

Cisco Firewall-SIP Enhancements ALG

The enhanced Session Initiation Protocol (SIP) inspection in the Cisco XE firewall provides basic SIP inspect functionality (SIP packet inspection and pinholes opening) as well as protocol conformance and application security. These enhancements give you control on what policies and security checks to apply to SIP traffic and the capability to filter out unwanted messages or users.

The development of additional SIP functionality in Cisco IOS XE software provides increased support for Cisco Call Manager, Cisco Call Manager Express, and Cisco IP-IP Gateway based voice/video systems. The application-layer gateway (ALG) SIP enhancement also supports RFC 3261 and its extensions.

- Prerequisites for Cisco Firewall-SIP Enhancements ALG, on page 1
- Restrictions for Cisco Firewall-SIP Enhancements ALG, on page 1
- Information About Cisco Firewall-SIP Enhancements ALG, on page 2
- How to Configure Cisco Firewall-SIP Enhancements ALG, on page 3
- Configuration Examples for Cisco Firewall-SIP Enhancements ALG, on page 7
- Additional References for Cisco Firewall-SIP Enhancements ALG, on page 8
- Feature Information for Cisco Firewall-SIP Enhancements ALG, on page 9

Prerequisites for Cisco Firewall-SIP Enhancements ALG

Your system must be running Cisco IOS XE Release 2.4 or a later release.

Restrictions for Cisco Firewall-SIP Enhancements ALG

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.

Cisco ASR 1000 Series Routers

This feature was implemented without support for application inspection and control (AIC) on the Cisco ASR 1000 series routers. The Cisco IOS XE Release 2.4 supports the following commands only: **class-map type inspect**, **class type inspect**, **match protocol**, and **policy-map type inspect**.

Cisco ISR 4000 Series Routers

The Cisco IOS XE Fuji 16.7.1 release does not support Transport Layer Security (TLS) or Secure Real-time Transport Protocol (SRTP).

Information About Cisco Firewall-SIP Enhancements ALG

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.

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 firewall is aware of all surrounding proxies and gateways and allows the following functionalities:

- 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.

SIP UDP and TCP Support

RFC 3261 is the current RFC for SIP, which replaces RFC 2543. This feature supports the SIP UDP and the TCP format for signaling.

SIP Inspection

This section describes the deployment scenarios supported by the Cisco Firewall--SIP ALG Enhancements feature.

Cisco IOS XE Firewall Between SIP Phones and CCM

The Cisco IOS XE firewall is located between Cisco Call Manager or Cisco Call Manager Express and SIP phones. SIP phones are registered to Cisco Call Manager or Cisco Call Manager Express through the firewall, and any SIP calls from or to the SIP phones pass through the firewall.

Cisco IOS XE Firewall Between SIP Gateways

The Cisco IOS XE firewall is located between two SIP gateways, which can be Cisco Call Manager, Cisco Call Manager Express, or a SIP proxy. Phones are registered with SIP gateways directly. The firewall sees the SIP session or traffic only when there is a SIP call between phones registered to different SIP gateways. In some scenarios an IP-IP gateway can also be configured on the same device as the firewall. With this scenario all the calls between the SIP gateways are terminated in the IP-IP gateway.

Cisco IOS XE Firewall with Local Cisco Call Manager Express and Remote Cisco Call Manager Express/Cisco Call Manager

The Cisco IOS XE firewall is located between two SIP gateways, which can be Cisco Call Manager, Cisco Call Manager Express, or a SIP proxy. One of the gateways is configured on the same device as the firewall. All the phones registered to this gateway are locally inspected by the firewall. The firewall also inspects SIP sessions between the two gateways when there is a SIP call between them. With this scenario the firewall locally inspects SIP phones on one side and SIP gateways on the other side.

Cisco IOS XE Firewall with Local Cisco Call Manager Express

The Cisco IOS XE firewall and Cisco Call Manager Express is configured on the same device. All the phones registered to the Cisco Call Manager Express are locally inspected by the firewall. Any SIP call between any of the phones registered will also be inspected by the Cisco IOS XE firewall.

ALG--SIP Over TCP Enhancement

When SIP is transferred over UDP, every SIP message is carried in one single UDP datagram. However, when SIP is transferred over TCP, one TCP segment may contain multiple SIP messages. And it is possible that the last SIP message in one of the TCP segments may be a partial one. Prior to Cisco IOS XE Release 3.5S, when there are multiple SIP messages in one received TCP segment, the SIP ALG parses only the first message. The data that is not parsed is regarded as one incomplete SIP message and returned to vTCP. When the next TCP segment is received, vTCP prefixes the unprocessed data to that segment to pass them to the SIP ALG and causes more and more data have to be buffered in vTCP.

In Cisco IOS XE Release 3.5S, the ALG--SIP over TCP Enhancement feature lets the SIP ALG to handle multiple SIP messages in one TCP segment. When a TCP segment is received, all complete SIP messages inside this segment are parsed one-by-one. If there is an incomplete message in the end, only that portion is returned to vTCP.

How to Configure Cisco Firewall-SIP Enhancements ALG

Enabling SIP Inspection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**

6. **policy-map type inspect** *policy-map-name*
7. **class type inspect** *class-map-name*
8. **inspect**
9. **exit**
10. **class class-default**
11. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**class-map type inspect match-any** *class-map-name* **Example:** `Device(config)# class-map type inspect match-any sip-class1`	Creates an inspect type class map and enters class-map configuration mode.
Step 4	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol sip`	Configures the match criterion for a class map based on the named protocol.
Step 5	**exit** **Example:** `Device(config-cmap)# exit`	Exits class-map configuration mode.
Step 6	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect sip-policy`	Creates an inspect type policy map and enters policy-map configuration mode.
Step 7	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect sip-class1`	Specifies the class on which the action is performed and enters policy-map class configuration mode.
Step 8	**inspect** **Example:** `Device(config-pmap-c)# inspect`	Enables stateful packet inspection.

	Command or Action	Purpose
Step 9	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy-map configuration mode.
Step 10	**class class-default** **Example:** `Device(config-pmap)# class class-default`	Specifies that these policy map settings apply to the predefined default class. • If traffic does not match any of the match criteria in the configured class maps, it is directed to the predefined default class.
Step 11	**end** **Example:** `Device(config-pmap)# end`	Exits policy-map configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

The following commands can be used to troubleshoot your SIP-enabled firewall configuration:

- **clear zone-pair**
- **debug cce**
- **debug policy-map type inspect**
- **show policy-map type inspect zone-pair**
- **show zone-pair security**

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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**zone security** {*zone-name* | **default**} **Example:** `Device(config)# zone security zone1`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.
Step 4	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 5	**zone security** {*zone-name* | **default**} **Example:** `Device(config)# zone security zone2`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.
Step 6	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] **Example:** `Device(config)# zone-pair security in-out source zone1 destination zone2`	Creates a zone pair and returns to security zone-pair configuration mode. **Note** To apply a policy, you must configure a zone pair.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	Attaches a firewall policy map to the destination zone pair. **Note** If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**exit** **Example:**	Exits security zone-pair configuration mode and returns to global configuration mode.

	Command or Action	Purpose
	`Device(config-sec-zone-pair)# exit`	
Step 10	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 11	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security zone1`	Assigns an interface to a specified security zone. **Note** When you make an interface a member of a security zone, all traffic in and out of that interface (except traffic bound for the device or initiated by the device) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 12	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 13	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/1/1`	Configures an interface and enters interface configuration mode.
Step 14	**zone-member security** *zone-name* **Example:** `Device(config-if)# zone-member security zone2`	Assigns an interface to a specified security zone.
Step 15	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Cisco Firewall-SIP Enhancements ALG

Example: Enabling SIP Inspection

```
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

```
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 Cisco Firewall-SIP Enhancements ALG

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Firewall commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Additional SIP Information	Guide to Cisco Systems VoIP Infrastructure Solution for SIP
vTCP support	*vTCP for ALG Support*

Standards and RFCs

Standard/RFC	Title
RFC 3261	SIP: Session Initiation Protocol

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 Cisco Firewall-SIP Enhancements ALG

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 Cisco Firewall-SIP Enhancements: ALG

Feature Name	Releases	Feature Information
AGL--SIP Over TCP Enhancement	Cisco IOS XE Release 3.5S	The ALG--SIP over TCP Enhancement feature lets the SIP ALG to handle multiple SIP messages in one TCP segment. When a TCP segment is received, all complete SIP messages inside this segment are parsed one-by-one. If there is an incomplete message in the end, only that portion is returned to vTCP.
Cisco Firewall--SIP ALG Enhancements	Cisco IOS XE Release 2.4	The Cisco Firewall--SIP ALG Enhancements feature provides voice security enhancements within the firewall feature set in Cisco IOS XE software on the Cisco ASR 1000 series routers. The following commands were implemented without support for Layer 7 (application-specific) syntax, on the Cisco ASR 1000 series routers:**class type inspect, class-map type inspect**, **match protocol**, **policy-map type inspect**.
Firewall--SIP ALG Enhancement for T.38 Fax Relay	Cisco IOS XE Release 2.4.1	The Firewall--SIP ALG Enhancement for T.38 Fax Relay feature provides an enhancement within the Firewall feature set in Cisco IOS XE software on the Cisco ASR 1000 series routers. The feature enables SIP ALG to support T.38 Fax Relay over IP, passing through the firewall on the Cisco ASR 1000 series routers.