the 5 tuple in a SIP packet—source address, destination address, source port, destination port, and protocol. The conventional method of using the 5 tuple to identify and match calls does not completely support SIP trunking and often leads to Layer 7 data memory leaks and call matching issues.

In contrast to other application-level gateways (ALGs), SIP ALG manages the SIP Layer 7 data by using a local database to store all media-related information contained in normal SIP calls and in SIP calls embedded in a SIP trunk. SIP ALG uses the Call-ID header field contained in a SIP message to search the local database for call matching and to manage and terminate calls. The Call-ID header field is a dialog identifier that identifies messages belonging to the same SIP dialog.

SIP ALG uses the call ID to perform search in the local database and to manage memory resources. In certain scenarios where SIP ALG is unable to free up a Layer 7 data record from the database, a session timer is used to manage and free resources to ensure that there are no stalled call records in the database.

---

**Note**

Because all Layer 7 data is managed by SIP ALG by using a local database, SIP ALG never replies on firewall and NAT to free SIP Layer 7 data; SIP ALG frees the data by itself. If you use the `clear` command to clear all NAT translations and firewall sessions, the SIP Layer 7 data in the local database is not freed.

---

**SIP ALG Via Header Support**

A Session Initiation Protocol (SIP) INVITE request contains a Via header field. The Via header field indicates the transport paths taken by a SIP request. The Via header also contains information about the return path for subsequent SIP responses, which includes the IP address and the port to which the response message is to be sent.

SIP ALG creates a firewall pinhole or a Network Address Translation (NAT) door based on the first value in the Via header field for each SIP request received, except the acknowledge (ACK) message. If the port number information is missing from the first Via header, the port number is assumed to be 5060.

**SIP ALG Method Logging Support**

The SIP ALG Hardening for NAT and Firewall feature provides support for detailed logging of the following methods in Session Initiation Protocol (SIP) application-level gateway (ALG) statistics:

- PUBLISH
- OPTIONS
- 1XX (excluding 100,180,183)
- 2XX (excluding 200)

The existing SIP methods that are logged in SIP ALG statistics include ACK, BYE, CANCEL, INFO, INVITE, MESSAGE, NOTIFY, REFER, REGISTER, SUBSCRIBE, and 1XX-6XX.
SIP ALG PRACK Call-Flow Support

Session Initiation Protocol (SIP) defines two types of responses: final and provisional. Final responses convey the result of processing a request and are sent reliably. Provisional responses, on the other hand, provide information about the progress of processing a request but are not sent reliably.

Provisional Response Acknowledgement (PRACK) is a SIP method that provides an acknowledgment (ACK) system for provisional responses. PRACK allows reliable exchanges of SIP provisional responses between SIP endpoints. SIP reliable provisional responses ensure that media information is exchanged and resource reservation can occur before connecting the call.

SIP uses the connection, media, and attribute fields of the Session Description Protocol (SDP) during connection negotiation. SIP application-level gateway (ALG) supports SDP information within a PRACK message. If media information exists in a PRACK message, SIP ALG retrieves and processes the media information. SIP ALG also handles the creation of media channels for subsequent media streams. SIP ALG creates a firewall pinhole and a NAT door based on the SDP information in PRACK messages.

SIP ALG Record-Route Header Support

The Record-Route header field is added by a Session Initiation Protocol (SIP) proxy to a SIP request to force future requests in a SIP dialog to be routed through the proxy. Messages sent within a dialog then traverse all SIP proxies, which add a Record-Route header field to the SIP request. The Record-Route header field contains a globally reachable Uniform Resource Identifier (URI) that identifies the proxy.

SIP application-level gateway (ALG) parses the Contact header and uses the IP address and the port value in the Contact header to create a firewall pinhole and a Network Address Translation (NAT) door. In addition, SIP ALG supports the parsing of the Record-Route header to create a firewall pinhole and a NAT door for future messages that are routed through proxies.

With the parsing of the Record-Route header, SIP ALG supports the following scenarios:

- A Cisco ASR 1000 Aggregation Services Router is deployed between two proxies.
- A Cisco ASR 1000 Aggregation Services Router is deployed between a User Agent Client (UAC) and a proxy.
- A Cisco ASR 1000 Aggregation Services Router is deployed between a proxy and a User Agent Server (UAS).
- No proxy exists between the client and the server. No record routing occurs in this scenario.

How to Configure SIP ALG Hardening for NAT and Firewall

Enabling NAT for SIP Support

NAT support for SIP is enabled by default on port 5060. If this feature has been disabled, perform this task to re-enable NAT support for SIP. To disable the NAT support for SIP, use the `no ip nat service sip` command.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip nat service sip \{tcp | udp\} port \textit{port-number}
4. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable \textit{Example:} Device&gt; enable</td>
<td>Enables privileged EXEC mode. • Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal \textit{Example:} Device# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 3 ip nat service sip {tcp</td>
<td>udp} port \textit{port-number} \textit{Example:} Device(config)# ip nat service sip tcp 5060</td>
</tr>
<tr>
<td>Step 4 end \textit{Example:} Device(config)# end</td>
<td>Exist global configuration mode and returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Enabling SIP Inspection

SUMMARY STEPS

1. enable
2. configure terminal
3. class-map type inspect match-any \textit{class-map-name}
4. match protocol \textit{protocol-name}
5. exit
6. policy-map type inspect \textit{policy-map-name}
7. class type inspect \textit{class-map-name}
8. inspect
9. exit
10. class class-default
11. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable \textit{Example:}</td>
<td>Enables privileged EXEC mode. • Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>

**Step 2**

configure terminal  
**Example:**  
Device# configure terminal

**Class-map type inspect match-any class-map-name**

**Example:**  
Device(config)# class-map type inspect match-any sip-class1

**Step 3**

match protocol protocol-name

**Example:**  
Device(config-cmap)# match protocol sip

**Step 4**

exit

**Example:**  
Device(config-cmap)# exit

**Step 5**

policy-map type inspect policy-map-name

**Example:**  
Device(config)# policy-map type inspect sip-policy

**Step 6**

class type inspect class-map-name

**Example:**  
Device(config-pmap)# class type inspect sip-class1

**Step 7**

inspect

**Example:**  
Device(config-pmap-c)# inspect

**Step 8**

exit

**Example:**  
Device(config-pmap-c)# exit

**Step 9**

class class-default

**Example:**  
Device(config-pmap)# class class-default

**Step 10**

end

**Example:**  
Device(config-pmap)# end

---

**SIP ALG Hardening for NAT and Firewall**

**Enabling SIP Inspection**

- **Purpose:** Enables stateful packet inspection.
- **Step 2:** Enables global configuration mode.
- **Step 3:** Creates an inspect type class map and enters class-map configuration mode.
- **Step 4:** Configures the match criterion for a class map based on the named protocol.
- **Step 5:** Exits class-map configuration mode.
- **Step 6:** Creates an inspect type policy map and enters policy-map configuration mode.
- **Step 7:** Specifies the class on which the action is performed and enters policy-map class configuration mode.
- **Step 8:** Enables stateful packet inspection.
- **Step 9:** Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **Step 10:** Specifies that these policy map settings apply to the predefined default class.
- **Step 11:** Exits policy-map configuration mode and returns to privileged EXEC mode.
Configuring a Zone Pair and Attaching a SIP Policy Map

SUMMARY STEPS

1. enable
2. configure terminal
3. zone security {zone-name | default}
4. exit
5. zone security {zone-name | default}
6. exit
7. zone-pair security zone-pair-name [source {source-zone-name | self | default} destination [destination-zone-name | self | default]]
8. service-policy type inspect policy-map-name
9. exit
10. interface type number
11. zone-member security zone-name
12. exit
13. interface type number
14. zone-member security zone-name
15. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: enable enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 zone security {zone-name</td>
<td>default}</td>
</tr>
<tr>
<td>Example: zone security zone1</td>
<td></td>
</tr>
<tr>
<td>Step 4 exit</td>
<td>Exits security zone configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example: exit</td>
<td></td>
</tr>
<tr>
<td>Step 5 zone security {zone-name</td>
<td>default}</td>
</tr>
<tr>
<td>Example: zone security zone2</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>6</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-sec-zone)# exit</td>
</tr>
<tr>
<td>7</td>
<td>zone-pair security zone-pair-name [source {source-zone-name</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# zone-pair security in-out source zonel destination zone2</td>
</tr>
<tr>
<td>8</td>
<td>service-policy type inspect policy-map-name</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-sec-zone-pair)# service-policy type inspect sip-policy</td>
</tr>
<tr>
<td>9</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-sec-zone-pair)# exit</td>
</tr>
<tr>
<td>10</td>
<td>interface type number</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface gigabitethernet 0/0/0</td>
</tr>
<tr>
<td>11</td>
<td>zone-member security zone-name</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# zone-member security zonel</td>
</tr>
<tr>
<td>12</td>
<td>exit</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# exit</td>
</tr>
<tr>
<td>13</td>
<td>interface type number</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config)# interface gigabitethernet 0/1/1</td>
</tr>
<tr>
<td>14</td>
<td>zone-member security zone-name</td>
</tr>
<tr>
<td></td>
<td>Example: Device(config-if)# zone-member security zone2</td>
</tr>
<tr>
<td>Step 15</td>
<td>Command or Action</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
</tbody>
</table>

**Example: Enabling NAT for SIP Support**

Device> enable  
Device# configure terminal  
Device(config)# ip nat service sip tcp port 5060  
Device(config)# end

**Example: Enabling SIP Inspection**

```plaintext
class-map type inspect match-any sip-class1  
    match protocol sip 
!  
policy-map type inspect sip-policy  
    class type inspect sip-class1  
        inspect 
!  
class class-default
```

**Example: Configuring a Zone Pair and Attaching a SIP Policy Map**

```plaintext
zone security zone1  
!  
zone security zone2  
!  
zone-pair security in-out source zone1 destination zone2  
    service-policy type inspect sip-policy 
!  
interface gigabitethernet 0/0/0  
    zone security zone1  
!  
interface gigabitethernet 0/1/1  
    zone security zone2
```
Additional References for SIP ALG Hardening for NAT and Firewall

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Command List, All Releases</td>
</tr>
<tr>
<td>NAT configuration</td>
<td>IP Addressing: NAT Configuration Guide</td>
</tr>
<tr>
<td>Firewall configuration</td>
<td>Security Configuration Guide: Zone-Based Policy Firewall</td>
</tr>
<tr>
<td>NAT commands</td>
<td>Cisco IOS IP Addressing Services Command Reference</td>
</tr>
<tr>
<td>Firewall commands</td>
<td>• Cisco IOS Security Command Reference: Commands A to C</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands D to L</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands M to R</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Security Command Reference: Commands S to Z</td>
</tr>
<tr>
<td>NAT and firewall ALG support</td>
<td>NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers matrix</td>
</tr>
</tbody>
</table>

Standards and RFCs

<table>
<thead>
<tr>
<th>Standard/RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3261</td>
<td>SIP: Session Initiation Protocol</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for SIP ALG Hardening for NAT and Firewall

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 1: Feature Information for SIP ALG Hardening for NAT and Firewall

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP ALG Hardening for NAT and Firewall</td>
<td>Cisco IOS XE Release 3.8S</td>
<td>The SIP ALG Hardening for NAT and Firewall feature provides better memory management and RFC compliance over the existing SIP ALG support for NAT and firewall.</td>
</tr>
</tbody>
</table>