目次

概要

多くのネットワーク管理者はセキュリティとの Cisco Unified Communications Manager Express（CME）設定することを選択します。 組み込み IOS 認証局（IOS-CA）の代りに、ネットワーク管理者は既存の公開鍵インフラストラクチャ（PKI）インフラストラクチャとセキュア CME を統合選択できます。 この資料にセキュア シグナリングと、およびサード パーティ 認証によってメディアを設定する方法を動作するためにセキュア CME 記述されています。

前提条件

要件

この資料は（CME）環境で Cisco Unified Communications Manager Express 動作するフル機能装備であると仮定します。 セキュア Cisco Unified CME で操作上である必要があるすべての電話は CME に登録に成功最初にできる必要があります。 CME を設定する方法の情報に関しては Cisco Unified Communications Manager Express な システム アドミニストレータ ガイドを参照して下さい。

この資料はまた音声およびセキュリティ機能が両方有効に なると仮定します。

使用するコンポーネント

この文書に記載されている情報は Cisco Unified Communications Manager Express に基づいています（CME）。

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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

注このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

サマリ コンフィギュレーションのステップ

1. IOS-CA 例を作成して下さい。
2. サード パーティ CA証明を保持するために trustpoints を作成して下さい。
3. trustpoints からの証明書署名要求（CSR）を生成して下さい。
4. サーバ認証 使用方法を用いる CSR に署名し、CA 認証を得て下さい。
5. CA 認証の trustpoints を認証し、それぞれ ID証明をインポートして下さい。
6. サード パーティ 認証 trustpoints を検証して下さい。
7. IOS CA CME トラストポイントを作成して下さい。
8. Certificate trust list （CTL） クライアントを設定して下さい。
9. 認証局 プロキシ 機能（CAPF）サーバを設定して下さい。
10. テレフォニーサービスを設定して下さい。
11. テスト電話を設定して下さい。
12. 確認事項。

詳細なコンフィギュレーション例

1. IOS-CA 例を作成して下さい。 IOS-CA 例は電話のローカルで固有の認証（LSC）に署名するのに使用する自己署名証明書を生成 します。
2. サード パーティ署名のための CSR を生成する trustpoints を作成して下さい。 これらの trustpoints は結局サード パーティ CA 認証、また CSR の結果である ID証明を保持します。

3. trustpoints からの生成する CSR。 **暗号 PKI は**コマンドを生成 します サード パーティ CA に署名するために提供される CSR を**登録します**。

   例 1：
   例 2：
4. サーバ認証権限の認証を生成するために 2 CSR を使用して下さい。
   注： 完全な証明書 チェーンが CA からの 2 つの認証の 1 つのために得られることは必要です。 証明書 チェーンは署名 CA からの CA および ID証明を両方提供します。認証がベース 64 形式でダウンロードされるようにして下さい。CA 認証が各トラストポイントの認証のために使用されることは、そして ID証明が各トラストポイントにインポートされることその順序で非常に重要、です。
5. CA証明が付いている trustpoints を認証し、SAST ID証明をインポートして下さい。

   例 1：

例 2：

6. CA および ID証明が両方それぞれ trustpoints にロードされたら、各トラストポイントのための証明書 チェーンを検証して下さい。 このステップは前の手順が正常に完了したことを確認します。

7. IOS CA CME トラストポイントを作成して下さい。

   IOS-CA トラストポイントがクライアント認証に（電話が付いている Transport Level Security （TLS）接続）使用することができないので、別のトラストポイントを作成し、それに IOS-CA 認証を置いて下さい。

   このトラストポイントが TLS 接続のための IP 電話の要求使用されています（従ってそれらしかきちんと登録できます）承認しないのに。

8. CTL クライアントを設定して下さい。

   注 CTL ファイルが正常に作成されたことを確認して下さい:

9. CAPF サーバを設定して下さい。

10. テレフォニーサービスを設定して下さい。

11. 認証をアップグレードし、暗号化されたモードを使用するためにテスト電話（ephone）を設定して下さい。 設定が完了した、電話をリセットし、登録するために待って下さい。

    注: 電話がリセットされる前に、セキュリティとコンフィギュレーション既にあっていないことを確認して下さい。 セキュリティとコンフィギュレーションがある場合、手動で取除かれるか、または登録前に Cisco Unified CME を保護するためにテスト電話のファクトリリセットを完了する必要があります。

    電話をリセットするために、これらのコマンドを実行して下さい:電話が更新済 LSC を受け取ったら、証明書**オペレーション アップグレード auth モード ヌルストリング** コマンドは削除されます。

12. 電話が認証および暗号化両方と登録されたことを確認して下さい。

Cisco Unified CME をサード パーティ 認証とフル機能装備べきです保護して下さい。

関連情報

- Cisco Unified Communications Manager Express システム アドミニストレータ ガイド
- Cisco TAC Wiki の音声を保護して下さい
- テクニカルサポートとドキュメント - Cisco Systems