音声とビデオのプロトコルのインスペクション

ここでは、音声とビデオのプロトコルのアプリケーションインスペクションについて説明します。特定のプロトコルに関してインスペクションを使用する必要がある理由、およびインスペクションを適用する全体的な方法については、アプリケーション レイヤ プロトコル インスペクションの準備を参照してください。

CTIQBE インスペクション

CTIQBE プロトコル インスペクションは、NAT、PAT、および双方向 NAT をサポートします。これによって、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を経由してコール セットアップを行えるようになります。

TAPI と JTAPI は、多くの Cisco VoIP アプリケーションで使用されます。CTIQBE は、Cisco TSP が Cisco CallManager と通信するために使用されます。

CTIQBE インスペクションをイネーブルにする方法については、アプリケーション レイヤ プロトコル インスペクションの設定を参照してください。

CTIQBE インスペクションの制限事項

CTIQBE コールのステートフル フェールオーバーはサポートされていません。

次に、CTIQBEアプリケーションインスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら 2 つの電話間のコールは失敗します。
- Cisco IP SoftPhone と比較して Cisco CallManager の方がセキュリティの高いインターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定することが必要なためです。
- PAT または外部 PAT を使用しているときに Cisco CallManager の IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録するためには、TCP ポート 2748 を PAT（インターフェイス）アドレスの同一ポートに対してスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されていて、Cisco CallManager、Cisco IP SoftPhone、Cisco TSP のいずれにおいてもユーザによる設定はできません。

H.323 インスペクション

H.323 インスペクションは RAS、H.225、H.245 をサポートし、埋め込まれた IP アドレスとポートをすべて変換する機能を備えています。ステートのトラッキングとフィルタリングを実行し、インスペクション機能のアクティベーションをカスケードできます。H.323 インスペクションは、電話番号のフィルタリング、T.120 のダイナミック制御、H.245 のトンネル機能制御、HSI グループ、プロトコルのステートトラッキング、H.323 通話時間制限の適用、T.38 Fax、音声/ビデオ制御をサポートします。

H.323 検査はデフォルトではイネーブルです。デフォルト以外の処理が必要な場合にのみ設定する必要があります。

ここでは、H.323 アプリケーション インスペクションについて説明します。

H.323 インスペクションの概要

H.323 インスペクションは、Cisco CallManager などの H.323 準拠のアプリケーションをサポートします。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。ASA は、H.323 v3 機能の同一コール シグナリング チャネルでの複数コールを含めて、H.323 を Version 6 までサポートします。

H.323 インスペクションをイネーブルにした場合、ASA は、H.323 Version 3 で導入された機能である同一コール シグナリング チャネルでの複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

H.323 の動作

H.323 のプロトコルのコレクションは、合計で最大 2 つの TCP 接続と 4 ～ 8 つの UDP 接続を使用できます。FastConnect は 1 つの TCP 接続だけを使用し、RAS は登録、アドミッション、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントは、最初に TCP ポート 1720 を使用して、H.323 サーバーへの TCP 接続を確立し、Q.931 コール セットアップを要求します。H.323 端末は、コール セットアップ プロセスの一部として、H.245 TCP 接続に使用するため、クライアントに 1 つのポート番号を供給します。H.323 ゲートキーパーが使用されている環境では、初期パケットは UDP を使用して送信されます。

H.323 インスペクションは、Q.931 TCP 接続をモニターして、H.245 ポート番号を決定します。H.323 端末が、FastConnect を使用していない場合は、ASA が H.225 メッセージのインスペクションに基づいて、H.245 接続をダイナミックに割り当てます。RAS を使用すると、H.225 接続もダイナミックに割り当てることができます。

各 H.245 メッセージ内で、H.323 エンドポイントが、後続の UDP データ ストリームに使用するポート番号を交換します。H.323 インスペクションは、H.245 メッセージを調査して、ポート番号を識別し、メディア交換用の接続をダイナミックに作成します。RTP はネゴシエートされたポート番号を使用し、RTCP はその次に高いポート番号を使用します。

H.323 制御チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 インスペクションでは、次のポートが使用されます。

- 1718：ゲートキーパー検出 UDP ポート
- 1719：RAS UDP ポート
- 1720：TCP 制御ポート

RAS シグナリング用に予約済み H.323 ポート 1719 のトラフィックを許可する必要があります。さらに、H.225 コール シグナリング用に、予約済み H.323 ポート 1720 のトラフィックを許可する必要があります。ただし、H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーの使用時、ASA は、ACF メッセージと RCF メッセージのインスペクションに基づいて H.225 接続を開きます。

H.225 メッセージを検査した後、ASA は H.245 チャネルを開き、H.245 チャネルで送信されるトラフィックも検査します。ASA を通過するすべての H.245 メッセージは、H.245 アプリケーション インスペクションを受けます。このインスペクションでは、埋め込み IP アドレスが変換され、H.245 メッセージでネゴシエートされたメディア チャネルが開かれます。

H.323 インスペクションを通過するパケットが通る各 UDP 接続は H.323 接続としてマークされ、**timeout** コマンドで設定された H.323 タイムアウト値でタイムアウトします。

（注） Gatekeeper がネットワーク内にある場合は、H.323 エンドポイント間のコール セットアップをイネーブルにできます。ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。デフォルトでは、このオプションは無効になっています。H.323 エンドポイント間のコール セットアップをイネーブルにするには、H.323 インスペクション ポリシー マップの作成時に、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes enable** コマンドを入力します。

H.245 メッセージでの H.239 サポート

ASA は、2 つの H.323 エンドポイントの間に存在します。2 つの H.323 エンドポイントが、スプレッドシート データなどのデータ プレゼンテーションを送受信できるようにテレプレゼンテーション セッションをセットアップするとき、ASA はエンドポイント間で H.239 ネゴシエーションが成功することを保証します。

H.239 は、H.300 シリーズ エンドポイントが 1 回のコールで追加ビデオ チャネルを開くことができる機能を提供する規格です。コールで、エンドポイント（ビデオ電話など）はビデオ用チャネルとデータ プレゼンテーション用チャネルを送信します。H.239 ネゴシエーションは H.245 チャネルで発生します。

ASA が追加メディア チャネル用とメディア制御チャネル用のピンホールを開きます。エンドポイントは、オープン論理チャネル メッセージ（OLC）を使用して新しいチャネルの作成を通知します。メッセージ拡張は H.245 バージョン 13 の一部です。

テレプレゼンテーション セッションの復号化と符号化は、デフォルトでイネーブルにされています。H.239 の符号化と復号化は ASN.1 コーダによって実行されます。

H.323 インスペクションの制限事項

H.323 インスペクションは、Cisco Unified Communications Manager（CUCM）7.0 でテストおよびサポートされています。CUCM 8.0 以降ではサポートされません。H.323 インスペクションは、他のリリースや製品で機能する場合があります。

H.323 アプリケーション インスペクションの使用に関して、次の既知の問題および制限があります。

- PAT は拡張 PAT または per-session PAT を除きサポートされます。
- スタティック PAT は、H.323 メッセージのオプション フィールドに埋め込まれた IP アドレスを正しく変換できないことがあります。この問題が発生した場合は、H.323 でスタティック PAT を使用しないでください。

- 同じセキュリティ レベルのインターフェイス間の NAT ではサポートされません。
- NAT64 ではサポートされません。
- H.323 インスペクションを使用する NAT は、エンドポイントで直接実行される場合には、NAT と互換性がありません。エンドポイントで NAT を実行する場合、H.323 インスペクションは無効にしてください。

H.323 インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、H.323 インスペクション ポリシー マップを作成して H.323 インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、H.323 インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect h323** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。**match-any** キーワードは、トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して発信側を照合します。
- **match** [**not**] **media-type** {**audio** | **data** | **video**}：メディア タイプを照合します。

ステップ 2 H.323 インスペクション ポリシー マップを作成します。**policy-map type inspect h323** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法を参照してください。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- H.323 クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- H.323 クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop** [**log**]：パケットをドロップします。メディア タイプの照合の場合、**log** キーワードを含めてシステム ログ メッセージを送信できます。
- **drop-connection**：パケットをドロップし、接続を閉じます。このオプションは、着信側または発信側の照合に使用できます。
- **reset**：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。このオプションは、着信側または発信側の照合に使用できます。

ステップ 5 インスペクションエンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **ras-rcf-pinholes enable**：H.323 エンドポイント間のコール セットアップをイネーブルにします。Gatekeeperがネットワーク内にある場合は、H.323エンドポイント間のコール セットアップをイネーブルにできます。RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くには、このオプションを使用します。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。デフォルトでは、このオプションは無効になっています。
- **timeout users** *time*：H.323 コールの制限時間（hh: mm: ss 形式）を設定します。タイムアウトを付けない場合は、00:00:00 を指定してください。範囲は、0:0:0 ～ 1193:0:0 です。
- **call-party-number**：コール設定時に発信側の番号を強制的に送信します。
- **h245-tunnel-block action** {**drop-connection** | **log**}：H.245 トンネル ブロッキングを適用します。接続をドロップするか、単にログに記録するだけかを選択します。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **state-checking** {**h225** | **ras**}：ステート チェック検証をイネーブルにします。個別にコマンドを入力して、H.225およびRASのステート チェックをイネーブルにすることができます。
- **early-message** *message_type*：H.225 SETUP メッセージの前に指定したタイプの H.225 メッセージを許可するかどうか。H.460.18 に従って、**facility** メッセージが早く到着するように許可できます。

  H.323/H.225 を使用するときに、接続が完了前に終了するコール セットアップの問題が発生した場合、このコマンドを使用して早期メッセージを許可します。また、必ず H.323 RAS と H.225 の両方にインスペクションをイネーブルにしてください（デフォルトではどちらもイネーブルになっています）。

ステップ 6 パラメータ コンフィギュレーション モードのままで、HSI グループを設定できます。

a) HSI グループを定義し、HSI グループ コンフィギュレーション モードを開始します。
hsi-group *id*

id には、HSI グループ ID を指定します。範囲は 0 ～ 2147483647 です。

b) IP アドレスを使用して HSI を HSI グループに追加します。**hsi** *ip_address*

HSI グループあたり最大 5 つのホストを追加できます。

c) HSI グループにエンドポイントを追加します。**endpoint** *ip_address if_name*

ip_address には追加するエンドポイント、*if_name* にはエンドポイントを ASA に接続するときに使用するインターフェイスを指定します。HSI グループあたり最大 10 個のエンドポイントを追加できます。

例

次の例は、電話番号のフィルタリングを設定する方法を示しています。

```
hostname(config)# regex caller 1 “5551234567”
hostname(config)# regex caller 2 “5552345678”
hostname(config)# regex caller 3 “5553456789”

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

MGCP インスペクション

MGCP インスペクションは、デフォルトのインスペクション ポリシーでイネーブルになっていないため、このインスペクションが必要な場合はイネーブルにする必要があります。ただし、デフォルトの inspect クラスにはデフォルトの MGCP ポートが含まれているので、デフォルトのグローバル インスペクション ポリシーを編集するだけで MGCP インスペクションを追加できます。または、たとえばインターフェイス固有のポリシーなど、必要に応じて新しいサービス ポリシーを作成することもできます。

ここでは、MGCP アプリケーション インスペクションについて説明します。

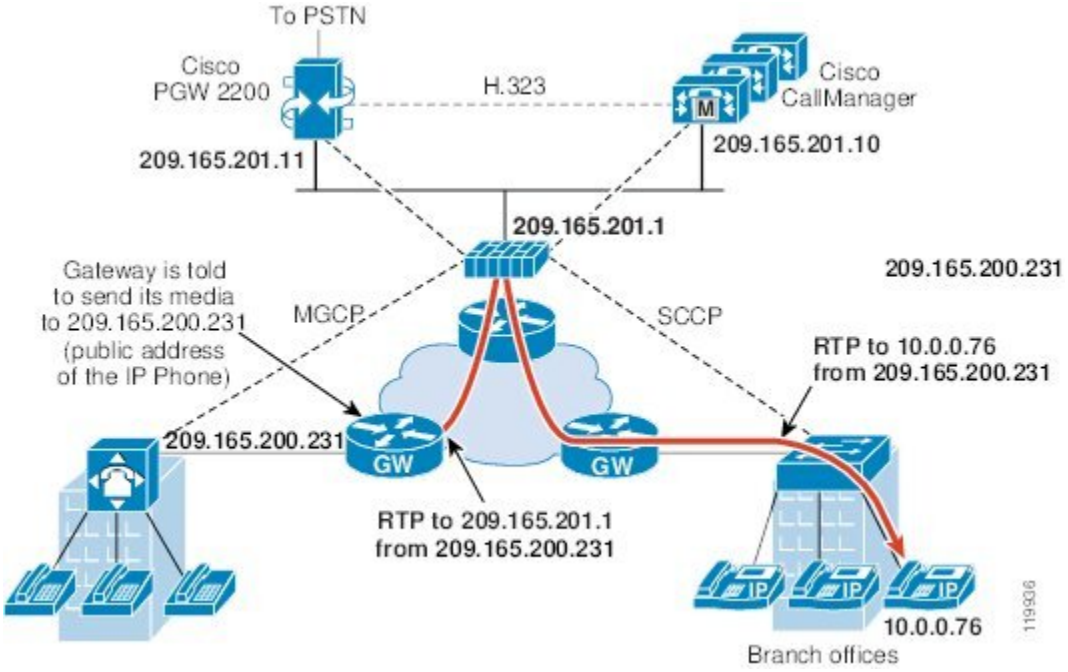
MGCP インスペクションの概要

MGCP は、メディア ゲートウェイ コントローラまたはコールエージェントと呼ばれる外部コール制御要素からメディアゲートウェイを制御するために使用されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブルモデムやケーブルセットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネス ゲートウェイ。従来のデジタル PBX（構内交換機）インターフェイスまたは統合 soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。次の図は、NAT と MGCP を使用する方法を示しています。

図 *1: NAT* と *MGCP* の使用



MGCP エンドポイントは、物理または仮想のデータ送信元および宛先です。メディア ゲートウェイには、他のマルチメディア エンドポイントとのメディア セッションを確立して制御するために、コール エージェントが接続を作成、変更、および削除できるエンドポイントが含まれています。また、コール エージェントは、特定のイベントを検出してシグナルを生成するようにエンドポイントに指示できます。エンドポイントは、サービス状態の変化を自動的にコール エージェントに伝達します。

- 通常、ゲートウェイは UDP ポート 2427 をリッスンしてコール エージェントからのコマンドを受信します。
- コール エージェントがゲートウェイからのコマンドを受信するポート。通常、コール エージェントは UDP ポート 2727 をリッスンしてゲートウェイからコマンドを受信します。

（注） MGCP インスペクションでは、MGCP シグナリングと RTP データで異なる IP アドレスを使用することはサポートされていません。一般的かつ推奨される方法は、ループバック IP アドレスや仮想 IP アドレスなどの復元力のある IP アドレスから RTP データを送信することです。ただし、ASA は、MGCP シグナリングと同じアドレスから RTP データを受信する必要があります。

MGCP インスペクション ポリシー マップの設定

ASA がピンホールを開く必要のあるコール エージェントとゲートウェイがネットワークに複数ある場合は、MGCP マップを作成します。作成した MGCP マップは、MGCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1 MGCP インスペクション ポリシー マップを作成します。**policy-map type inspect mgcp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

ステップ 4 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **call-agent** *ip_address group_id*：1 つ以上のゲートウェイを管理できるコール エージェント グループを設定します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ group_id を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。group_id オプションには、0 ～ 4294967295 の数字を指定します。ip_address オプションには、コール エージェントの IP アドレスを指定します。

  （注）
  MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、ASA を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

- **gateway** *ip_address group_id*：特定のゲートウェイを管理しているコール エージェントのグループを指定します。ip_address オプションを使用して、ゲートウェイの IP アドレスを指定します。group_id オプションには 0 ～ 4294967295 の数字を指定します。この数字は、ゲートウェイを管理しているコール エージェントの group_id に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

- **command-queue** *command_limit*：MGCP コマンド キューで許容されるコマンドの最大数（1 ～ 2147483647）を設定します。デフォルトは 200 です。

例

次の例は、MGCP マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

次のタスク

マップを使用するためのインスペクションポリシーを設定できるようになりました。「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

RTSP インスペクション

RTSP インスペクションはデフォルトでイネーブルになっています。デフォルト以外の処理が必要な場合にのみ設定する必要があります。ここでは、RTSP アプリケーション インスペクションについて説明します。

RTSP インスペクションの概要

RTSP インスペクション エンジンを使用することにより、ASA は RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注） Cisco IP/TV では、RTSP TCP ポート 554 および 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP 制御チャネルは、クライアント上で設定されているトランスポート モードに応じて、音声/ビデオ トラフィックの送信に使用されるデータ チャネルのネゴシエーションに使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA は、ステータス コード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合、サーバーは ASA との相対位置関係で外部に存在するこ

とになるため、サーバーから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージがアウトバウンド方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RTSP インスペクションは、PAT またはデュアル NAT をサポートしていません。また、ASA は、RTSP メッセージが HTTP メッセージ内に隠される HTTP クローキングを認識できません。

RealPlayer 設定要件

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバーからクライアントに、またはその逆に access-list コマンドを追加します。RealPlayer の場合、[Options] > [Preferences] > [Transport] > [RTSP Settings] をクリックして転送モードを変更します。

RealPlayer で TCP モードを使用する場合は、[Use TCP to Connect to Server] チェックボックスおよび [Attempt to use TCP for all content] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合、[Use TCP to Connect to Server] および [Attempt to use UDP for static content] チェックボックスをオンにします。マルチキャストでの使用ができないライブ コンテンツについては、ASA で、inspect rtsp コマンドを追加します。

RSTP インスペクションの制限事項

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化できますが、ASA ではフラグメント化されたパケットに対して NAT を実行することはできません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバが内部ネットワークにあるときにだけ NAT を使用できます。

RTSP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、RTSP インスペクション ポリシー マップを作成して RTSP インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順に従って、RTSP インスペクションのクラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect rtsp** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。**match-any** キーワードは、トラフィックが少なくとも基準の 1 つに一致したらクラス マップと一致することを指定します。CLI がクラスマップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **request-method** *method*：RTSP 要求方式を照合します。要求方式は、announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown です。
- **match** [**not**] **url-filter regex** {*regex_name* | **class** *class_name*}：指定した正規表現または正規表現クラスに対して URL を照合します。

ステップ 2 RTSP インスペクション ポリシー マップを作成します。**policy-map type inspect rtsp** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- RTSP クラス マップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- RTSP クラス マップで記述された **match** コマンドの 1 つかを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop-connection** [**log**]：パケットをドロップし、接続を閉じ、任意でシステム ログ メッセージを送信します。このオプションは、URL のマッチングに使用できます。
- **log**：システム ログ メッセージを送信します。
- **rate-limit** *message_rate*：1 秒あたりのメッセージのレートを制限します。このオプションは、要求方式の照合に使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **reserve-port-protect**：メディア ネゴシエーション中の予約ポートの使用を制限します。

- **url-length-limit** *bytes*：メッセージで使用できる URL の長さを 0 ～ 6000 バイトで設定します。

例

次の例は、RTSP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global
```

次のタスク

マップを使用するためのインスペクションポリシーを設定できるようになりました。「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

SIP インスペクション

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーションセキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インスペクションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにする

ためにTLSプロキシを設定する場合にのみ設定する必要があります。ここでは、SIPインスペクションについてより詳細に説明します。

SIP インスペクションの概要

IETF で定義されている SIP により、特に 2 者間の音声会議などのコール処理セッションまたは「コール」が使用可能になります。SIP はSDP と連携して通話処理を行います。SDP は、メディア ストリーム用のポートを指定します。SIP を使用することにより、ASA はSIP VoIP ゲートウェイおよび VoIP プロキシ サーバーをサポートできます。SIP と SDP の定義は、次の RFC に記載されています。

- SIP：Session Initiation Protocol、RFC 3261
- SDP：Session Description Protocol、RFC 2327

ASA経由のSIPコールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザーデータ部分に IP アドレスを埋め込みます。ASA がサポートする SIP 要求 URI の最大長は 255 であることに注意してください。

インスタントメッセージング（IM）アプリケーションでは、SIP拡張機能（RFC 3428で定義されている）およびSIP固有のイベント通知（RFC 3265 で定義されている）も使用します。ユーザーがチャット セッション（登録/サブスクリプション）を開始した後、ユーザーが互いにチャットするときに、IM アプリケーションでは、MESSAGE/INFO 方式 202 Accept 応答を使用します。たとえば、2 人のユーザーはいつでもオンラインになる可能性がありますが、何時間もチャットをすることはありません。そのため、SIP インスペクション エンジンは、設定されているSIP タイムアウト値に従ってタイムアウトするピンホールを開きます。この値は、登録継続時間よりも 5 分以上長く設定する必要があります。登録継続時間は Contact Expires 値で定義し、通常 30 分です。

MESSAGE/INFO 要求は、通常、ポート 5060 以外の動的に割り当てられたポートを使用して送信されるため、SIP インスペクション エンジンを通過する必要があります。

（注） SIP インスペクションは、チャット機能のみをサポートします。ホワイトボード、ファイル転送、アプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

SIP インスペクションの制限事項

SIP インスペクションは、Cisco Unified Communications Manager（CUCM）7.0、8.0、8.6、および10.5 でテストされ、サポートされています。CUCM 8.5 または 9.x.ではサポートされません。SIP インスペクションは、他のリリースや製品で機能する場合があります。

SIP 電話機が Call Manager に接続していないことを確認したら、次の CLI コマンドを使用して未処理の TCP セグメントの最大数を増やすことができます。**sysopt connection tcp-max-unprocessed-seg** *6-24*。デフォルトは 6 であるため、より大きな数値を試してください。

SIP インスペクションは、T.38 MIME インターネット ファクシミリ プロトコル （IFP） をサポートしていません。SIP インスペクションは、T.38 MIME オーディオ サブタイプを使用する SIP 招待をドロップします。このタイプを許可する必要がある場合は、SIP インスペクションを無効にして、RTP ストリームを許可するアクセス コントロール ルールを作成します。

SIP インスペクションの NAT 制限事項

- SIP インスペクションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス（「trying」応答メッセージの SIP ヘッダー内の「from」）は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。
- セキュリティ レベルが同じインターフェイス、または低セキュリティ レベル（送信元）から高セキュリティ レベル（宛先）に至るインターフェイスに対しては NAT または PAT を設定しないでください。この設定はサポートされません。
- 対象となるトラフィック クラス （つまり、inspection_default 以外のトラフィック クラス）に SIP インスペクションを設定する場合は、双方向 ACL を使用し、5060 宛先ポートのみを指定するようにしてください。そうしないと、IP パケットが正しく変換されても、SIP ヘッダーの IP アドレスが変換されない NAT の問題が発生する可能性があります。
- SIP 招待の VIA ヘッダーにマッピングアドレスをハードコーディングする場合は、SIP インスペクションを有効にしないでください。静的 NAT を使用して送信元クライアントアドレスを変換し、デフォルトルートのインターフェイスがクライアントの使用する接続ルートのインターフェイスと異なる場合、問題が発生する可能性があります。

SIP インスペクションの PAT 制限事項

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバが外部ネットワークにある。
  - エンドポイントからプロキシ サーバに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者/作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プ

ロトコルの制限によるものです。PAT では、変換するためにポートが必要なので、変換は失敗します。

- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

デフォルトの SIP インスペクション

SIP インスペクションはデフォルトでイネーブルになっており、次を含むデフォルトのインスペクション ポリシー マップを使用します。

- SIP インスタント メッセージ（IM）の拡張機能：イネーブル
- SIP トラフィック以外の SIP ポート使用：禁止。
- サーバとエンドポイントの IP アドレスの非表示：ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
- 1 以上の宛先ホップ カウントを保証：イネーブル
- RTP 準拠：適用強制しない
- SIP 準拠：ステート チェックとヘッダー検証を実行しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP インスペクション ポリシー マップの設定

ネットワークに対してデフォルトのインスペクション動作が十分でない場合は、SIP インスペクション ポリシー マップを作成して SIP インスペクションのアクションをカスタマイズできます。

始める前に

一部のトラフィック照合オプションでは、照合のために正規表現を使用します。これらのテクニックの 1 つを使用する場合は、最初に正規表現または正規表現のクラス マップを作成します。

手順

ステップ 1 （任意）次の手順を実行して、SIP インスペクション クラス マップを作成します。

クラスマップは複数のトラフィックとの照合をグループ化します。または、**match** コマンドを直接ポリシー マップに指定できます。クラス マップを作成することとインスペクション ポリシー マップでトラフィックとの照合を直接定義することの違いは、クラス マップでは複雑な照合基準を作成でき、クラス マップを再利用できるということです。

クラス マップと照合しないトラフィックを指定するには、**match not** コマンドを使用します。たとえば、**match not** コマンドで文字列「example.com」を指定すると、「example.com」が含まれるすべてのトラフィックはクラス マップと照合されません。

このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップでトラフィックに対して実行するアクションを指定します。

match コマンドごとに異なるアクションを実行する場合、ポリシーマップに直接トラフィックを特定する必要があります。

a) クラス マップを作成します。**class-map type inspect sip** [**match-all** | **match-any**] *class_map_name*

class_map_name には、クラス マップの名前を指定します。**match-all** キーワードはデフォルトです。トラフィックがクラスマップと一致するには、すべての基準と一致する必要があることを指定します。match-anyキーワードは、トラフィックが少なくとも1つの **match** ステートメントと一致したらクラス マップと一致することを指定します。CLI がクラス マップ コンフィギュレーション モードに入り、1 つ以上の **match** コマンドを入力できます。

b) （任意）クラス マップに説明を追加します。**description** *string*

string には、クラス マップの説明を 200 文字以内で指定します。

c) 次のいずれかの **match** コマンドを使用して、アクションを実行するトラフィックを指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

- **match** [**not**] **called-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、To ヘッダーで指定された着信側を照合します。
- **match** [**not**] **calling-party regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して、From ヘッダーで指定された発信側を照合します。
- **match** [**not**] **content length gt** *bytes*：SIP ヘッダーのコンテンツの長さが指定されたバイト数（0 ～ 65536）を超えているメッセージを照合します。
- **match** [**not**] **content type** {**sdp** | **regex** {*regex_name* | **class** *class_name*}：コンテンツ タイプを SDP として、または指定された正規表現または正規表現クラスに対して照合します。
- **match** [**not**] **im-subscriber regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP IM サブスクライバを照合します。
- **match** [**not**] **message-path regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対して SIP via ヘッダーを照合します。

- **match** [**not**] **request-method** *method*：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update の SIP 要求方式を照合します。
- **match** [**not**] **third-party-registration regex** {*regex_name* | **class** *class_name*}：指定された正規表現または正規表現クラスに対してサードパーティ登録の要求者を照合します。
- **match** [**not**] **uri {sip | tel} length gt** *bytes*：指定された長さ（0 ～ 65536 バイト）を超えている、選択したタイプ（SIP または TEL）の SIP ヘッダーの URI を照合します。

d) クラス マップ コンフィギュレーション モードを終了するには、「**exit**」と入力します。

ステップ 2 SIP インスペクション ポリシー マップを作成します。**policy-map type inspect sip** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 3 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 4 一致したトラフィックにアクションを適用するには、次の手順を実行します。

a) 次のいずれかの方法を使用して、アクションを実行するトラフィックを指定します。

- SIP クラスマップを作成した場合は、次のコマンドを入力してそれを指定します。**class** *class_map_name*
- SIP クラス マップで記述された **match** コマンドの 1 つを使用して、ポリシー マップでトラフィックを直接指定します。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

b) 次のコマンドのいずれかを入力して、一致するトラフィックに対して実行するアクションを指定します。

- **drop**：一致するすべてのパケットをドロップします。
- **drop-connection**：パケットをドロップし、接続を閉じます。
- **reset**：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。
- **log**：システム ログ メッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。
- **rate-limit** *message_rate*：メッセージのレートを制限します。レート制限は、「invite」および「register」に一致する要求方式の場合にのみ使用できます。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。**class** コマンドと **match** コマンドの順序については、複数のトラフィック クラスの処理方法を参照してください。

ステップ 5 インスペクション エンジンに影響のあるパラメータを設定するには、次の手順を実行します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **im**：インスタント メッセージングをイネーブルにします。
- **ip-address-privacy**：IPアドレスのプライバシーをイネーブルにし、サーバーとエンドポイントの IP アドレスを非表示にします。
- **max-forwards-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：これにより、宛先に到達するまで0にすることができないMax-Forwardsヘッダーの値がチェックされます。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **software-version action** {**mask [log]** | **log**}：Server および User-Agent（エンドポイント）ヘッダー フィールドを使用するソフトウェア バージョンを識別します。SIP メッセージのソフトウェア バージョンをマスクしてオプションでロギングするか、単にロギングのみ実行することができます。
- **state-checking action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：状態遷移チェックをイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **strict-header-validation action** {**drop** | **drop-connection** | **reset** | **log**} [**log**]：RFC 3261 に従って SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにします。また、不適合なトラフィックに対して実行するアクション（パケットのドロップ、接続のドロップ、リセット、またはログ）と、ロギングをイネーブルまたはディセーブルのどちらにするかを選択する必要もあります。
- **traffic-non-sip**：既知の SIP シグナリング ポートで SIP 以外のトラフィックを許可します。
- **trust-verification-server ip** *ip_address*：信頼検証サービス サーバーを指定します。信頼検証サービス サーバーは、HTTPS の確立時に Cisco Unified IP Phone がアプリケーション サーバーを認証できるようにします。最大 4 回コマンドを入力して 4 つのサーバーを指定できます。SIP インスペクションは登録された電話機ごとに各サーバーに対するピンホールを開き、電話機はどれを使用するかを決定します。CUCM サーバーで信頼検証サービス サーバーを設定します。

- **trust-verification-server port** *number*：信頼検証サービス ポートを指定します。デフォルト ポートは 2445 です。したがって、サーバーが異なるポートを使用する場合にのみ、このコマンドを使用します。使用できるポートの範囲は 1026 ～ 32768 です。
- **uri-non-sip action** {**mask [log]** | **log**}：Alert-Info および Call-Info ヘッダー フィールドにある SIP 以外の URI を識別します。SIP メッセージの情報をマスクしてオプションでロギングするか、単にロギングのみ実行することができます。

例

次の例は、SIP を使用したインスタント メッセージをディセーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

次の例は、4 つの信頼検証サービス サーバーを識別する例を示します。

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

Skinny（SCCP）インスペクション

SCCP（Skinny）アプリケーション インスペクションでは、パケット データ、ピンホールの動的開放に埋め込まれている IP アドレスとポート番号を変換します。また、追加のプロトコル準拠チェックと基本的なステート トラッキングも行います。

SCCP インスペクションはデフォルトではイネーブルです。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。

ここでは、SCCP アプリケーション インスペクションについて説明します。

SCCP インスペクションの概要

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager と併用すると、SCCP クライアントは、H.323 準拠端末と同時使用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバーの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注） ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べて高セキュリティ インターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングはスタティックである必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリにより、セキュリティの高いインターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。

Cisco IP Phone では、TFTP サーバにアクセスして、Cisco CallManager サーバに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバに接続する必要があります。TFTP サーバに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバーおよび Cisco CallManager と比べてセキュリティの高いインターフェイス上にある場合、Cisco IP Phone が接続を開始できるようにするために、ACL やスタティック エントリは必要ありません。

SCCP インスペクションの制限事項

SCCP インスペクションは、Cisco Unified Communications Manager（CUCM）7.0、8.0、8.6、および 10.5 でテストされ、サポートされています。CUCM 8.5 または 9.x.ではサポートされません。SCCP インスペクションは、他のリリースや製品で機能する場合があります。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、ASA は TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注） ASA は、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

デフォルトの SCCP インスペクション

SCCP インスペクションは、次のデフォルト値を使用してデフォルトでイネーブルになっています。

- 登録：適用強制しない
- メッセージの最大 ID：0x181
- プレフィックスの長さの最小値：4
- メディア タイムアウト：00:05:00
- シグナリング タイムアウト：01:00:00
- RTP 準拠：適用強制しない

Skinny（SCCP）インスペクション ポリシー マップの設定

メッセージがパラメータに違反したときのアクションを指定するには、SCCP インスペクション ポリシー マップを作成します。作成したインスペクション ポリシー マップは、SCCP インスペクションをイネーブルにすると適用できます。

手順

ステップ 1 SCCP インスペクション ポリシー マップを作成します：**policy-map type inspect skinny** *policy_map_name*

policy_map_name には、ポリシー マップの名前を指定します。CLI はポリシー マップ コンフィギュレーション モードに入ります。

ステップ 2 （任意）説明をポリシー マップに追加します。**description** *string*

ステップ 3 （任意）SCCP メッセージのステーション メッセージ ID フィールドに基づいてトラフィックをドロップします。

a) 0x0 ～ 0xffff の 16 進数のステーション メッセージ ID の値に基づいてトラフィックを識別します。**match** [**not**] **message-id** コマンドを使用して、単一の ID または ID の範囲を指定できます。**match not** コマンドを使用すると、**match not** コマンドの基準に一致しないすべてのトラフィックにアクションが適用されます。

match message-id {*value* | **range** *start_value end_value*}

例：

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

b) 一致したパケットに対して実行するアクションを指定します。パケットをドロップし、必要に応じてログに記録できます。**drop** [**log**]

c) ドロップするすべてのメッセージ ID を指定するまで、このプロセスを繰り返します。

ステップ 4 インスペクション エンジンに影響するパラメータを設定します。

a) パラメータ コンフィギュレーション モードを開始します。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 1 つまたは複数のパラメータを設定します。次のオプションを設定できます。オプションをディセーブルにするには、コマンドの **no** 形式を使用してください。

- **enforce-registration**：コールを発信する前に強制的に登録を実行します。
- **message-ID max** *hex_value*：許可される最大 SCCP ステーション メッセージ ID を設定します。メッセージ ID は 16 進数で指定します。デフォルトの最大値は 0x181 です。
- **rtp-conformance** [**enforce-payloadtype**]：ピンホール上を流れる RTP パケットのプロトコル準拠をチェックします。オプションの enforce-payloadtype キーワードを指定すると、シグナリング交換に基づいてペイロード タイプを強制的に音声やビデオにします。
- **sccp-prefix-len** {**max** | **min**} *length*：許可される最大または最小の SCCP プレフィックスの長さを設定します最小値と最大値の両方を設定するには、このコマンドを 2 回入力します。デフォルトの最小値は 4 で、デフォルトの最大値はありません。
- **timeout** {**media** | **signaling**} *time*：メディアおよびシグナリング接続のタイムアウトを設定します（hh: mm: ss 形式）。タイムアウトを設定しない場合は、番号に 0 を指定

します。デフォルトのメディア タイムアウトは 5 分、デフォルトのシグナリング タイムアウトは 1 時間です。

例

次の例は、SCCP インスペクション ポリシー マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

次のタスク

マップを使用するためのインスペクション ポリシーを設定できるようになりました。「アプリケーション レイヤ プロトコル インスペクションの設定」を参照してください。

STUN インスペクション

RFC 5389 で定義されている Session Traversal Utilities for NAT（STUN）は、プラグインが不要になるように、ブラウザベースのリアルタイム コミュニケーション用に WebRTC クライアントによって使用されます。WebRTC クライアントは、多くの場合、クラウド STUN サーバを使用してパブリック IP アドレスおよびポートを学習します。WebRTC は、Interactive Connectivity Establishment（ICE、RFC 5245）を使用してクライアント間の接続を確認します。これらのクライアントは、TCP やその他のプロトコルを使用することもできますが、通常、UDP を使用します。

ファイアウォールは、多くの場合、発信 UDP トラフィックをブロックするため、Cisco Spark などの WebRTC 製品が接続を完了できないことがあります。STUN インスペクションでは、STUN エンドポイント用のピンホールが開かれ、STUN と ICES の基本コンプライアンスが適用されます。これにより、両側で接続チェックが確認応答された場合にクライアントの通信が許可されます。このため、これらのアプリケーションをイネーブルにするためにアクセスルールで新しいポートを開く必要がなくなります。

デフォルトのインスペクション クラスで STUN インスペクションをイネーブルにすると、STUN トラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。

STUN インスペクションには NAT に関するいくつかの制限があります。WebRTC トラフィックについては、スタティック NAT/PAT44 がサポートされます。Cisco Spark はピンホールを必要としないので、Spark は追加のタイプの NAT をサポートできます。また、ダイナミック NAT/PAT を含む NAT/PAT64 を Cisco Spark で使用することもできます。

ピンホールが複製されるとき、STUN インスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN 要求の受信後にノードに障害が発生し、別のノードが STUN 応答を受信した場合、STUN 応答はドロップされます。

（注） STUN インスペクションでは、要求と応答を照合するためにトランザクション ID が使用されます。デバッグを使用して接続のドロップをトラブルシューティングする場合は、システムがデバッグ出力の ID の形式（エンディアンネス）を変更するため、pcap で表示される ID と直接比較されないことに注意してください。

STUN インスペクションのイネーブル化の詳細については、アプリケーション レイヤ プロトコル インスペクションの設定 を参照してください。

音声とビデオのプロトコル インスペクションの履歴

機能名	リリース	機能情報
SIP、SCCP、および TLS プロキシでの IPv6 のサポート	9.3(1)	SIP、SCCP、および TLS プロキシ（SIP または SCCP を使用）を使用している場合、IPv6 トラフィックを検査できるようになりました。 変更されたコマンドはありません。
SIP での信頼検証サービス、NAT66、CUCM 10.5、およびモデル 8831 電話機のサポート。	9.3(2)	SIP インスペクションで信頼検証サービス用サーバを設定できるようになりました。NAT66 も使用できます。SIP インスペクションは CUCM 10.5 でテスト済みです。 **trust-verification-server** パラメータ コマンドが追加されました。
複数のコアを搭載した ASA での SIP インスペクションのパフォーマンスが向上。	9.4(1)	複数のコアで ASA を通過する SIP シグナリングチングが複数存在する場合の SIP インスペクション パフォーマンスが向上しました。ただし、TLS、電話、または IME プロキシを使用する場合、パフォーマンスの向上は見られません。 変更されたコマンドはありません。

機能名	リリース	機能情報
ASA クラスタリングでの SIP インスペクションのサポート	9.4(1)	ASA クラスタで SIP インスペクションを設定できます。制御フローは、任意のユニットで作成できますが（ロード バランシングのため）、その子データ フローは同じユニットに存在する必要があります。TLS プロキシ設定はサポートされていません。 **show ssh sessions detail** コマンドが導入されました。
電話プロキシおよびUC-IME プロキシに対する SIP インスペクションのサポートが削除されました。	9.4(1)	SIP インスペクションを設定する際、電話プロキシまたはUC-IME プロキシは使用できなくなります。暗号化されたトラフィックを検査するには、TLS プロキシを使用します。 **phone-proxy**、**uc-ime** の各コマンドが削除されました。**inspect sip** コマンドから **phone-proxy** キーワードと **uc-ime** キーワードが削除されました。
H.460.18 互換性に関連する H.225 SETUP メッセージの前に着信する H.255 FACILITY メッセージに対する H.323 インスペクションのサポート。	9.6(1)	H.225 FACILITY メッセージが H.225 SETUP メッセージの前に着信する（これは、エンドポイントが H.460.18 に準拠する場合に発生する場合があります）ことを許可するように H.323 インスペクション ポリシー マップを設定できるようになりました。 次のコマンドが導入されました。**early-message**。
Session Traversal Utilities for NAT（STUN）インスペクション	9.6(2)	Cisco Spark を含む WebRTC アプリケーションの STUN トラフィックを検査できるようになりました。インスペクションでは、リターン トラフィックに必要なピンホールが開きます。 **inspect stun**、**show asp drop**、**show conn detail**、**show service-policy inspect stun** の各コマンドが追加または変更されました。
TLS プロキシでの TLSv1.2 と Cisco Unified Communications Manager 10.5.2 のサポート。	9.7(1)	暗号化 SIP 用の TLS プロキシでの TLSv1.2、または Cisco Unified Communications Manager 10.5.2 での SCCP インスペクションを使用できるようになりました。TLS プロキシは、**client cipher-suite** コマンドの一部として追加された TLSv1.2 暗号スイートをサポートします。 **client cipher-suite** コマンドが変更されました。
SCCP（Skinny）インスペクションでは、TLS プロキシが廃止されました。	9.13(1)	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは廃止されました。このキーワードは今後のリリースで **inspect skinny** コマンドから削除される予定です。

機能名	リリース	機能情報
SCCP（Skinny）インスペクションでは、TLS プロキシのサポートがなくなりました。	9.14(1)	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは削除されました。
デフォルトの SIP インスペクション ポリシーマップは、非 SIP トラフィックをドロップします。	9.16(1)	SIP インスペクションされるトラフィックでは、現在、デフォルトでは非 SIP トラフィックがドロップされます。以前のデフォルトでは、SIP のインスペクション対象ポートで非 SIP トラフィックが許可されていました。 デフォルトの SIP ポリシーマップが変更され、**no traffic-non-sip** コマンドが追加されました。

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。