NAT およびファイアウォールに対する SIP ALG 強化

NAT およびファイアウォールに対する SIP ALG 強化機能は、既存のネットワーク アドレス変換（NAT）およびファイアウォール対応のセッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートよりも優れたメモリ管理および RFC 準拠を提供します。 この機能では、次の拡張機能が提供されます。

- すべての SIP レイヤ 7 データのローカル データベースの管理
- Via ヘッダーの処理
- 追加の SIP メソッドのロギングのサポート
- Provisional Response Acknowledgment（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の拡張機能はデフォルトで使用可能です。NAT またはファイアウォールでの追加の設定は必要ありません。

このモジュールでは、SIP ALG 拡張機能について説明し、SIP の NAT およびファイアウォール サポートをイネーブルにする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

NAT およびファイアウォールに対する SIP ALG 強化の制約事項

- セッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）では、セキュリティ機能は提供されません。
- SIP ALG は、コール ID に基づいてローカル データベースを管理します。 同じコール ID を持つ 2 つの異なるクライアントから 2 つのコールを受信したために、コール ID の重複が発生する場合がまれにあります。

NAT およびファイアウォールに対する SIP ALG 強化について

SIP の概要

セッション開始プロトコル（SIP）は、1 人または複数の参加者とのセッションを作成、変更、および終了するためのアプリケーション層コントロール（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 は HTTP のような要求/応答トランザクション モデルに基づいています。 各トランザクションは、サーバで特定のメソッドまたは関数を呼び出す 1 つの要求と 1 つ以上の応答で構成されます。

セッションの作成に使用される SIP の招待は、互換性のあるメディア タイプのセットに参加者が同意できるセッション記述を伝送しています。 SIP は、プロキシ サーバと呼ばれる要素を利用して、ユーザの所在地への要求のルーティング、サービスのためのユーザ認証および許可、プロバイダーのコールルーティング ポリシーの実装、およびユーザへの機能提供を行っています。 また、SIP には、プロキシ サーバから使用できるように、ユーザの所在地をアップロードできる登録機能があります。 SIP は複数のトランスポート プロトコルを基礎として実行されます。

アプリケーション レベル ゲートウェイ

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション層ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内のIPアドレス情報を変換するアプリケーションです。 ALG はアプリケーション層プロトコルを解釈し、ファイアウォールおよびネットワーク アドレス変換（NAT）アクションを実行するために使用されます。 これらのアクションは、ファイアウォールおよび NAT の設定に応じた次の 1 つ以上のアクションです。

- ダイナミック TCP または UDP ポートを使用したサーバ アプリケーションとの通信をクライアント アプリケーションに許可します。
- アプリケーション固有のコマンドを認識し、それらのコマンドに対するきめ細かなセキュリティ制御を提供します。
- データ交換を行う 2 台のホスト間のデータの複数のストリームまたはセッションを同期します。
- アプリケーション ペイロードで使用可能なネットワーク層アドレス情報を変換します。

ファイアウォールがピンホールを開き、NATは、アプリケーション層データ ストリームで送信元および宛先 IP アドレスを伝送しない TCP または UDP トラフィックで変換サービスを実行します。 IPアドレス情報を埋め込む特定のプロトコルまたはアプリケーションには、ALGのサポートが必要です。

SIP ALG ローカル データベース管理

セッション開始プロトコル（SIP）トランクは、SIP を使用した IP ネットワーク経由での IP PBX からサービス プロバイダーへの直接接続です。 SIP トランクには、多数の同時発生コールが存在できます。 コール セットアップ プロセス中、すべてのコールは、コールの確立に同じ制御チャネルを使用します。 複数のコールが、コール セットアップに同じ制御チャネルを使用します。 同じ制御チャネルが複数のコールで使用される場合、制御チャネル セッションに保存されているステートフル情報の信頼性が失われます。 SIP ステートフル情報は、メディア データを送信するためにクライアントおよびサーバのエンドポイントで使用されるIPアドレスやポート番号などのメディア チャネル情報で構成されます。メディア チャネル情報は、ファイアウォールおよびNATで、D チャネル用のファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアをそれぞれ作成するために使用されます。 複数のコールがコールセットアップに同じ制御チャネルを使用するため、メディア データのセットが複数存在します。

SIP トランクでは、複数のコールが同じファイアウォールおよび NAT セッションを共有します。 NAT およびファイアウォールでは、SIP パケットの 5 タプル（送信元アドレス、宛先アドレス、送信元ポート、宛先ポート、およびプロトコル）を使用して、SIPセッションを識別および管理します。 5 タプルを使用してコールを識別および照合する従来の方法では、SIP トランキングが完全にはサポートされません。そのため、多くの場合、レイヤ 7 データのメモリ リークやコールの照合の問題が発生します。

他のアプリケーション レベル ゲートウェイ（ALG）とは対照的に、SIP ALG では、通常の SIP コールおよび SIP トランクに埋め込まれている SIP コールに含まれるすべてのメディア関連情報

を保存するために、ローカルデータベースを使用してSIP レイヤ7データを管理します。 SIP ALG では、SIP メッセージに含まれる Call-ID ヘッダー フィールドを使用して、コールの照合のためにローカル データベースを検索したり、コールを管理および終了したりします。 Call-ID ヘッダー フィールドは、同じ SIP ダイアログに属するメッセージを識別するダイアログ ID です。

SIP ALG では、コール ID を使用して、ローカル データベースでの検索およびメモリ リソースの管理を行います。 SIP ALG がレイヤ 7 データ レコードをデータベースから解放できない特定のシナリオでは、データベース内にコール レコードが残っていないことを確認するために、セッション タイマーを使用してリソースが管理および解放されます。

（注） すべてのレイヤ7データはローカルデータベースを使用してSIP ALGにより管理されるため、SIP ALG が SIP レイヤ 7 データを解放するためにファイアウォールおよび NAT で応答することはありません。SIP ALG 自身がデータを解放します。 すべての NAT 変換およびファイアウォール セッションをクリアするために **clear** コマンドを使用する場合、ローカル データベース内の SIP レイヤ 7 データは解放されません。

SIP ALG Via ヘッダーのサポート

セッション開始プロトコル（SIP）INVITE 要求には、Via ヘッダー フィールドが含まれます。 Via ヘッダー フィールドは、SIP 要求が通過するトランスポート パスを示します。 Via ヘッダーには、後続の SIP 応答のリターン パスに関する情報も含まれています。これには、応答メッセージが送信される IP アドレスとポートが含まれます。

SIP ALG では、受信した各 SIP 要求の Via ヘッダー フィールドの最初の値に基づいて、ファイアウォール ピンホールまたはネットワーク アドレス変換（NAT）ドアを作成します。ただし、確認応答（ACK）メッセージは除きます。 ポート番号情報が最初の Via ヘッダーに含まれていない場合、ポート番号は 5060 と想定されます。

SIP ALG 方式のロギング サポート

NAT およびファイアウォールに対する SIP ALG 強化機能では、セッション開始プロトコル（SIP）アプリケーション レベル ゲートウェイ（ALG）統計で、次の方式の詳細ロギングをサポートします。

- PUBLISH
- OPTIONS
- 1XX（100、180、183 を除く）
- 2XX（200 を除く）

SIP ALG 統計に記録される既存の SIP 方式には、ACK、BYE、CANCEL、INFO、INVITE、MESSAGE、NOTIFY、REFER、REGISTER、SUBSCRIBE、および 1XX-6XX があります。

SIP ALG PRACK コール フロー サポート

セッション開始プロトコル（SIP）では、最終応答と暫定応答の 2 種類の応答が定義されています。最終応答では要求の処理結果が伝達され、信頼性の高い方法で送信されます。一方、暫定応答では要求処理の進行状況に関する情報が伝えられ、信頼性の高い方法では送信されません。

Provisional Response Acknowledgement（PRACK）は、暫定応答用の確認応答（ACK）システムを提供する SIP 方式です。 PRACK を使用すると、SIP エンドポイント間の SIP の暫定応答を確実に交換できます。 SIP の信頼性の高い暫定応答は、メディア情報が交換され、リソース予約がコールの接続前に実行できるようにします。

SIP は、接続ネゴシエーション中に、セッション記述プロトコル（SDP）の接続、メディア、および属性のフィールドを使用します。 SIP アプリケーション レベル ゲートウェイ（ALG）は、PRACK メッセージ内の SDP 情報をサポートします。 メディア情報が PRACK メッセージ内に存在する場合、SIP ALG はメディア情報を取得して処理します。 また、SIP ALG は後続のメディア ストリームでのメディア チャネルの作成を行います。 SIP ALG では、PRACK メッセージ内の SDP 情報に基づいて、ファイアウォール ピンホールおよび NAT ドアを作成します。

SIP ALG Record-Route ヘッダー サポート

Record-Route ヘッダー フィールドは、セッション開始プロトコル（SIP）プロキシによって SIP 要求に追加され、SIP ダイアログにおける将来の要求がプロキシ経由でルーティングされるよう強制します。 これにより、ダイアログ内で送信されるメッセージはすべての SIP プロキシを経由し、SIP 要求に Record-Route ヘッダー フィールドが追加されます。 Record-Route ヘッダー フィールドには、プロキシを識別する、グローバルに到達可能な Uniform Resource Identifier（URI）が含まれます。

SIP アプリケーション レベル ゲートウェイ（ALG）は Contact ヘッダーを解析し、Contact ヘッダー内の IP アドレスおよびポート値を使用して、ファイアウォール ピンホールおよびネットワーク アドレス変換（NAT）ドアを作成します。 さらに、SIP ALG では、プロキシ経由でルーティングされる将来のメッセージ用にファイアウォール ピンホールおよび NAT ドアを作成するための Record-Route ヘッダーの解析をサポートします。

Record-Route ヘッダーを解析することにより、SIP ALG では次のシナリオをサポートします。

- Cisco ASR 1000 アグリゲーション サービス ルータが、2 つのプロキシ間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、ユーザ エージェント クライアント（UAC）とプロキシの間に配置されます。
- Cisco ASR 1000 アグリゲーション サービス ルータが、プロキシとユーザ エージェント サーバ（UAS）の間に配置されます。
- クライアントとサーバの間にプロキシが存在しません。 このシナリオではレコードのルーティングは行われません。

NAT およびファイアウォールに対する SIP ALG 強化の設定方法

SIP に対する NAT サポートのイネーブル化

SIP に対する NAT サポートは、デフォルトでポート 5060 でイネーブルになります。 この機能がディセーブルの場合、SIP に対する NAT のサポートを再びイネーブルにするには、この作業を実行します。 SIP に対する NAT サポートをディセーブルにするには、**no ip nat service sip** コマンドを使用してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip nat service sip** {**tcp** | **udp**} **port** *port-number*
4. **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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**ip nat service sip** {**tcp**	**udp**} **port** *port-number* 例： `Device(config)# ip nat service sip tcp port 5060`	SIP に対する NAT サポートをイネーブルにします。
ステップ 4	**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。

SIP インスペクションのイネーブル化

手順の概要

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**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any sip-class1`	検査タイプ クラス マップを作成し、クラス マップ コンフィギュレーション モードを開始します。
ステップ 4	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol sip`	指定したプロトコルに基づいてクラス マップの一致基準を設定します。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `Device(config-cmap)# exit`	クラスマップ コンフィギュレーション モードを終了します。
ステップ 6	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect sip-policy`	検査タイプ ポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。
ステップ 7	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect sip-class1`	アクションを実行するクラスを指定し、ポリシー マップ クラス コンフィギュレーション モードを開始します。
ステップ 8	**inspect** 例： `Device(config-pmap-c)# inspect`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 9	**exit** 例： `Device(config-pmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了し、ポリシーマップ コンフィギュレーションモードに戻ります。
ステップ 10	**class class-default** 例： `Device(config-pmap)# class class-default`	これらのポリシー マップ設定が事前に定義したデフォルト クラスに適用されることを指定します。 • 設定済みクラスマップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 11	**end** 例： `Device(config-pmap)# end`	ポリシー マップ 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。

ゾーン ペアの設定および SIP ポリシー マップの付加

手順の概要

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**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**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	**zone security** {*zone-name*	**default**} 例： `Device(config)# zone security zone1`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**zone security** {*zone-name* | **default**} 例： `Device(config)# zone security zone2`	インターフェイスを割り当てることができるセキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**zone-pair security** *zone-pair-name* [**source** {*source-zone-name* | **self** | **default**} **destination** [*destination-zone-name* | **self** | **default**]] 例： `Device(config)# zone-pair security in-out source zone1 destination zone2`	ゾーン ペアを作成し、セキュリティ ゾーン ペア コンフィギュレーション モードに戻ります。 （注） ポリシーを適用するには、ゾーン ペアを設定する必要があります。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect sip-policy`	ファイアウォール ポリシー マップを宛先ゾーン ペアに付加します。 （注） ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone1`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。

	コマンドまたはアクション	目的
		（注） インターフェイスをセキュリティゾーンのメンバーにした場合、方向に関係なくインターフェイスを通過するすべてのトラフィック（デバイス宛のトラフィックまたはデバイス発信のトラフィックを除く）は、デフォルトでドロップされます。 トラフィックがインターフェイス通過するには、ゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。 ポリシーがトラフィックを許可すると、トラフィックはそのインターフェイスを通過できます。
ステップ 12	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 13	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/1`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 14	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security zone2`	インターフェイスを指定したセキュリティ ゾーンに割り当てます。
ステップ 15	**end** 例： `Device(config-if)# end`	インターフェイス 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。

NAT およびファイアウォールに対する SIP ALG 強化の設定例

例：SIP に対する NAT サポートのイネーブル化

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

例：SIP インスペクションのイネーブル化

```
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
```

例：ゾーン ペアの設定および SIP ポリシー マップの付加

```
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
```

NAT およびファイアウォールに対する SIP ALG 強化に関するその他の関連資料

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』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『*Security Configuration Guide: Zone-Based Policy Firewall*』
NAT コマンド	『Cisco IOS IP Addressing Services Command Reference』
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』

関連項目	マニュアル タイトル
NAT およびファイアウォール ALG サポート	『NAT and Firewall ALG and AIC Support on Cisco ASR 1000 Series Aggregation Services Routers』マトリクス

標準および RFC

標準/RFC	タイトル
RFC 3261	『*SIP: Session Initiation Protocol*』

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

NAT およびファイアウォールに対する SIP ALG 強化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *1*：*NAT* およびファイアウォールに対する *SIP ALG* 強化の機能情報

機能名	リリース	機能情報
NAT およびファイアウォールに対する SIP ALG 強化	Cisco IOS XE Release 3.8S	NAT およびファイアウォールに対する SIP ALG 強化機能では、既存の NAT およびファイアウォールに対する SIP ALG サポートよりも優れたメモリ管理および RFC 準拠を提供します。