Cisco Firewall—SIP Enhancements: ALG

First Published: April 14, 2008
Last Updated: August 27, 2009

Enhanced Session Initiation Protocol (SIP) inspection in the Cisco firewall provides basic SIP inspect functionality (SIP packet inspection and pinholes opening) as well as protocol conformance and application security. These enhancements give the user a more control than in previous releases 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 (CCM), Cisco Call Manager Express (CCME), and Cisco IP-IP Gateway based voice/video systems. The Application Layer Gateway (ALG) SIP enhancement also supports RFC 3261 and its extensions.

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 Cisco Firewall—SIP Enhancements: ALG" section on page 8.

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

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

Prerequisites for Cisco Firewall—SIP Enhancements: ALG

Your system must be running Cisco IOS XE Release 2.4 or a later Cisco IOS XE software 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 AIC on the Cisco ASR 1000 series routers. This release includes support for the following commands only: **class-map type inspect**, **class type inspect**, **match protocol**, and **policy-map type inspect**.

Information About Cisco Firewall—SIP Enhancements: ALG

Firewall and SIP Overviews

Cisco IOS XE Firewall

The Cisco IOS XE 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 XE 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 XE firewall is designed to easily allow a new application inspection whenever support is needed.

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 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 the user's current location, 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 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.

SIP UDP and TCP Support

RFC 3261 is the current RFC for SIP, which replaces RFC 2543. This feature supports the SIP User Datagram Protocol (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 CCM or CCME and SIP phones. SIP phones are registered to CCM or CCME 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 CCM, CCME, 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 CCME and Remote CCME/CCCM

The Cisco IOS XE firewall is located between two SIP gateways, which can be CCM, CCME, 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 CCME

The Cisco IOS XE firewall and CCME is configured on the same device. All the phones registered to the CCME 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.

How to Configure Cisco Firewall—SIP Enhancements: ALG

Enabling SIP Inspection on Cisco ASR Series Routers

To enable SIP packet inspection, perform the steps in this section.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect match-any** *class-map-name*
4. **match protocol** *protocol-name*
5. **match protocol** *protocol-name*
6. **exit**
7. **policy-map type inspect** *policy-map-name*
8. **class type inspect** *class-map-name*
9. **inspect**
10. **service-policy** *policy-map-name*
11. **class class-default**
12. **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.

	Command or Action	Purpose
Step 3	**class-map type inspect match-any** *class-map-name* **Example:** `Router(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:** `Router(config-cmap)# match protocol sip`	Configures the match criterion for a class map on the basis of the named protocol.
Step 5	**match protocol** *protocol-name* **Example:** `Router(config-cmap)# match protocol tftp`	Configures the match criterion for a class map on the basis of the named protocol.
Step 6	**exit** **Example:** `Router(config-cmap)# exit`	Exits class-map configuration mode.
Step 7	**policy-map type inspect** *policy-map-name* **Example:** `Router(config)# policy-map type inspect sip_policy`	Creates an inspect type policy map and enters policy-map configuration mode.
Step 8	**class type inspect** *class-map-name* **Example:** `Router(config-pmap)# class type inspect sip_class1`	Specifies the class on which the action is performed and enters policy-map-class configuration mode.
Step 9	**inspect** **Example:** `Router(config-pmap-c)# inspect`	Enables stateful packet inspection.
Step 10	**service-policy** *policy-map-name* **Example:** `Router(config-pmap-c)# service-policy policy_2`	Attaches the policy map to the service policy for the interface or virtual circuit.
Step 11	**class class-default** **Example:** `Router(config-pmap-c)# 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 12	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits policy-map-class configuration mode.

Troubleshooting Tips

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

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

Configuration Examples for Cisco Firewall—SIP Enhancements: ALG

Example: Firewall and SIP Configuration on Cisco ASR 1000 Series Routers

The following example shows how to configure the Cisco ASR 1000 series routers to enable SIP inspection:

```
class-map type inspect match-any c_appl
match protocol sip
match protocol tftp

policy-map type inspect p1
class type inspect c_appl
inspect
class class-default

zone security z_in
zone security z_out

interface fastethernet0/3/6
zone-member security z_in
interface fastethernet0/3/7
zone-member security z_out

zone-pair security in2out source z_in destination z_out
service-policy type inspect p1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Commands List, All Releases*
Cisco IOS firewall commands	*Cisco IOS Security Command Reference*
Additional SIP Information	Guide to Cisco Systems VoIP Infrastructure Solution for SIP

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS XE software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

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

Table 1 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 1 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 1 Feature Information for Cisco Firewall—SIP Enhancements: ALG

Feature Name	Releases	Feature Information
Cisco Firewall—SIP ALG Enhancements	Cisco IOS XE Release 2.4	This 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	This feature provides an enhancement within the Firewall feature set in Cisco IOS XE software on the Cisco ASR 1000 series routers. It enables SIP ALG to support T.38 Fax Relay over IP, passing through the firewall on the Cisco ASR 1000 series routers.