DoS 攻撃に対する SIP ALG レジリエンス

DoS 攻撃に対する SIP ALG レジリエンス機能は、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）へのサービス妨害（DoS）攻撃に対する保護を提供します。この機能は、DoS 攻撃を防ぐために、設定可能なロック制限、動的ブラックリスト、および設定可能なタイマーをサポートします。

このモジュールでは、機能と SIP アプリケーション レイヤ ゲートウェイ（ALG）に対する DoS 保護の設定方法を説明します。ネットワーク アドレス変換およびゾーンベース ポリシー ファイアウォールは、この機能をサポートしています。

DoS 攻撃に対する SIP ALG レジリエンスに関する情報

DoS 攻撃に対する SIP ALG レジリエンスの概要

DoS 攻撃に対する SIP ALG レジリエンス機能は、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）へのサービス妨害（DoS）攻撃に対する保護を提供します。この機能は、DoS 攻撃を防ぐために、設定可能なロック制限、動的ブラックリスト、および設定可能なタイマーをサポートします。この機能はネットワーク アドレス変換（NAT）およびゾーンベース ポリシー ファイアウォールによってサポートされています。

SIP は、IP データ ネットワーク上の参加者の間でリアルタイム セッションをセットアップ、変更、および終了するための、アプリケーション レベル シグナリング プロトコルです。SIP セッションには、インターネット電話の通話、マルチメディアの配布、マルチメディア会議などがあります。SIP DoS 攻撃は、ネットワークに対する大きな脅威です。

SIP DoS 攻撃のタイプを次に示します。

- SIP 登録フラッディング：登録フラッドは、多数の VoIP デバイスが同時にネットワークに登録を試みると発生します。登録メッセージの量がデバイスの容量を超過すると、一部

のメッセージは失われます。こうしたデバイスは再び登録を試行するため、輻輳が増加します。このようなネットワークの輻輳により、ユーザは一定の期間ネットワークにアクセスできない可能性があります。

- SIP INVITE フラッディング：INVITE フラッディングは、多数の INVITE メッセージがサーバに送信され、それらのメッセージのすべてをサーバが対応できなくなると発生します。攻撃レートが非常に高くなると、サーバのメモリが枯渇します。
- SIP 破損認証およびセッション攻撃：この攻撃は、攻撃者がダイジェスト認証を使用して有効なユーザの ID を推定するときに発生します。認証サーバが攻撃者の身元を確認しようとすると、検証は無視され、攻撃者は別のセッション ID を使用して新しい要求を開始します。これらの攻撃は、サーバのメモリを消費します。

SIP ALG 動的ブラックリスト

サービス妨害（DoS）攻撃の一般的な方法の 1 つは、ターゲット ネットワークを外部通信要求で飽和させ、ネットワークが正当なトラフィックに応答できなくすることです。この問題を解決するために、SIP ALG の DoS 攻撃レジリエンス機能は、設定可能なブロックリストを使用します。ブロックリストは、特定の権限、サービス、またはアクセスが拒否されているエンティティのリストです。動的ブラックリストはデフォルトで無効になっています。宛先アドレスに対する要求が、設定されたブロックリストの定義済みトリガーの基準を超えると、Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）は、これらのパケットをドロップします。

次の異常な SIP セッションパターンは、動的ブロックリストによって監視されます。

- 設定された期間内に、送信元が宛先に複数の要求を送信し、宛先から 2xx 以外（RFC 3261 に従って、200 から 299 までのステータス コードを持つすべての応答は「2xx 応答」です）の最終応答を受信する場合。
- 設定された期間に、送信元が宛先に複数の要求を送信し、宛先からまったく応答を受信しない場合。

SIP ALG ロック制限

ネットワーク アドレス変換（NAT）とファイアウォールは、どちらも Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）を使用して SIP メッセージを解析し、トークンからセッションを作成します。セッション状態を維持するために、SIP ALG はコール単位のデータ構造とレイヤ 7 データを使用して、セッションの開始時に割り当てられセッションの解除時に解放されるコール関連情報を保存します。SIP ALG がコールの終了を示すメッセージを受信しない場合、ネットワーク リソースはコール用に保持されます。

レイヤ 7 データはスレッド間で共有されるため、データにアクセスするためにロックが必要です。サービス妨害（DoS）攻撃や分散型 DoS 攻撃の発生時は、同じロックを取得するために多くのスレッドが待機するため、CPU 使用率が高くなり、システムが不安定になります。システムが不安定になることを防ぐために、ロックを待機できるスレッドの数を抑制するように制限が追加されています。SIP セッションは、要求/応答モードで確立されます。1 つの SIP コールに対して同時 SIP メッセージの数が多すぎる場合、ロック制限を超えたパケットはドロップされます。

SIP ALG タイマー

あるタイプの DoS 攻撃は、Session Initiation Protocol（SIP）サーバのリソースを枯渇させるために、SIP コールの終わりを示しません。こうしたタイプの DoS 攻撃を防ぐために、保護タイマーが追加されました。

SIP ALG の DoS 攻撃に対するレジリエンス機能は、次のタイマーを使用します。

- 応答される SIP コールの最大長を制御する、コール継続時間タイマー。
- 応答されない SIP コールの最大長を制御する、コール進行時間タイマー。

設定された最大時間を超えると、SIP アプリケーション レイヤ ゲートウェイ（ALG）は、このコールのリソースを解放し、このコールに関連する将来のメッセージは、SIP ALG によって適切に解析されないことがあります。

DoS 攻撃に対する SIP ALG レジリエンスの設定方法

DoS 攻撃に対する SIP ALG レジリエンスの設定

ネットワーク アドレス変換（NAT）およびゾーン ベース ポリシー ファイアウォールによって使用される Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）用のサービス妨害（DoS）防止パラメータを設定できます。

手順の概要

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** 時刻
8. **alg sip timer max-call-duration** 秒
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**alg sip processor session max-backlog** *concurrent-processor-usage* 例： `Device(config)# alg sip processor session max-backlog 5`	共有リソースを待機するバックログ メッセージ数に対するセッションごとの制限を設定します。
ステップ 4	**alg sip processor global max-backlog** *concurrent-processor-usage* 例： `Device(config)# alg sip processor global max-backlog 5`	すべての SIP セッションで共有リソースを待機するバックログ メッセージの最大数を設定します。
ステップ 5	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **destination** *ip-address* 例： `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 destination 10.1.1.1`	指定した宛先 IP アドレスに関するダイナミック SIP ALG ブラックリスト基準を設定します。
ステップ 6	**alg sip blacklist trigger-period** *trigger-period* **trigger-size** *minimum-events* **block-time** *block-time* [**destination** *ip-address*] 例： `Device(config)# alg sip blacklist trigger-period 90 trigger-size 30 block-time 30`	設定済みの制限を超えた場合に送信元からのパケットがブロックされる期間（秒単位）を設定します。
ステップ 7	**alg sip timer call-proceeding-timeout** 時刻 例： `Device(config)# alg sip timer call-proceeding-timeout 35`	応答を受信しない SIP コールを終了するための最大時間（秒単位）で設定します。
ステップ 8	**alg sip timer max-call-duration** 秒 例： `Device(config)# alg sip timer max-call-duration 90`	正常な SIP コールの最大コール期間（秒単位）を設定します。
ステップ 9	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DoS 攻撃に対する SIP ALG レジリエンスの確認

機能のトラブルシューティングには、次のコマンドを使用します。

手順の概要

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**}

手順の詳細

ステップ 1 enable

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 show alg sip

Session Initiation Protocol（SIP）アプリケーション レイヤ ゲートウェイ（ALG）の情報を表示します。

例：

```
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
```

ステップ 3 show platform hardware qfp {active | standby} feature alg statistics sip

Cisco Quantum Flow Processor（QFP）の SIP ALG 固有の統計情報を表示します。

例：

```
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
```

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

すべての SIP ブロックリストデータに関する概要情報を表示します。

例：

```
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
```

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

すべての SIP ブロックリストの設定が表示されます。

例：

```
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
```

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

SIP プロセッサの設定を表示します。

例：

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

Session:     14        Global:    189

Current global wlock count:      0
```

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

SIP タイマーの設定を表示します。

例：

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

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

ステップ 8 **debug alg** {**all** | **info** | **trace** | **warn**}

例：

```
Device# debug alg warn
```

ALG 警告メッセージのロギングをイネーブルにします。

DoS 攻撃に対する SIP ALG レジリエンスの設定例

例：DoS 攻撃に対する SIP ALG レジリエンスの設定

```
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
```

DoS 攻撃に対する SIP ALG レジリエンスに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
ファイアウォール コマンド	• 『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 コマンド	『IP Addressing Services Command References』

標準および RFC

標準/RFC	タイトル
RFC 4028	『*Session Timers in the Session Initiation Protocol (SIP)*』

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。