CHAPTER 10

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、音声およびビデオ 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インスペクションを使用する理由に関する基本情報については、「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」（P.8-1）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 を越えてコール 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」（P.8-10）を参照してください。

CTIQBE インスペクションの制限事項

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE アプリケーション インスペクションは、**alias** コマンドを使用するコンフィギュレーションをサポートしません。
- 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。

- CTIQBE インスペクションをデバッグする 、メッセージの送信が遅れて、リアルタイム環境のパフォーマンスに影響を与える可能性があります。このデバッグまたはログをイネーブルにし、ASA を介して Cisco IP SoftPhone でコール セットアップを完了できない場合は、Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

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 の方が高セキュリティ 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 の使用時に Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録させるには、TCP ポート 2748 を PAT（インターフェイス）アドレスと同じポートに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

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 や VocalTec Gatekeeper など、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。

(注)　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 ITU 規準では、メッセージ長を定義する TPKT ヘッダーが最初に送信されてから、H.225 と H.245 が信頼できる接続上を送信されることが要求されています。TPKT ヘッダーは、必ずしも H.225 メッセージや H.245 メッセージと同一の TCP パケットで送信される必要はないため、ASA は、メッセージを正しく処理して復号化するために TPKT 長を記憶しておく必要があります。ASA は、次のメッセージに備えて、TPKT 長が含まれるレコードを接続ごとに保持します。

ASA でメッセージ内の IP アドレスに NAT を行う必要がある場合、チェックサム、UUIE 長、および TPKT（H.225 メッセージが入っている TCP パケットに含まれている場合）は変更されます。TPKT が別の TCP パケットで送信される場合、ASA がその TPKT へのプロキシ ACK を実行し、新しい TPKT を新しい長さで H.245 メッセージに追加します。

(注)　ASA は、TPKT に対する ACK の代理処理では TCP オプションをサポートしていません。

H.323 インスペクションを受け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、[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ペインで設定された H.323 タイムアウト値でタイムアウトします。

(注)　ゲートキーパー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受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。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.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 以上ではサポートされていません。H.323 インスペクションは、他のリリースおよび製品と連携できる場合があります。

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。

- 完全にサポートされているのは、スタティック NAT だけです。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。
- ダイナミック NAT または PAT ではサポートされません。
- 拡張 PAT ではサポートされません。
- 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。
- 外部 NAT ではサポートされません。
- NAT64 ではサポートされません。

- NetMeeting クライアントが H.323 ゲートキーパーに登録し、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイを呼び出そうとすると、接続は確立されますが、どちらの方向でも音声が聞こえません。この問題は、ASA の問題ではありません。
- ネットワーク スタティック アドレスを設定した場合、このネットワーク スタティック アドレスが第三者のネットマスクおよびアドレスと同じであると、すべてのアウトバウンド H.323 接続が失敗します。

H.323 インスペクションの設定

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、音声/ビデオ制御をサポートします。

H.323 インスペクション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。H.323 インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「H.323 インスペクション クラス マップの設定」（P.10-5）
ステップ 2　「H.323 インスペクション ポリシー マップの設定」（P.10-6）
ステップ 3　「H.323 インスペクションのサービス ポリシーの設定」（P.10-8）

H.323 インスペクション クラス マップの設定

オプションで H.323 インスペクションのクラス マップを作成し、H.323 インスペクションのトラフィック クラスを定義できます。もう 1 つのオプションでは、H.323 インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [H.323] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。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] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。

b. 一致基準を選択し、その値を定義します。

- [Called Party]：選択した正規表現または正規表現クラスに対して H.323 の着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して H.323 の発信側を照合します。
- [Media Type]：メディア タイプ（音声、ビデオ、またはデータ）と照合します。

c. [OK] をクリックします。

ステップ 6　[H.323 Traffic Class Map] ダイアログ ボックスで [OK] をクリックします。

これで、H.323 インスペクション ポリシー マップでクラス マップを使用できるようになります。

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。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [H.323] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。

- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[H.323 Inspect Map] ダイアログボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、H.323 インスペクションのサービス ポリシー ルールでマップを使用します。

ヒント　[Phone Number Filtering] ボタンは、着信側または発信側のインスペクションを設定するためのショートカットです。これについては、後で説明します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a. [State Checking] タブをクリックし、RAS および H.225 メッセージの状態遷移のチェックをイネーブルにするかどうか選択します。

また、RCF メッセージをチェックして、RRQ メッセージ内の通話信号アドレスのピンホールを開くこともできます。これにより、ゲートキーパーがネットワーク内にある場合に H.323 エンドポイント間のコール セットアップがイネーブルになります。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受信されるので、発信側エンドポイントの IP アドレスは不明で、ASA は発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。デフォルトでは、このオプションは無効になっています。

b. [Call Attributes] タブをクリックし、コールの制限時間（最大値は 1193 時間）を適用するかどうか、またはコールのセットアップ中に発信側番号と着信側番号のプレゼンスを強制するかどうかを選択します。

c. [Tunneling and Protocol Conformance] タブをクリックし、H.245 トンネリングをチェックするかどうかを選択します。接続をドロップするか、ロギングすることができます。

ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択することもできます。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

ステップ 6　必要に応じて、[HSI Group Parameters] タブをクリックし、HSI グループを定義します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しいグループを追加します。
- 既存のグループを選択し、[Edit] をクリックします。

b. グループ ID（0 ～ 2147483647）と HSI の IP アドレスを指定します。

c. HSI グループにエンドポイントを追加するには、IP アドレスを入力し、エンドポイントが ASA に接続するときに使用するインターフェイスを選択して、[Add>>] をクリックします。不要になったエンドポイントを削除します。グループあたり最大 10 個のエンドポイントを設定できます。

d. [OK] をクリックして、グループを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、H.323 クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する H.323 クラス マップを選択する場合は [Multiple Match] を選択します（「H.323 インスペクション クラス マップの設定」（P.10-5）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。次に、基準を以下のように設定します。

- [Called Party]：選択した正規表現または正規表現クラスに対して H.323 の着信側を照合します。
- [Calling Party]：選択した正規表現または正規表現クラスに対して H.323 の発信側を照合します。
- [Media Type]：メディア タイプ（音声、ビデオ、またはデータ）と照合します。

d. トラフィックの照合で実行するアクションを選択します。発信側または着信側を照合する場合は、パケットをドロップするか、接続をドロップするか、接続をリセットできます。メディア タイプの照合の場合、アクションは常にパケットのドロップです。このアクションではロギングをイネーブルにすることができます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 8　[H.323 Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを H.323 インスペクションのサービス ポリシーで使用できるようになります。

H.323 インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスでグローバルに適用されるデフォルト ポートでの H.323、H.255、および RAS のインスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。

- H.323 インスペクション ルール、つまり H.323 インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[H.323 H.255] および [H.323 RAS] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した H.323 インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「H.323 インスペクション ポリシー マップの設定」（P.10-6）を参照してください。

マップをポリシーに割り当てるには、[Select H.323 Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

H.323 および H.225 タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで H.323/H.255 グローバル タイムアウト値を設定できます。H.255 シグナリング接続を閉じるまでの非アクティビティ間隔（デフォルトは 1 時間）または H.323 制御接続を閉じるまでの非アクティブ間隔（デフォルトは 5 分）を設定できます。

MGCP インスペクション

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。

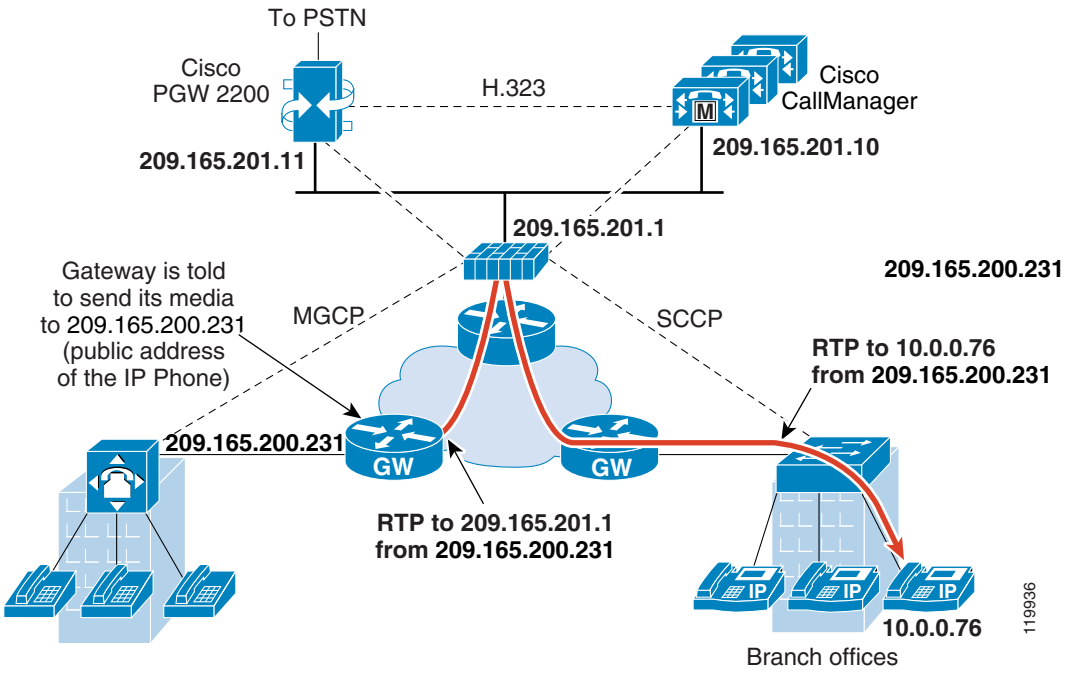
MGCP インスペクションの概要

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の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するマスター /スレーブ プロトコルです。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 10-1　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 インスペクションの設定

MGCP インスペクションをイネーブルにするには、次のプロセスを使用します。

手順

ステップ 1　「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.10-11）

ステップ 2　「MGCP インスペクションのサービス ポリシーの設定」（P.10-12）

インスペクション制御を追加するための 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、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　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [MGCP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　（オプション）[Command Queue] タブをクリックし、MGCP コマンド キューで使用できるコマンドの最大数を指定します。デフォルトは 200 で、使用できる範囲は 1 ～ 2147483647 です。

ステップ 5　[Gateways and Call Agents] タブをクリックし、マップのゲートウェイとコール エージェントのグループを設定します。

a. [Add] をクリックして新しいグループを作成するか、グループを選択して [Edit] をクリックします。

b. コール エージェント グループの**グループ ID** を入力します。コール エージェント グループで、1 つ以上のコール エージェントを 1 つ以上の MGCP メディア ゲートウェイと関連付けます。0 ～ 2147483647 の範囲の値を指定できます。

c. 関連付けられているコール エージェントによって制御されるメディア ゲートウェイの IP アドレスをグループに追加するには、それらの IP アドレスを [Gateway to Be Added] に入力し、[Add>>] をクリックします。使用しなくなったゲートウェイを削除します。

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。通常、ゲートウェイはコマンドを、コール エージェントのデフォルト MGCP ポート（UDP 2727）に送信します。

d. MGCP メディア ゲートウェイを制御するコール エージェントの IP アドレスを追加するには、それらの IP アドレスを [Call Agent to Be Added] に入力し、[Add>>] をクリックします。不要になったエージェントを削除します。

通常、コール エージェントはコマンドを、ゲートウェイのデフォルト MGCP ポート（UDP 2427）に送信します。

e. [MGCP Group] ダイアログ ボックスで [OK] をクリックします。必要に応じてプロセスを繰り返し、その他のグループを追加します。

ステップ 6　[MGCP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを MGCP インスペクションのサービス ポリシーで使用できるようになります。

MGCP インスペクションのサービス ポリシーの設定

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、デフォルトのインスペクション クラスにはデフォルトの MGCP ポートが含まれるため、デフォルトのグローバル インスペクション ポリシーを編集して MGCP インスペクションを追加するだけで済みます。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- MGCP インスペクション ルール、つまり RTSP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[MGCP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した MGCP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための MGCP インスペクション ポリシー マップの設定」（P.10-11）を参照してください。

ポリシー マップを割り当てるには、[Select MGCP Inspect Map] ダイアログボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

MGCP タイムアウト値の設定

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の MGCP グローバル タイムアウト値を設定できます。MGCP メディア接続を閉じるまでの非アクティブ間隔を設定できます（デフォルトは 5 分）。PAT xlate のタイムアウトも設定できます（30 秒）。

RTSP インスペクション

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 の場合、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、インバウンド方向に移動している場合、サーバは 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。

RFC 2326 では、クライアント ポートとサーバ ポートが、SETUP 応答メッセージ内に含まれていることは必要でないため、ASA では、状態を維持し、SETUP メッセージ内のクライアント ポートを記憶します。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバは、サーバ ポートだけで応答します。

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** *port* 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。

RSTP インスペクションの設定

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。RTSP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「RTSP インスペクションのクラス マップの設定」（P.10-14）
ステップ 2　「RTSP インスペクションのポリシー マップの設定」（P.10-15）
ステップ 3　「RTSP インスペクションのサービス ポリシーの設定」（P.10-17）

RTSP インスペクションのクラス マップの設定

オプションで RTSP インスペクションのクラス マップを作成し、RTSP インスペクションのトラフィック クラスを定義できます。もう 1 つのオプションでは、RTSP インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [RTSP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。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] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [URL Filter]：選択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。
- [Request Method]：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかの要求方式と照合します。

c. [OK] をクリックします。

ステップ 6　[RTSP Traffic Class Map] ダイアログボックスで [OK] をクリックします。

これで、RTSP インスペクション ポリシー マップでクラス マップを使用できるようになります。

RTSP インスペクションのポリシー 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。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [RTSP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- マップを選択し、[Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[Parameters] タブをクリックし、必要なオプションを設定します。

- [Enforce Reserve Port Protection]：メディア ポート ネゴシエーション中の予約済みポートの使用を制限するかどうか。
- [Maximum URL Length]：メッセージで使用できる URL の最大長（0 ～ 6000）。

ステップ 5　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、RTSP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する RTSP クラス マップを選択する場合は [Multiple Match] を選択します（「RTSP インスペクションのクラス マップの設定」（P.10-14）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を以下のように設定します。

- [URL Filter]：選択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。
- [Request Method]：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown のいずれかの要求方式と照合します。

d. トラフィックの照合で実行するアクションを選択します。URL の照合の場合は、接続をドロップするかロギングし、ドロップした接続のロギングをイネーブルにすることができます。要求方式の照合の場合は、レート制限（パケット/秒）を適用できます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 6　[RTSP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを RTSP インスペクションのサービス ポリシーで使用できるようになります。

RTSP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの RTSP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- RTSP インスペクション ルール、つまり RTSP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[RTSP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、デフォルト マップを使用するか、設定した RTSP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「RTSP インスペクションのポリシー マップの設定」（P.10-15）を参照してください。

ポリシー マップを割り当てるには、[Select RTSP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

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 プロキシを識別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」（P.10-18）
- 「SIP インスペクションの制限事項」（P.10-18）
- 「SIP インスタント メッセージ」（P.10-19）

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（「コール」）が使用可能になります。SIP は、コール シグナリング用の SDP で動作します。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。

SIP インスペクションの制限事項

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。

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 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。

SIP インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムにユーザ間でメッセージを転送することです。SIP は、Windows Messenger RTC Client バージョン 4.7.0105 を使用する Windows XP のチャット機能のみをサポートします。次の RFC で定義されているように、MESSAGE/INFO 方式および 202 Accept 応答を使用して IM をサポートします。

- Session Initiation Protocol（SIP）Specific Event Notification、RFC 3265
- Session Initiation Protocol（SIP）Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録または加入の後、任意の時点で着信する可能性があります。たとえば、2 人のユーザ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） チャット機能のみがサポートされています。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 インスペクションは、テキストベースの SIP メッセージを変換し、メッセージの SDP 部分の内容長を再計算した後、パケット長とチェックサムを再計算します。また、エンドポイントが受信すべきアドレスまたはポートとして、SIP メッセージの SDP 部分に指定されたポートに対するメディア接続をダイナミックに開きます。

SIP インスペクションでは、SIP ペイロードから取得したインデックス CALL_ID/FROM/TO を持つデータベースが使用されます。これらのインデックスにより、コール、送信元、宛先が識別されます。このデータベースには、SDP のメディア情報フィールド内で見つかったメディア アドレスとメディア ポート、およびメディア タイプが格納されます。1 つのセッションに対して、複数のメディア アドレスとポートが存在することが可能です。ASA は、これらのメディア アドレス/ポートを使用して、2 つのエンドポイント間に RTP/RTCP 接続を開きます。

初期コール セットアップ（INVITE）メッセージでは、予約済みポート 5060 を使用する必要があります。ただし、後続のメッセージにはこのポート番号がない場合もあります。SIP インスペクション エンジンはシグナリング接続のピンホールを開き、それらの接続を SIP 接続としてマークします。これは、SIP アプリケーションに到達した変換対象のメッセージに対して行われます。

コールのセットアップ時に、SIP セッションは、着信側エンドポイントから応答メッセージでメディア アドレスとメディア ポートを受信し、着信側エンドポイントがどの RTP ポートで受信するかを知らされるまで「一時的な」状態にあります。1 分以内に、応答メッセージの受信に障害があった場合は、シグナリング接続は切断されます。

最終的なハンドシェイクが行われると、コール状態はアクティブに移行し、シグナリング接続は、BYE メッセージの受信まで継続されます。

内部エンドポイントが、外部エンドポイントに発呼した場合、メディア ホールが、外部インターフェイスに対して開き、内部エンドポイントから送信された INVITE メッセージで指定された内部エンドポイントのメディア アドレスとメディア ポートに、RTP/RTCP UDP パケットが流れることが許可されます。内部インターフェイスに対する要求外の RTP/RTCP UDP パケットは、ASA のコンフィギュレーションで特別に許可されない限り、ASA を通過できません。

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：許可
- 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

また、暗号化されたトラフィックのインスペクションはイネーブルになっていません。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 インスペクションの設定

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 プロキシを識別する場合にのみ設定する必要があります。SIP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「SIP インスペクションのクラス マップの設定」（P.10-20）
ステップ 2　「SIP インスペクション ポリシー マップの設定」（P.10-22）
ステップ 3　「SIP インスペクションのサービス ポリシーの設定」（P.10-24）

SIP インスペクションのクラス マップの設定

オプションで SIP インスペクションのクラス マップを作成し、SIP のトラフィック クラスを定義できます。もう 1 つのオプションでは、SIP インスペクションのポリシー マップで直接トラフィック クラスを定義します。クラス マップを作成することとインスペクション マップでトラフィックの照合を直接定義することの違いは、クラス マップでは複雑な一致基準を作成でき、クラス マップを再利用できるという点です。

ヒント　以下で説明する手順に加えて、インスペクション マップまたはサービス ポリシーの作成中にもクラス マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Class Maps] > [SIP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいクラス マップを追加します。
- マップを選択して [Edit] をクリックします。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　照合オプションとして [Match All] または [Match Any] を選択します。

[Match All] がデフォルトです。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] は、少なくとも 1 つの基準に一致したトラフィックがクラス マップに一致することを意味します。

ステップ 5　一致テーブルでエントリを追加または編集して、一致基準を設定します。対象トラフィックを定義するために必要な数のエントリを追加します。

a. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。

b. 一致基準を選択し、その値を定義します。

- [Called Party]：選択し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。
- [Calling Party]：選択し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。
- [Content Length]：指定された長さ（0 ～ 65536 バイト）より長い SIP コンテンツ ヘッダーを照合します。
- [Content Type]：Content Type ヘッダー、つまり SDP タイプか、選択した正規表現または正規表現クラスと一致するタイプを照合します。
- [IM Subscriber]：選択し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。
- [Message Path]：選択し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。
- [Request Method]：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update のいずれかの SIP 要求方式を照合します。
- [Third-Party Registration]：選択し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。
- [URI Length]：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。

c. [OK] をクリックします。

ステップ 6　[SIP Traffic Class Map] ダイアログ ボックスで [OK] をクリックします。

これで、SIP インスペクション ポリシー マップでクラス マップを使用できるようになります。

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。

ヒント　以下で説明する手順に加えて、サービス ポリシーの作成中にもインスペクション マップを設定できます。マップの内容は、作成方法に関係なく同じです。

はじめる前に

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いずれかを使用する場合は、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　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [SIP] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[SIP Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順はスキップして、SIP インスペクションのサービス ポリシー ルールでマップを使用します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a. [Filtering] タブをクリックし、SIP インスタント メッセージング（IM）拡張機能をイネーブルにするかどうか、または SIP ポート上の SIP 以外のトラフィックを許可するかどうかを選択します。

b. [IP Address Privacy] タブをクリックし、サーバとエンドポイントの IP アドレスを非表示にするかどうかを選択します。

c. [Hop Count] タブをクリックし、宛先までのホップ数が 0 を超えていることを確認するかどうかを選択します。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。

d. [RTP Conformance] タブをクリックし、ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択します。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

e. [SIP Conformance] タブをクリックし、状態遷移チェックとヘッダー フィールドの厳格な検証をイネーブルにするかどうかを選択します。選択したオプションごとに、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します。

f. [Field Masking] タブをクリックし、Alert-Info および Call-Info ヘッダーの SIP 以外の URI を検査するかどうか、User-Agent および Server ヘッダーのサーバおよびエンドポイントのソフトウェア バージョンを検査するかどうかを選択します。選択したオプションごとに、実行するアクション（マスクまたはロギング）と、ロギングをインネーブルまたはディセーブルのどちらにするかを選択します。

ステップ 6　[Inspections] タブをクリックして、トラフィックの特性に基づいて実装する特定のインスペクションを定義します。

トラフィック一致基準は、SIP クラス マップをベースにするか、インスペクション マップで一致を直接設定するか、またはこの両方によって定義できます。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準を直接定義する場合は [Single Match] を選択し、基準を定義する SIP クラス マップを選択する場合は [Multiple Match] を選択します（「SIP インスペクションのクラス マップの設定」（P.10-20）を参照）。

c. 基準をここで定義した場合は、基準の一致タイプとして [Match]（トラフィックは基準と一致する必要がある）または [No Match]（トラフィックは基準と異なる必要がある）を選択します。たとえば、文字列「example.com」で [No Match] を選択した場合、「example.com」を含むトラフィックはすべてクラス マップの対象外になります。次に、基準を以下のように設定します。

- [Called Party]：選択し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。
- [Calling Party]：選択し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。
- [Content Length]：指定された長さ（0 ～ 65536 バイト）より長い SIP コンテンツ ヘッダーを照合します。
- [Content Type]：Content Type ヘッダー、つまり SDP タイプか、選択した正規表現または正規表現クラスと一致するタイプを照合します。
- [IM Subscriber]：選択し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。
- [Message Path]：選択し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。
- [Request Method]：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update のいずれかの SIP 要求方式を照合します。
- [Third-Party Registration]：選択し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。
- [URI Length]：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. 一致する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、ログ）と、ロ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します。「invite」および「register」に一致する要求方式の場合は、レート制限（パケット/秒）も適用できます。

e. [OK] をクリックしてインスペクションを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[SIP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを SIP インスペクションのサービス ポリシーで使用できるようになります。

SIP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SIP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SIP インスペクション ルール、つまり SIP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[SIP] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した SIP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「SIP インスペクション ポリシー マップの設定」（P.10-22）を参照してください。

b. 暗号化された SIP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要な場合は [Manage] をクリックして作成します）。

電話プロキシまたは UC-IME プロキシを選択してこれらのプロキシに TLS プロキシを関連付けることはできますが、この設定は推奨されません。電話プロキシまたは UC-IME プロキシに一度に割り当てることができるのは、1 つの TLS プロキシのみです。電話プロキシまたは UC-IME プロキシ インスペクションに複数のサービス ポリシー ルールを設定し、異なる TLS プロキシをそれらのルールに割り当てようとすると、ASDM は、電話プロキシと UC-IME インスペクションに設定されているその他のすべてのサービス ポリシー ルールが、最後に選択された TLS プロキシを使用するように変更されるという警告を表示します。

UC-IME プロキシ コンフィギュレーションでは、2 つの TLS プロキシ（インバウンド トラフィック用とアウトバウンド トラフィック用）が必要です。TLS プロキシを UC-IME プロキシに直接関連付けるのではなく、電話プロキシの場合のように、TLS プロキシは SIP インスペクション ルールを介して UC-IME プロキシに間接的に関連付けられます。

c. [Select SIP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

SIP タイムアウト値の設定

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、これは設定可能なタイムアウトであり、時間間隔は変更することが可能です。

[Configuration] > [Firewall] > [Advanced] > [Global Timeouts] ページで複数の SIP グローバル タイムアウト値を設定できます。

Skinny（SCCP）インスペクション

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」（P.10-25）
- 「Cisco IP Phone のサポート」（P.10-26）
- 「SCCP インスペクションの制限事項」（P.10-26）
- 「デフォルトの SCCP インスペクション」（P.10-26）
- 「SCCP（Skinny）インスペクションの設定」（P.10-27）

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 Phone 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 エントリを使用すると、高セキュリティ インターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

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 の方が低セキュリティ 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 サーバおよび Cisco CallManager と比べて*高*セキュリティ 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際に、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

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 は現在のところ 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 では、コール セットアップ中であるコール以外の SCCP 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。

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以下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ります。

- 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

また、暗号化されたトラフィックのインスペクションはイネーブルになっていません。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。

SCCP（Skinny）インスペクションの設定

SCCP（Skinny）アプリケーション インスペクションでは、パケット データ内に埋め込まれている IP アドレスとポート番号の変換、およびピンホールの動的なオープンを実行します。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 プロキシを識別する場合にのみ設定する必要があります。SCCP インスペクションをカスタマイズする場合は、次の手順に従います。

手順

ステップ 1　「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.10-27）

ステップ 2　「SCCP インスペクションのサービス ポリシーの設定」（P.10-28）

インスペクション制御を追加するための 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　[Configuration] > [Firewall] > [Objects] > [Inspect Maps] > [SCCP (Skinny)] の順に選択します。

ステップ 2　次のどちらかを実行します。

- [Add] をクリックして、新しいマップを追加します。
- 内容を表示するマップを選択します。マップのセキュリティ レベルは直接変更するか、[Customize] をクリックすることで編集できます。残りの手順は、マップをカスタマイズするか追加することが前提になります。

ステップ 3　新しいマップの場合、名前（最大 40 文字）と説明を入力します。マップの編集時には、説明のみを変更できます。

ステップ 4　[SCCP (Skinny) Inspect Map] ダイアログ ボックスの [Security Level] ビューで、目的の設定に最も一致するレベルを選択します。デフォルトのレベルは [Low] です。

プリセット レベルの 1 つが要件と一致する場合は、これで完了です。[OK] をクリックし、残りの手順をスキップして、SCCP インスペクションのサービス ポリシー ルールでマップを使用します。

ステップ 5　設定をさらにカスタマイズする必要がある場合は、[Details] をクリックし、次の操作を実行します。

a. [Parameters] タブをクリックし、次のオプションから選択します。

- [Enforce endpoint registration]：コールを発信または着信する前に Skinny エンドポイントを登録するかどうか。
- [Maximum Message ID]：許可される最大の SCCP ステーション メッセージ ID。デフォルトの最大値は 0x181 です。16 進数値は 0x0 ～ 0xffff です。

- [SCCP Prefix Length]：最大および最小の SCCP プレフィックス長。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。
- [Timeouts]：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するかどうか、およびそれらのタイムアウト値。デフォルトはメディアの場合は 5 分、シグナリングの場合は 1 時間です。

b. [RTP Conformance] タブをクリックし、ピンホールに流れる RTP パケットがプロトコルに準拠していることをチェックするかどうかを選択します。また、準拠をチェックする場合は、シグナリング交換に基づいてペイロードを音声またはビデオに限定するかどうかを選択できます。

ステップ 6　（オプション）[Message ID Filtering] タブをクリックし、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ドロップするトラフィックを指定します。

a. 次のいずれかを実行します。

- [Add] をクリックして、新しい基準を追加します。
- 既存の基準を選択し、[Edit] をクリックします。

b. 基準の一致タイプとして [Match]（トラフィックは基準に一致する必要がある）または [No Match]（トラフィックは基準とは異なっている必要がある）を選択します。

c. [Value] フィールドで、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指定します。1 つのメッセージ ID の値を入力するか、ID の範囲の開始値と終了値を入力します。

d. 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します。デフォルトのアクションは、常にパケットのドロップです。

e. [OK] をクリックして、フィルタを追加します。必要に応じてこのプロセスを繰り返します。

ステップ 7　[SCCP (Skinny) Inspect Map] ダイアログ ボックスで [OK] をクリックします。

これで、このインスペクション マップを SCCP インスペクションのサービス ポリシーで使用できるようになります。

SCCP インスペクションのサービス ポリシーの設定

デフォルトの ASA 設定には、すべてのインターフェイスにグローバルに適用されるデフォルト ポートの SCCP インスペクションが含まれます。インスペクション設定をカスタマイズするには、デフォルトのグローバル ポリシーをカスタマイズするのが一般的です。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。

手順

ステップ 1　[Configuration] > [Firewall] > [Service Policy] の順に選択し、ルールを開きます。

- デフォルトのグローバル ポリシーを編集するには、[Global] フォルダの「inspection_default」ルールを選択し、[Edit] をクリックします。
- 新しいルールを作成するには、[Add] > [Add Service Policy Rule] をクリックします。「通過トラフィックのサービス ポリシー ルールの追加」（P.1-11）に従って、ウィザードを使って [Rules] ページに進みます。
- SCCP インスペクション ルール、つまり SCCP インスペクションを追加しているルールがある場合は、そのルールを選択し、[Edit] をクリックします。

ステップ 2　[Rule Actions] ウィザード ページまたはタブで、[Protocol Inspection] タブを選択します。

ステップ 3　[SCCP （Skinny）] を選択します。

ステップ 4　デフォルト以外のインスペクションが必要な場合は、[Configure] をクリックし、次の操作を実行します。

a. デフォルト マップを使用するか、設定した SCCP インスペクション ポリシー マップを使用するかを選択します。この時点でマップを作成できます。詳細については、「インスペクション制御を追加するための Skinny（SCCP）インスペクション ポリシー マップの設定」（P.10-27）を参照してください。

b. 暗号化された SCCP トラフィックを検査する場合は、[Enable encrypted traffic inspection] を選択し、TLS プロキシを選択します（必要な場合は [Manage] をクリックして作成します）。

ASA に設定されている電話機プロキシを使用して Skinny アプリケーション トラフィックを検査することもできますが、この設定は推奨されません。

c. [Select SCCP Inspect Map] ダイアログ ボックスで [OK] をクリックします。

ステップ 5　[OK] または [Finish] をクリックしてサービス ポリシー ルールを保存します。

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
IPv6 に対する SIP、SCCP、および TLS プロキシのサポート	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 ASDM 画面はありません。