Cisco ファイアウォール SIP 機能拡張 ALG

Cisco XE ファイアウォールの強化された Session Initiation Protocol（SIP）インスペクションには、基本的な SIP 検査機能（SIP パケット インスペクションとピンホールのオープン）に加え、プロトコル準拠機能とアプリケーションセキュリティ機能があります。これらの機能拡張によって、SIP トラフィックおよび機能に適用するポリシーとセキュリティ チェックを制御し、不要なメッセージやユーザを除外できます。

Cisco IOS XE ソフトウェアで追加の SIP 機能を開発することで、Cisco Call Manage、Cisco Call Manager Express、および Cisco IP-IP Gateway ベースの音声/ビデオ システムのサポートが改善されます。また、アプリケーション レイヤ ゲートウェイ（ALG）SIP の機能拡張では、RFC 3261 とその拡張もサポートされています。

Cisco ファイアウォール SIP 拡張機能 ALG の前提条件

システムが Cisco IOS XE リリース 2.4 以降のリリースを実行している必要があります。

Cisco ファイアウォール SIP 拡張機能 ALG に関する制約事項

DNS 名前解決

SIP メソッドでは、IP アドレスを直接指定する代わりにドメイン ネーム システム（DNS）名を使用できますが、この機能は現在 DNS 名をサポートしていません。

Cisco ASR 1000 シリーズ ルータ

この機能は、Cisco ASR 1000 シリーズ ルータ上のアプリケーション インスペクションおよびコントロール（AIC）をサポートせずに実装されました。Cisco IOS XE リリース 2.4 では、次コマンドのみがサポートされています。**class-map type inspect**、**class type inspect**、**match protocol**、および **policy-map type inspect**。

Cisco ISR 4000 シリーズ ルータ

Cisco IOS XE Fuji 16.7.1 リリースは、Transport Layer Security（TLS）または Secure Real-time Transport Protocol（SRTP）をサポートしていません。

Cisco ファイアウォール SIP 拡張機能 ALG について

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。

SIP 用ファイアウォールの機能の説明

SIP 用ファイアウォールのサポート機能を使用すると、SIP シグナリング要求は、ゲートウェイ間の直接伝送によって、または複数のプロキシを介して、宛先ゲートウェイまたは電話に送信できます。最初の要求後に、Record-Route ヘッダー フィールドを使用しない場合、後続の要求は、Contact ヘッダー フィールドに指定されている宛先ゲートウェイ アドレスに直接伝送できます。そのため、ファイアウォールは、周囲のすべてのプロキシとゲートウェイを認識し、次の機能を使用できます。

- SIP シグナリング応答は、SIP シグナリング要求と同じパスを伝送できます。
- 後続のシグナリング要求は、エンドポイント（宛先ゲートウェイ）に直接伝送できます。
- メディア エンドポイントは、相互にデータを交換できます。

SIP UDP および TCP のサポート

RFC 3261 は最新の SIP の RFC であり、RFC 2543 の置き換えです。この機能は、シグナリングに SIP UDP と TCP 形式をサポートします。

SIP インスペクション

ここでは、Cisco ファイアウォール - SIP ALG 拡張機能でサポートされる展開シナリオについて説明します。

SIP 電話と CCM 間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、Cisco Call Manager または Cisco Call Manager Express と SIP 電話の間にあります。SIP 電話はファイアウォールを介して Cisco Call Manager または Cisco Call Manager Express に登録され、SIP 電話とのすべての SIP コールはファイアウォールを通過します。

SIP ゲートウェイ間の Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）の間にあります。電話は SIP ゲートウェイに直接登録されます。ファイアウォールから SIP セッションまたはトラフィックを認識するのは、異なる SIP ゲートウェイに登録された電話間で SIP コールが存在する場合のみです。シナリオによっては、IP-IP ゲートウェイをファイアウォールと同じデバイスに設定することもできます。このシナリオでは、SIP ゲートウェイ間のすべてのコールは IP-IP ゲートウェイで終端します。

ローカルの Cisco Call Manager Express とリモートの Cisco Call Manager Express/Cisco Call Manager を使用する Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールは、2 つの SIP ゲートウェイ（Cisco Call Manager、Cisco Call Manager Express、または SIP プロキシ）の間にあります。ゲートウェイの 1 つは、ファイアウォールと同じデバイスで設定されます。このゲートウェイに登録されているすべての電話は、ファイアウォールによってローカルで検査されます。また、2 つのゲートウェイ間に SIP コールがある場合、ファイアウォールによってその SIP セッションも検査されます。このシナリオでは、ファイアウォールの一方では SIP 電話がローカルで検査され、もう一方では SIP ゲートウェイが検査されます。

ローカルの Cisco Call Manager Express を使用する Cisco IOS XE ファイアウォール

Cisco IOS XE ファイアウォールと Cisco Call Manager Express は、同じデバイスで設定されます。Cisco Call Manager Express に登録されているすべての電話は、ファイアウォールによってローカルで検査されます。また、登録されている任意の電話間で行われる SIP コールも、Cisco IOS XE ファイアウォールによって検査されます。

ALG--SIP Over TCP の拡張機能

SIP が UDP を介して転送されると、すべての SIP メッセージが 1 つの UDP データグラムで送信されます。ただし、SIP が TCP を介して転送されると、1 つの TCP セグメントに複数の SIP メッセージが含まれることがあります。また、いずれかの TCP セグメント内の最後の SIP メッセージが部分的なメッセージである可能性があります。Cisco IOS XE リリース 3.5S 以前では、受信した 1 つの TCP セグメント内に複数の SIP メッセージがある場合、SIP ALG は最初のメッセージだけを解析します。解析されないデータは 1 つの不完全な SIP メッセージと見なされ、vTCP に戻されます。次の TCP セグメントを受信すると、vTCP は未処理データをそのセグメントの前に置き、それらを SIP ALG に渡すため、vTCP でバッファする必要があるデータが増えていきます。

Cisco IOS XE リリース 3.5S では、ALG--SIP over TCP 機能拡張機能により、SIP ALG は 1 つの TCP セグメント内の複数の SIP メッセージを処理できます。TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

Cisco ファイアウォール SIP 拡張機能 ALG の設定方法

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）。

	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	**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`	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。
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：	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。

	コマンドまたはアクション	目的
	`Device(config-pmap)# end`	

トラブルシューティングのヒント

SIP 対応のファイアウォール設定の問題を解決するには、次のコマンドを使用できます。

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

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）。

	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	**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。
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：	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
	`Device(config-if)# zone-member security zone1`	（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。
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。

シスコ ファイアウォール SIP 拡張機能：ALG の設定例

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
```

シスコ ファイアウォール SIP 拡張機能：ALG 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』
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』
追加の SIP 情報	『Guide to Cisco Systems VoIP Infrastructure Solution for SIP』
vTCP のサポート	*vTCP for ALG* サポート

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

Cisco ファイアウォール SIP 拡張機能：ALG に関する機能情報

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: Cisco* ファイアウォール *SIP* 拡張機能：*ALG* に関する機能情報

機能名	リリース	機能情報
ALG--SIP over TCP の拡張機能	Cisco IOS XE リリース 3.5S	ALG--SIP over TCP 拡張機能は、SIP ALG で 1 つの TCP セグメント内の複数の SIP メッセージを処理できるようにします。TCP セグメントを受信すると、このセグメント内のすべての完全な SIP メッセージは、1 つずつ解析されます。最終的に不完全なメッセージがある場合、その部分だけが vTCP に戻されます。

機能名	リリース	機能情報
Cisco ファイアウォール--SIP ALG 拡張機能	Cisco IOS XE リリース 2.4	Cisco ファイアウォール--SIP ALG 拡張機能は、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアのファイアウォール機能セットに含まれる音声セキュリティ機能を拡張します。 Cisco ASR 1000 シリーズ ルータでは、次のコマンドはレイヤ 7（アプリケーション固有）シンタックスをサポートせずに実装されました。**class type inspect, class-map type inspect**、**match protocol**、**policy-map type inspect**。
T.38 Fax Relay 用のファイアウォール --SIP ALG 拡張機能	Cisco IOS XE リリース 2.4.1	T.38 Fax Relay 用のファイアウォール--SIP ALG 拡張機能は、Cisco ASR 1000 シリーズ ルータ上の Cisco IOS XE ソフトウェアのファイアウォール機能セットに含まれる機能を拡張します。 この機能は、SIP ALG で、Cisco ASR 1000 シリーズ ルータ上のファイアウォールを通過する T.38 Fax Relay over IP をサポートできるようにします。

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。