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

目次

概要

この文書に Cisco ビデオ コミュニケーション サーバ（VCS）と Cisco Unified コミュニケーション マネージャ（CUCM）間のセキュア リアルタイムトランスポートプロトコル （RTP）を設定する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- CUCM
- Cisco VCS か 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くものです。

- CUCM
- Cisco VCS か Cisco Expressway

  注: この記事は説明の為に示されるところ Cisco Expressway 製品を（以外）使用しますが、配置が Cisco VCS を使用する場合情報はまた適用します。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 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。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

条件

- CUCM と Expressway の間でルーティングされる Session Initiation Protocol （SIP）呼び出し
- メディア暗号化は ExpresswayC と CUCM 間でベストエフォート型/オプションです

説明

CUCM と VCS/Expressway の間でルーティングされる SIP 呼び出しのための最もよい努力メディア暗号化の設定用の報告される問題がずっとあります。 よくあるミスコンフィギュレーションはベストエフォートによって暗号化される呼び出しの失敗を引き起こすセキュア リアルタイムトランスポートプロトコル（SRTP）によって CUCM と Expressway 間の転送がセキュアのとき暗号化されたメディアのシグナリングに、影響を与えます。

転送がセキュアではない場合、メディア暗号化シグナリングは立ち聞きする人によって読むことができます。 この場合、メディア暗号化シグナル情報は Session Description Protocol （SDP）から除去されます。 ただし、（受け取ると期待するため）保護されていない接続に信号を送るメディア暗号化を送信 するために CUCM を設定することは可能性のあるであり。 呼び出しが CUCM へルーティングされたトランク側またはライン側であるかどうか 2 つの方法の 1 つのこのミスコンフィギュレーションを、依存回避できます。

トランク側およびライン側の例

トランク側: SIP トランクは Expressway の方の CUCM で設定されます。 対応する隣接ゾーンは CUCM の方の Expressway で設定されます。 VCS 登録された（Expressway はレジストラではないですが、VCS はあります）エンド ポイントに CUCM 登録されたエンド ポイントを呼出してほ

しかった場合トランクを必要とします。 もう一つの例は配備で相互に作用する H.323 を有効にすることです。

ライン側: ライン側の呼び出しは CUCM に、ないトランクによって直接行きます。 すべての登録およびコール制御が CUCM によって提供される場合、配備は Expressway にトランクを必要としないかもしれません。 たとえば、Expressway がモービルおよびリモートアクセス（MRA）のために全く配置されれば、それライン側が外部エンド ポイントから CUCM に呼出すプロキシ。

軽減戦略

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はベストエフォート型暗号化コールが拒否されないように SDP を適切に書き換えます。 このスクリプトは CUCM の以降のリリースによって自動的にインストールされています、ベストエフォートによって暗号化される呼び出しを拒否してもらえば CUCM のバージョンのための最新の VC 相互運用スクリプトをダウンロードし、インストールすることを Cisco は推奨します。

コールがライン側 CUCM に行く場合、CUCM はメディア暗号化がオプションである場合 x cisco srtp ヘッダを見ると期待します。 CUCM がこのヘッダを見ない場合、コールが暗号化必須であると考慮します。 このヘッダのサポートはバージョン X8.2 の Expressway に追加されました、従って Cisco は MRA（コラボレーション エッジ）のための X8.2 またはそれ以降を推奨します。

設定

ライン側の設定

[CUCM] <--ベストエフォート--> [ExpresswayC] <--必須--> [Expressway-E] <--必須--> [エンド ポイント]

ExpresswayC からの CUCM にライン側の呼び出しのベストエフォート型暗号化を有効に するため:

- サポートされた配備/ソリューションを使用して下さい（たとえば、MRA）
- CUCM のミックス モード セキュリティを使用して下さい
- その Expressway および各当事者の証明書に署名する CUCM 信頼を互い確認して下さい（認証局（CA）は他の当事者によって信頼する必要があります）
- Expressway のバージョン X8.2 またはそれ以降を使用して下さい
- 保護します認証されるか、または暗号化されてデバイスセキュリティ モード セットが CUCM の電話プロファイルを、使用して下さいトランスポート タイプは-これらのモードのための…です Transport Layer Security（TLS）

トランク側設定

- サポートされた配備/ソリューションを使用して下さい
- CUCM のミックス モード セキュリティを使用して下さい
- その Expressway および CUCM 信頼を互い確認して下さい（各当事者の証明書に署名する CA は他の当事者によって信頼する必要があります）

- 暗号化モードとして最もよい努力および隣接ゾーンの転送として Expressway から CUCM に TLS を選択して下さい（これらの値はライン側のケースで自動的に事前に読み込まれます）
- SIP トランク セキュリティプロファイルの受信および送信転送として TLS を選択して下さい
- CUCM からの Expressway に SIP トランクで（注意文を参照して下さい）許可される SRTP をチェックして下さい
- をチェックし、CUCM のバージョンのための正しい正規化スクリプトおよび Expressway 必要ならば適用して下さい

注意： SRTP によって許可されるチェックボックスをチェックする場合、Cisco はキーおよび他のセキュリティに関する情報がコールネゴシエーションの間に露出されて得ないように暗号化された TLS プロファイルを使用することを強く推奨します。 非セキュア プロファイルを使用する場合、SRTP はまだはたらきます。 ただし、キーはシグナリングおよびトレースで露出されます。 そのケースでは、トランクの CUCM と宛先側間のネットワークのセキュリティを確保して下さい。

メディア暗号化オプション

なし

暗号化は許可されません。 暗号化を必要とする呼び出しはセキュアである場合もないので失敗する必要があります。 CUCM および Expressway はこのケースのためのシグナリングで一貫しています。

CUCM および Expressway は両方 SDP でメディアを記述するために `m=RTP/AVP` 使用します。 暗号属性がありません（SDP のメディア セクションの `a=crypto…`行無し）。

Mandatory

メディア暗号化が必要となります。 非暗号化呼び出しは常に失敗する必要があります; フォールバックが割り当てられません。 CUCM および Expressway はこのケースのためのシグナリングで一貫しています。

CUCM および Expressway は両方 SDP でメディアを記述するために `m=RTP/SAVP` 使用します。 SDP に暗号属性があります（SDP のメディア セクションの `a=crypto…`行）。

ベスト エフォート

暗号化することができる呼び出しは暗号化されます。 暗号化が確立することができない場合呼び出しは非暗号化メディアに戻って下るかもしれないし、必要があります。 CUCM および Expressway はこの場合矛盾しています。

Expressway は転送が伝送制御 プロトコル（TCP）または User Datagram Protocol （UDP; ユーザ データグラム プロトコル）である場合暗号化を常に拒否します。 メディア暗号化がほしいと思う場合 CUCM と Expressway 間の転送を保護して下さい。

SDP （CUCM としてそれを書きます）: 暗号化されたメディアは `m=RTP/SAVP` および `a=crypto` 行が

SDP に書かれていると同時に記述されています。 これはメディア暗号化のための正しいシグナリングですが、転送がセキュアではない場合暗号行は読解可能です。

CUCM が x cisco srtp ヘッダを見る場合、コールが非暗号化に戻って下るようにします。 このヘッダが不在である場合、CUCM はコールが暗号化を必要とすることを仮定します（フォールバックを許可しません）。

X8.2 現在で、Expressway は最もよい努力を CUCM がライン側のケースでするのと同じ方法します。

SDP（Expressway としてトランク側を書きます）: 暗号化されたメディアは `m=RTP/AVP` および `a=crypto` 行が SDP に書かれていると同時に記述されています。

ただし a=crypto 行が不在である可能性があることを、2 が推論しましたあります:

1. Expressway の SIP プロキシに/からの転送ホップがセキュアのとき、プロキシは安全でないホップの公開からそれらを防ぐために暗号行を除去します。
2. 返事パーティは信号を送るか、または暗号化をしないことをために暗号行をできないことに除去します。

CUCM の正しい SIP 正規化スクリプトの使用は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。

トラブルシューティング

現在のところ、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

関連読み取り

- 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 ソリューションガイド（リリース 2.0）のための最適化された会議ソリューション
- Cisco Expressway（SIP トランク）配置ガイドを持つ Cisco Unified Communications Manager（Cisco Expressway X8.2 および統一された CM 8.6x および 9.x のために）
- Cisco VCS（SIP トランク）配置ガイドを持つ Cisco Unified Communications Manager（Cisco VCS X8.2 および統一された CM 8.6.x および 9.x のために）
- Cisco VCS 配置ガイドでの Unified Communication モービルおよびリモートアクセス（Cisco VCS X8.2 および Cisco Unified CM 9.1(2)SU1 またはそれ以降のために）
- Cisco Expressway 配置ガイドでの Unified Communication モービルおよびリモートアクセス（Cisco Expressway X8.2 および Cisco Unified CM 9.1(2)SU1 またはそれ以降のために）

- テクニカル サポートとドキュメント – Cisco Systems

関連 RFC

- RFC 3261 SIP: Session Initiation Protocol
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: セキュリティ説明