CUCM と VCS または Expressway の間のセキュア RTP 設定例

内容

概要

このドキュメントでは、Cisco Video Communication Server（VCS）と Cisco Unified Communications Manager（CUCM）間で Secure Real-Time Transport Protocol（RTP）をセットアップする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM
- Cisco VCS または Cisco Expressway

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM
- Cisco VCS または Cisco Expressway

  注：この記事では、説明に Cisco Expressway 製品を使用していますが、この情報は Cisco VCS を使用する導入の場合も適用されます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

条件

- CUCM と Expressway 間にルーティングされた Session Initiation Protocol（SIP）コール
- メディア暗号化は、Expressway-C と CUCM 間のベスト エフォートであり、任意です。

説明

CUCM と VCS/Expressway 間にルーティングされた SIP コールのベスト エフォート メディア暗号化の設定については問題が報告されています。一般的な不適切な設定が Secure Real-Time Transport Protocol（SRTP）による暗号化メディアのシグナリングに影響し、CUCM と Expressway 間のトランスポートがセキュアでない場合にベスト エフォートの暗号化コールに障害を引き起こします。

トランスポートがセキュアでない場合、メディア暗号化シグナリングは、盗聴者によって読み取られる可能性があります。この場合、メディア暗号化シグナリング情報が Session Description Protocol（SDP）からストリップされます。 ただし、セキュアでない接続上にメディア暗号化シグナリングを送信（および受信を期待）するように CUCM を設定することは可能です。この不適切な設定は、コールを CUCM へトランク側からルーティングするか、回線側からルーティングするかによって、2 つの方法のいずれかで対処できます。

トランク側と回線側の例

トランク側：SIP トランクは、Expressway に対して CUCM 上に設定されます。対応するネイバー ゾーンは CUCM に対して Expressway 上に設定されます。VCS 登録（Expressway ではなく VCS がレジストラ）エンドポイントに CUCM 登録エンドポイントをコールさせる場合はトランクが必要です。別の例では、導入で H.323 インターワーキングを有効にします。

回線側：回線側のコールはトランク経由ではなく、直接 CUCM に向かいます。すべての登録とコール制御が CUCM によって行われている場合の導入では、Expressway へのトランクは必要ない場合があります。たとえば、モバイルおよびリモート アクセス（MRA）のためだけに Expressway を導入する場合、回線側のコールは外部エンドポイントから CUCM に送信します。

軽減のための戦略

CUCM と Expressway 間に SIP トランクがある場合、CUCM の正規化スクリプトが SDP を適切に書き換えるため、ベスト エフォート暗号化コールは拒否されません。このスクリプトは CUCM の最近のリリースでは自動的にインストールされますが、ベスト エフォート暗号化コールが拒否される場合は、使用中の CUCM バージョンの最新の vcs-interop をダウンロードし、インストールすることを推奨します。

コールが回線側から CUCM に向かう場合、メディア暗号化が任意のときは、CUCM は `x-cisco-srtp-fallback` ヘッダーがあることを予期しています。CUCM がこのヘッダーを確認できない場合、そのコールは暗号化が必須であると見なします。このヘッダーに対するサポートはバージョン X8.2 で Expressway に追加されました。MRA（コラボレーション エッジ）には X8.2 以降を推奨します。

設定

回線側の設定

[CUCM]<—best-effort—>[Expressway-C]<—mandatory—>[Expressway-E]<—mandatory—>[Endpoint]

Expressway-C から CUCM への回線側コールのベスト エフォート暗号化を有効にするには、次の手順を実行します。

- サポートされている導入/ソリューション（MRA など）を使用します。
- CUCM 上で混合モード セキュリティを使用します。
- Expressway および CUCM が相互に信頼されていることを確認します（各当事者の証明書に署名する認証局（CA）は他方の当事者によって信頼されている必要があります）。
- バージョン X8.2 以降の Expressway を使用します。
- CUCM でセキュアな電話機プロファイルと、認証済みまたは暗号化済みに設定されたデバイス セキュリティ モードを使用します。これらのモードの場合のトランスポート タイプは Transport Layer Security（TLS）です。

トランク側の設定

- サポートされる導入/ソリューションを使用します。
- CUCM 上で混合モード セキュリティを使用します。
- Expressway および CUCM が相互に信頼されていることを確認します（各当事者の証明書に署名する CA は他方の当事者によって信頼されている必要があります）。
- 暗号化モードとしてベスト エフォートを、Expressway から CUCM へのネイバー ゾーン上のトランスポートとして TLS を選択します（回線側の場合、これらの値は自動的に事前に挿

入されます）。
- SIP トランク セキュリティ プロファイルのインバウンドとアウトバウンドのトランスポートとして TLS を選択します。
- CUCM から Expressway への SIP トランクの [SRTPSRTP Allowed] をオンにします（「注意」を参照してください）。
- 使用中の CUCM および Expressway のバージョンに適切な正規化スクリプトを確認し、必要に応じて適用します。

注意：[SRTP Allowed] チェックボックスをオンにする場合、キーやその他のセキュリティ関連情報がコール ネゴシエーション時に暴露されないようにするために、暗号化 TLS プロファイルを使用することを強く推奨します。セキュアでないプロファイルを使用しても SRTP は機能します。ただし、キーはシグナリングやトレースで暴露されます。この場合、CUCM とトランクの宛先側間のネットワークのセキュリティを確保する必要があります。

メディア暗号化のオプション

なし

暗号化は許可されていません。暗号化が必要なコールは、セキュアでないため、失敗します。CUCM と Expressway は、この場合のシグナリングに整合性があります。

CUCM と Expressway は両方とも `m=RTP/AVP SDP` 暗号属性はありません（SDP のメディア セクションに `a=crypto...`

必須

メディア暗号化が必要です。暗号化されていないコールは常に失敗します。フォールバックは許可されません。CUCM と Expressway は、この場合のシグナリングに整合性があります。

CUCM と Expressway は両方とも `m=RTP/SAVP SDP` SDP には暗号属性があります（SDP のメディア セクションの `a=crypto...`

ベスト エフォート

暗号化できるコールは暗号化されます。暗号化が確立できない場合、コールは暗号化されていないメディアにフォールバックされる場合があり、また、フォールバックする必要があります。CUCM と Expressway はこの場合は整合性があります。

Expressway は、トランスポートが Transmission Control Protocol（TCP）または User Datagram Protocol（UDP）である場合、暗号化を拒否します。 メディア暗号化が必要な場合は、CUCM と Expressway 間のトランクを保護する必要があります。

SDP（CUCM が書き込む場合）暗号化メディアは、`m=RTP/SAVP a=crypto SDP` メディア暗号化ではこれは正しいシグナリングですが、トランスポートがセキュアでない場合、暗号行は読み取り可能です。

CUCM が `x-cisco-srtp-fallback` このヘッダーがない場合、CUCM はコールに暗号化が必要である（フォールバックを許可しない）と想定します。

X8.2 現在、Expressway は回線側では CUCM と同様にベスト エフォートを行っています。

SDP（Expressway がトランク側を書き込む場合）暗号化メディアは、`m=RTP/AVP a=crypto  SDP`

ただし、a=crypto 行がなくなる場合がある理由として 2 つ考えられます。

1. Expressway の SIP プロキシに対するトランスポート ホップがセキュアでない場合、プロキシは暗号行をストリップし、セキュアでないホップ上で暴露されないようにします。
2. 応答側が暗号化できない、またはしない信号のために、応答側が暗号行をストリップします。

正しい SIP 正規化スクリプトを CUCM で使用することがこの問題を軽減します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

関連資料

- Cisco Unified Communications Manager セキュリティ ガイド リリース 10.0(1)
- Cisco Unified Communications Manager および Cisco VCS の会議最適化ソリューションガイド（リリース 2.0）
- Cisco Expressway（SIP トランク）を搭載した Cisco Unified Communications Manager 導入ガイド（Cisco Expressway X8.2 および Unified CM 8.6x and 9.x 向け）
- Cisco VCS（SIP トランク）Cisco Unified Communications Manager 導入ガイド（For Cisco VCS X8.2 および Unified CM 8.6.x and 9.x 向け）
- Cisco VCS によるユニファイド コミュニケーション モバイルおよびリモート アクセス導入ガイド（Cisco VCS X8.2 および Cisco Unified CM 9.1(2)SU1 以降向け）
- Cisco Expressway によるユニファイド コミュニケーション モバイルおよびリモート アクセス導入ガイド（Cisco Expressway X8.2 および Cisco Unified CM 9.1(2)SU1 以降向け）
- テクニカル サポートとドキュメント – Cisco Systems

関連 RFC

- RFC 3261 SIP：セッション開始プロトコル

- RFC 4566 SDP：セッション記述プロトコル
- RFC 4568 SDP：セキュリティの説明