SIP ALG Resilience to DoS Attacks

The SIP ALG Resilience to DoS Attacks feature provides protection against Session Initiation Protocol (SIP) application layer gateway (ALG) denial of service (DoS) attacks. This feature supports a configurable lock limit, a dynamic blacklist, and configurable timers to prevent DoS attacks.

This module explains the feature and how to configure DoS prevention for the SIP application layer gateway (ALG). Network Address Translation and zone-based policy firewalls support this feature.

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Information About SIP ALG Resilience to DoS Attacks

SIP ALG Resilience to DoS Attacks Overview

The SIP ALG Resilience to DoS Attacks feature provides protection against denial of service (DoS) attacks to the Session Initiation Protocol (SIP) application layer gateway (ALG). This feature supports a configurable lock limit, a dynamic blacklist, and configurable timers to prevent DoS attacks. This feature is supported by Network Address Translation (NAT) and zone-based policy firewalls.

SIP is an application-level signaling protocol for setting up, modifying, and terminating real-time sessions between participants over an IP data network. These sessions could include Internet telephone calls, multimedia distribution, and multimedia conferences. SIP DoS attacks are a major threat to networks.

The following are types of SIP DoS attacks:

- SIP register flooding: A registration flood occurs when many VoIP devices try to simultaneously register to a network. If the volume of registration messages exceeds the device capability, some messages are lost. These devices then attempt to register again, adding more congestion. Because of the network congestion, users may be unable to access the network for some time.
- SIP INVITE flooding: An INVITE flood occurs when many INVITE messages are sent to servers that cannot support all these messages. If the attack rate is very high, the memory of the server is exhausted.
- SIP broken authentication and session attack: This attack occurs when an attacker presumes the identity of a valid user, using digest authentication. When the authentication server tries to verify the identity of the attacker, the verification is ignored and the attacker starts a new request with another session identity. These attacks consume the memory of the server.

SIP ALG Dynamic Blacklist

One of the common methods of denial of service (DoS) attacks involves saturating the target network with external communication requests making the network unable to respond to legitimate traffic. To solve this issue, the SIP ALG Resilience to DoS Attacks feature uses configurable blocked lists. A blocked list is a list of entities that are denied a particular privilege, service, or access. Dynamic blacklists are disabled by default. When requests to a destination address exceed a predefined trigger criteria in the configured blocked list, the Session Initiation Protocol (SIP) application layer gateway (ALG) will drop these packets.

The following abnormal SIP session patterns are monitored by dynamic blocked lists:

- In the configured period of time if a source sends multiple requests to a destination and receives non-2xx (as per RFC 3261, any response with a status code between 200 and 299 is a "2xx response") final responses from the destination.
- In the configured period of time if a source sends multiple requests to a destination and does not receive any response from the destination.

SIP ALG Lock Limit

Both Network Address Translation (NAT) and the firewall use the Session Initiation Protocol (SIP) application layer gateway (ALG) to parse SIP messages and create sessions through tokens. To maintain session states, the SIP ALG uses a per call data structure and Layer 7 data to store call-related information that is allocated when a session is initiated and freed when a session is released. If the SIP ALG does not receive a message that indicates that the call has ended, network resources are held for the call.

Because Layer 7 data is shared between threads, a lock is required to access the data. During denial of service (DoS) and distributed DoS attacks, many threads wait to get the same lock, resulting in heavy CPU usage, which makes the system unstable. To prevent the system from becoming unstable, a limit is added to restrict the number of threads that can wait for a lock. SIP sessions are established by request/response mode. When there are too many concurrent SIP messages for one SIP call, packets that exceed the lock limit are dropped.

SIP ALG Timers

To exhaust resources on Session Initiation Protocol (SIP) servers, some denial of service (DoS) attacks do not indicate the end of SIP calls. To prevent these types of DoS attacks, a protection timer is added.

The SIP ALG Resilience to DoS Attacks feature uses the following timers:

- Call-duration timer that controls the maximum length of an answered SIP call.

- Call-proceeding timer that controls the maximum length of an unanswered SIP call.

When the configured maximum time is reached, the SIP application layer gateway (ALG) releases resources for this call, and future messages related to this call may not be properly parsed by the SIP ALG.

How to Configure SIP ALG Resilience to DoS Attacks

Configuring SIP ALG Resilience to DoS Attacks

You can configure the prevention of denial of service (DoS) parameters for the Session Initiation Protocol (SIP) application layer gateway (ALG) that is used by Network Address Translation (NAT) and the zone-based policy firewall.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **alg sip processor session max-backlog** *concurrent-processor-usage*
4. **alg sip processor global max-backlog** *concurrent-processor-usage*
5. **alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **destination** *ip-address*
6. **alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **block-time** *block-time* [**destination** *ip-address*]
7. **alg sip timer call-proceeding-timeout** *time*
8. **alg sip timer max-call-duration** *seconds*
9. **end**

DETAILED STEPS

	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	**alg sip processor session max-backlog** *concurrent-processor-usage* **Example:** `Device(config)# alg sip processor session max-backlog 5`	Sets a per session limit for the number of backlog messages waiting for shared resources.
Step 4	**alg sip processor global max-backlog** *concurrent-processor-usage* **Example:**	Sets the maximum number of backlog messages waiting for shared resources for all SIP sessions.

	Command or Action	Purpose
	`Device(config)# alg sip processor global max-backlog 5`	
Step 5	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **destination** *ip-address* **Example:** `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 destination 10.1.1.1`	Configures dynamic SIP ALG blacklist criteria for the specified destination IP address.
Step 6	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **block-time** *block-time* [**destination** *ip-address*] **Example:** `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 block-time 30`	Configures the time period, in seconds, when packets from a source are blocked if the configured limit is exceeded.
Step 7	**alg sip timer call-proceeding-timeout** *time* **Example:** `Device(config)# alg sip timer call-proceeding-timeout 35`	Sets the maximum time interval, in seconds, to end SIP calls that do not receive a response.
Step 8	**alg sip timer max-call-duration** *seconds* **Example:** `Device(config)# alg sip timer max-call-duration 90`	Sets the maximum call duration, in seconds, for a successful SIP call.
Step 9	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying SIP ALG Resilience to DoS Attacks

Use the following commands to troubleshoot the feature.

SUMMARY STEPS

1. **enable**
2. **show alg sip**
3. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip**
4. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dbl**
5. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dblcfg**
6. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip processor**
7. **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip timer**
8. **debug alg** {**all** | **info** | **trace** | **warn**}

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show alg sip**

Displays all Session Initiation Protocol (SIP) application layer gateway (ALG) information.

Example:

```
Device# show alg sip

sip timer configuration
   Type                      Seconds
   max-call-duration         380
   call-proceeding-timeout   620

sip processor configuration
   Type           Backlog number
   session         14
   global          189

sip blacklist configuration
   dst-addr         trig-period(ms)    trig-size     block-time(sec)
   10.0.0.0             60                 30              2000
   10.1.1.1             20                 30              30
   192.0.2.115          1000               5               30
   198.51.100.34        20                 30              388
```

Step 3 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip**

Displays SIP ALG-specific statistics information in the Cisco Quantum Flow Processor (QFP).

Example:

```
Device# show platform hardware qfp active feature alg statistics sip

Events
...
Cr dbl entry:                10   Del dbl entry:                10
Cr dbl cfg entry:             8   Del dbl cfg entry:             4
start dbl trig tmr:          10   restart dbl trig tmr:       1014
stop dbl trig tmr:           10   dbl trig timeout:           1014
start dbl blk tmr:            0   restart dbl blk tmr:           0
stop dbl blk tmr:             0   dbl blk tmr timeout:           0
start dbl idle tmr:          10   restart dbl idle tmr:        361
stop dbl idle tmr:            1   dbl idle tmr timeout:          9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:            0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:         0
Session wlock ovflw:          0    Global wlock ovflw:           0
Blacklisted:                561
```

Step 4 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dbl**

Displays brief information about all SIP blocked list data.

Example:

```
Device# show platform hardware qfp active feature alg statistics sip dbl

SIP dbl pool used chunk entries number: 1

 entry_id          src_addr         dst_addr         remaining_time(sec)
 a4a051e0a4a1ebd   10.74.30.189     10.74.5.30               25
```

Step 5 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip dblcfg**

Displays all SIP blocked list settings.

Example:

```
Device# show platform hardware qfp active feature alg statistics sip dblcfg

SIP dbl cfg pool used chunk entries number: 4
 dst_addr        trig_period(ms)    trig_size    block_time(sec)
 10.1.1.1              20              30             30
 10.74.5.30            1000             5             30
 192.0.2.2             60              30           2000
 198.51.100.115        20              30            388
```

Step 6 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip processor**

Displays SIP processor settings.

Example:

```
Device# show platform hardware qfp active feature alg statistics sip processor

Session:     14        Global:    189

Current global wlock count:      0
```

Step 7 **show platform hardware qfp** {**active** | **standby**} **feature alg statistics sip timer**

Displays SIP timer settings.

Example:

```
Device# show platform hardware qfp active feature alg statistics sip timer

call-proceeding:    620      call-duration:    380
```

Step 8 **debug alg** {**all** | **info** | **trace** | **warn**}

Example:

```
Device# debug alg warn
```

Enables the logging of ALG warning messages.

Configuration Examples for SIP ALG Resilience to DoS Attacks

Example: Configuring SIP ALG Resilience to DoS Attacks

```
Device# configure terminal
Device(config)# alg sip processor session max-backlog 5
Device(config)# alg sip processor global max-backlog 5
Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 destination 10.1.1.1
Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 block-time 30
Device(config)# alg sip timer call-proceeding-timeout 35
Device(config)# alg sip timer max-call-duration 90
Device(config)# end
```

Additional References for SIP ALG Resilience to DoS Attacks

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
NAT commands	IP Addressing Services Command References

Standards and RFCs

Standard/RFC	Title
RFC 4028	*Session Timers in the Session Initiation Protocol (SIP)*

MIBs

MIB	MIBs Link
	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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support