NAT とファイアウォールの SIP ALG 強化

NAT およびファイアウォール向けの SIP ALG ハードニング機能は、ネットワーク アドレス変換（NAT）とファイアウォールの既存の Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）サポートに対して、より優れたメモリ管理と RFC 準拠性を提供します。この機能は次の点で強化されています。

- すべての SIP レイヤ 7 データ用のローカル データベースの管理
- Via ヘッダーの処理
- 追加 SIP メソッドの記録に関するサポート
- 暫定応答確認（PRACK）コール フローのサポート
- Record-Route ヘッダーのサポート

上記の機能強化はデフォルトで使用できます。NAT やファイアウォールでの追加設定は必要ありません。

このモジュールでは、SIP ALG の機能拡張について説明し、SIP に対する NAT およびファイアウォールのサポートを有効にする方法について説明します。

NAT とファイアウォールの SIP ALG 強化に関する制約事項

- Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）は、セキュリティ機能を提供しません。

- 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。2 台のクライアントからコール ID が同じ 2 つのコールが送られ、コール ID が重複するという、異常ケースが発生する場合もあるかもしれません。

NAT とファイアウォールの SIP ALG 強化に関する情報

SIP の概要

Session Initiation Protocol（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認可、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 レイヤ 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 レイヤ 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 の設定に応じて次の 1 つまたは複数のアクションになります。

- クライアント アプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバ アプリケーションと通信できるようにします。
- アプリケーション固有のコマンドを認識し、これらのコマンドに対するきめ細かいセキュリティ制御を提供します。
- データ交換を行う 2 つのホスト間の複数のデータ ストリームまたはデータ セッションを同期します。
- アプリケーション ペイロードで使用できる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、アプリケーション レイヤ データストリームの送信元 IP アドレスおよび宛先 IP アドレスを伝送しない TCP または UDP トラフィックに対する変換

サービスをNATが実行します。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

Session Initiation Protocol（SIP）トランクは、サービス プロバイダーへの IP PBX の直接接続で、SIP を使用して IP ネットワークを経由します。SIP トランクでは、多数の同時コールを実現できます。コール セットアップ プロセスの間に、すべてのコールはコール確立のため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用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と、制御チャネルセッションに保存されたステートフル情報の信頼性が低くなります。SIP ステートフル情報は、メディア データを送信するクライアントおよびサーバ 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ています。メディア チャネル情報は、ファイアウォールおよびNAT に対して、それぞれのデータ チャネルのファイアウォール ピンホールとネットワーク アドレス変換（NAT）ドアを作成するために使用されます。複数のコールがコール セットアップ用に同じ制御チャネルを使用するため、メディア データの複数のセットが存在します。

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は、SIP パケットの 5 つのタプル（送信元アドレス、宛先アドレス、発信元ポート、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 つの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は、SIP トランキングを完全にはサポートしないため、レイヤ7データのメモリ リークやコール照合の問題が発生することがよくあります。

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 はローカル データベースを使用して、通常の SIP コールおよび SIP トランクに埋め込まれた SIP コールに含まれるすべてのメディア関連の情報を保存することで、SIP レイヤ 7 データを管理します。SIP ALG は、SIP メッセージに含まれるコール ID ヘッダー フィールドを使用してローカル データベース内で一致するコールを検索し、コールを管理および終了します。コール 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識別子です。

SIP ALG は、コール ID を使用してローカル データベース内を検索し、メモリ リソースを管理します。SIP ALG がデータベースからレイヤ7データ レコードを解放できない特定の状況で、リソースの管理と解放にセッション タイマーが使用され、データベース内に停止したコール レコードが存在しないようにします。

（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たSIP ALGにより管理されるので、SIP ALG は 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 に応答しません。SIP ALG はデータを自ら解放します。**clear** コマンドを使用して、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した場合、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

Session Initiation Protocol (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 要求によって採用される転送パスを示します。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ます。その中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 は、確認応答（ACK）メッセージを除き、受信した SIP 要求の Via ヘッダー フィールド内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。最初の Via ヘッダーにポート番号情報がない場合、ポート番号は 5060 であるとみなされます。

SIP ALG メソッド ロギングのサポート

NAT およびファイアウォール向けの SIP ALG ハードニング機能は、Session Initiation Protocol（SIP）アプリケーション レベル ゲートウェイ（ALG）の統計情報で次のメソッドの詳細な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 統計情報に記録される既存の SIP メソッドには 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 フローのサポート

Session Initiation Protocol（SIP）は、最終と暫定という 2 つのタイプの応答を定義します。最終応答は、要求処理の結果を知らせるもので、確実に送信されます。一方で暫定応答は、要求処理の進行状況に関する情報を提供しますが、確実には送信されません。

暫定応答確認（PRACK）は、暫定応答の確認応答（ACK）システムを提供する SIP メソッドです。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、Session Description Protocol（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。SIP ALG はまた、後続のメディア ストリームのメディア チャネルの作成を処理します。SIP ALG 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 ヘッダーのサポート

Record-Route ヘッダー フィールドは、Session Initiation Protocol（SIP）プロキシによって SIP 要求に追加され、SIP ダイアログ内の将来の要求がプロキシを介してルーティングされることを強制します。その後、ダイアログ内で送信されるメッセージはすべての SIP プロキシを通過し、Record-Route ヘッダー フィールドが SIP 要求に追加されます。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 アドレスとポート番号を使用して、ファイアウォール ピンホールとネットワーク アドレス変換（NAT）ドアを作成します。さらに、SIP ALG は、プロキシを経由してルーティングされる将来のメッセージ用のファイアウォール ピンホールと NAT ドアを作成するために、Record-Route ヘッダーの解析をサポートします。

NAT とファイアウォールに対する SIP ALG 強化の設定方法

SIP の NAT サポートの有効化

SIP の NAT サポートは、デフォルトでポート 5060 でイネーブルになっています。この機能が無効になっている場合、SIP の NAT サポートを再びイネーブルにするには、次の作業を実行します。SIP の NAT サポートを無効にするには、**no ip nat service sip** コマンドを使用します。

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	**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。

	コマンドまたはアクション	目的
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 の NAT サポートを有効にします。
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有効化

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	**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：	名前付き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
	`Device(config-cmap)# match protocol sip`	
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 ペアの設定と SIP ポリシー マップのアタッチ

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	**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。
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。

	コマンドまたはアクション	目的
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。 （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、そのインターフェイスを通して送受信されるすべてのトラフィックは、デフォルトでドロップされます（ただしデバイス宛のトラフィックとデバイス発のトラフィックを除く）。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`	インターフェイス設定モードを終了し、グローバル設定モードに戻ります。
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。

	コマンドまたはアクション	目的
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 とファイアウォールに対する SIP ALG 強化の設定例

例：SIP サポート用の NAT の有効化

```
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有効化

```
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 ペアの設定と SIP ポリシー マップのアタッチ

```
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 とファイアウォールの SIP ALG 強化に関する追加情報

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』
NAT 設定	『*IP Addressing: NAT Configuration Guide*』
ファイアウォールの設定	『セキュリティ設定ガイド：ゾーンベース ポリシー ファイアウォール』
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』

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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。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 とファイアウォールの SIP ALG 強化に関する機能情報

表 *1 : NAT* とファイアウォールの *SIP ALG* 強化に関する機能情報

機能名	リリース	機能情報
NAT とファイアウォールの SIP ALG 強化	Cisco IOS XE リリース 3.8S	NAT とファイアウォールの SIP ALG 強化機能は、既存の NAT とファイアウォールの SIP ALG サポートでより適切なメモリ管理と RFC 準拠を可能にします。

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。