

IP Phone を使用する SSLVPN トンネルの設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[基本的な ASA SSL VPN のコンフィギュレーション](#)

[CUCM：自己署名証明書を使用した ASA SSL VPN のコンフィギュレーション](#)

[CUCM：サードパーティ証明書を使用した ASA SSL VPN のコンフィギュレーション](#)

[基本的な IOS SSL VPN のコンフィギュレーション](#)

[CUCM：自己署名証明書を使用した IOS SSL VPN のコンフィギュレーション](#)

[CUCM：サードパーティ証明書を使用した IOS SSL VPN のコンフィギュレーション](#)

[Unified CME：自己署名証明書またはサードパーティ証明書を使用した ASA またはルータの SSL VPN のコンフィギュレーション](#)

[SSL VPN を備えた UC 520 IP Phone の設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、WebVPN としても知られる Secure Sockets Layer VPN (SSL VPN) を介して IP Phone を設定する方法について説明します。このソリューションでは、2 つの Cisco Unified Communications Manager (CallManager) および 3 種類の証明書が使用されます。次に、使用する CallManager を示します。

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Communications Manager Express (Cisco Unified CME)

次に、使用する証明書タイプを示します。

- 自己署名証明書
- Entrust、Thawte および GoDaddy などのサードパーティ証明書
- Cisco IOS[®]/Adaptive Security Appliance (ASA) 認証局 (CA)

ここで理解しておく重要な概念は、SSL VPN ゲートウェイおよび CallManager の設定が完了したら、IP Phone にローカルで参加する必要があるということです。これにより、電話を CUCM に登録し、正しい VPN 情報および証明書を使用できます。電話は、ローカルに登録されない場合、SSL VPN ゲートウェイを検出できず、SSL VPN ハンドシェイクを完了する正しい証明書を使用できません。

一般的な設定は、ASA 自己署名証明書および Cisco IOS 自己署名証明書を使用した CUCM/Unified CME です。これは最も簡単な設定です。

前提条件

要件

次の項目に関する知識が推奨されます。

- Cisco Unified Communications Manager (CUCM) または Cisco Unified Communications Manager Express (Cisco Unified CME)
- SSL VPN (WebVPN)
- Cisco Adaptive Security Appliance (ASA)
- 証明書タイプ (自己署名、サードパーティ、認証局など)

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。

- ASA Premium ライセンス
- AnyConnect VPN phone ライセンス
 - ASA リリース 8.0.x の場合、ライセンスは、AnyConnect for Linksys Phone です。
 - ASA リリース 8.2.x 以降の場合、ライセンスは、AnyConnect for Cisco VPN Phone です。
- SSL VPN ゲートウェイ ASA 8.0 以降 (AnyConnect for Cisco VPN Phone ライセンス) または Cisco IOS ソフトウェア リリース 12.4T 以降
 - Cisco IOS ソフトウェア リリース 12.4T 以降は、『[SSL VPN コンフィギュレーションガイド](#)』で示されているように公式にはサポートされません。
 - Cisco IOS ソフトウェア リリース 15.0(1)M では、SSL VPN ゲートウェイは Cisco 880、Cisco 890、Cisco 1900、Cisco 2900、および Cisco 3900 の各プラットフォームでシート数のカウントによるライセンス方式の機能です。SSL VPN セッションを正常に行うには、有効なライセンスが必要です。
- CallManager : CUCM 8.0.1 以降または Unified CME 8.5 以降

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。

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。

特定の show コマンドが [アウトプット インタープリタ ツール \(登録ユーザ専用 \)](#) でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

基本的な ASA SSL VPN のコンフィギュレーション

基本的な ASA SSL VPN コンフィギュレーションについては、次のドキュメントで説明していません。

- [ASA 8.x : 自己署名証明書を使用した AnyConnect VPN クライアントによる VPN アクセスの設定例](#)
- [AnyConnect VPN Client 接続の設定](#)

このコンフィギュレーションが完了すると、リモートのテスト PC は、SSL VPN ゲートウェイへの接続、AnyConnect 経由の接続、および CUCM への ping ができるようになります。ASA に AnyConnect for Cisco IP Phone ライセンスがあることを確認します。(show ver コマンドを使用します。) TCP と UDP の両方のポート 443 をゲートウェイとクライアントの間で開いておく必要があります。

注: 負荷分散された SSL VPN は VPN 電話でサポートされません。

CUCM : 自己署名証明書を使用した ASA SSL VPN のコンフィギュレーション

詳細については、「[AnyConnect を使用した ASA への IP Phone SSL VPN](#)」を参照してください。

ASA には、AnyConnect for Cisco VPN Phone のライセンスが必要です。SSL VPN を設定したら、VPN の CUCM を設定します。

1. ASA から自己署名証明書をエクスポートするには、次のコマンドを使用します。

```
ciscoasa(config)# crypto ca export trustpoint name identity-certificate
```

このコマンドを使用すると、PEM エンコードされたアイデンティティ証明書が端末に表示されます。

2. 証明書をテキスト エディタにコピーおよびペーストして、.pem ファイルとして保存します。BEGIN CERTIFICATE および END CERTIFICATE ラインを含める必要があります。含めない場合は、証明書が正しくインポートされません。証明書の形式を変更しないでください。変更した場合、電話が ASA を認証するときに問題が発生します。
3. [Cisco Unified Operating System Administration] > [Security] > [Certificate Management] > [Upload Certificate/Certificate Chain] に移動して、CUCM の CERTIFICATE MANAGEMENT セクションに証明書ファイルをロードします。
4. ASA からの自己署名証明書のロードに使用したエリアと同じエリアから、CallManager.pem、CAPF.pem および Cisco_Manufacturing_CA.pem 証明書をダウンロードし (ステップ 1 を参照)、デスクトップに保存します。
 1. たとえば、CallManager.pem を ASA にインポートするには、次のコマンドを使用します

。

```
ciscoasa(config)# crypto ca trustpoint certificate-name
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate certificate-name
```

2. トラストポイントの対応する証明書をコピーおよびペーストするように要求されたら、保存したファイルを CUCM から開いて、Base64 エンコードされた証明書をコピーおよびペーストします。必ず BEGIN CERTIFICATE および END CERTIFICATE ライン (ハイフンを使用) を含めてください。
 3. end と入力して、[Return] を押します。
 4. 証明書を信頼するか求められたら、yes と入力し、Enter キーを押します。
 5. CUCM から他の 2 つの証明書 (CAPF.pem、Cisco_Manufacturing_CA.pem) で、ステップ 1 ~ 4 を繰り返します。
5. [CUCM IPphone VPN config.pdf](#) で説明されているように、正しい VPN 構成で CUCM を設定します。

注: CUCM で設定される VPN ゲートウェイは、VPN ゲートウェイで設定される URL と一致する必要があります。ゲートウェイおよび URL が一致しない場合、電話はアドレスを名前解決できません。VPN ゲートウェイではデバッグは表示されません。

- CUCM の場合、VPN ゲートウェイ URL は <https://192.168.1.1/VPNPhone> です。
- ASA では、次のコマンドを使用します。

```
ciscoasa# configure terminal
ciscoasa(config)# tunnel-group VPNPhones webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://192.168.1.1/VPNPhone
enable
ciscoasa(config-tunnel-webvpn)# exit
```

- これらのコマンドは、Adaptive Security Device Manager (ASDM) または接続プロファイルで使用できます。

CUCM : サードパーティ証明書を使用した ASA SSL VPN のコンフィギュレーション

このコンフィギュレーションは、「[CUCM : 自己署名証明書を使用した ASA SSLVPN のコンフィギュレーション](#)」セクションで説明されているコンフィギュレーションと非常に似ていますが、サードパーティ証明書を使用する点が異なります。「[ASA 8.x WebVPN で使用するサードパーティベンダーの証明書を手動でインストールする設定例](#)」で説明されているように、サードパーティ証明書を使用して ASA で SSL VPN を設定します。

注: すべての証明書チェーンを ASA から CUCM にコピーし、すべての中間およびルート証明書を含める必要があります。CUCM がチェーン全体を含んでいない場合、電話は認証に必要な証明書を持つことができず、SSL VPN ハンドシェイクは失敗します。

基本的な IOS SSL VPN のコンフィギュレーション

注: IP Phone は、IOS SSL VPN ではサポートされていません。コンフィギュレーションはベスト エフォートです。

基本的な Cisco IOS SSL VPN コンフィギュレーションについては、次のドキュメントで説明しています。

- [SDM を使用した IOS での SSL VPN Client \(SVC \) の設定例](#)
- [IOS ゾーンベースのポリシーファイアウォールを使用した IOS ルータでの AnyConnect VPN クライアントの設定例](#)

このコンフィギュレーションが完了すると、リモートのテスト PC は、SSL VPN ゲートウェイへの接続、AnyConnect 経由の接続、および CUCM への ping ができるようになります。Cisco IOS 15.0 以降では、このタスクを完了するために有効な SSL VPN ライセンスが必要です。TCP と UDP の両方のポート 443 をゲートウェイとクライアントの間で開いておく必要があります。

CUCM : 自己署名証明書を使用した IOS SSL VPN のコンフィギュレーション

このコンフィギュレーションは、「[CUCM : サードパーティ証明書を使用した ASA SSLVPN のコンフィギュレーション](#)」および「[CUCM : 自己署名証明書を使用した ASA SSLVPN のコンフィギュレーション](#)」セクションで説明されているコンフィギュレーションと似ています。次に、これらの違いを示します。

1. ルータから自己署名証明書をエクスポートするには、次のコマンドを使用します。

```
R1(config)# crypto pki export trustpoint-name pem terminal
```

2. CUCM 証明書をインポートするには、次のコマンドを使用します。

```
R1(config)# crypto pki trustpoint certificate-name  
R1(config-ca-trustpoint)# enrollment terminal  
R1(config)# crypto ca authenticate certificate-name
```

WebVPN コンテキスト コンフィギュレーションにより、次のテキストが示されます。

```
R1(config)# crypto pki trustpoint certificate-name  
R1(config-ca-trustpoint)# enrollment terminal  
R1(config)# crypto ca authenticate certificate-name
```

「[CUCM : 自己署名証明書を使用した ASA SSLVPN のコンフィギュレーション](#)」セクションで説明されているコンフィギュレーションと似ています。

CUCM : サードパーティ証明書を使用した IOS SSL VPN のコンフィギュレーション

このコンフィギュレーションは、「[CUCM : 自己署名証明書を使用した ASA SSLVPN のコンフィギュレーション](#)」セクションで説明されているコンフィギュレーションと似ています。サードパーティ証明書を使用して WebVPN を設定します。

注: すべての WebVPN 証明書チェーンを CUCM にコピーし、すべての中間およびルート証明書を含める必要があります。CUCM がチェーン全体を含んでいない場合、電話は認証に必要な証明書を持つことができず、SSL VPN ハンドシェイクは失敗します。

Unified CME : 自己署名証明書またはサードパーティ証明書を使用した ASA また

はルータの SSL VPN のコンフィギュレーション

Unified CME のコンフィギュレーションは、CUCM のコンフィギュレーションと似ています。たとえば、WebVPN エンドポイント コンフィギュレーションは同じです。大きな違いは、Unified CME コール エージェントのコンフィギュレーションだけです。「[SCCP IP Phone に SSL VPN クライアントを設定](#)」で説明されているように、Unified CME の VPN グループおよび VPN ポリシーを設定します。

注: Unified CME は、Skinny Call Control Protocol (SCCP) のみをサポートし、VPN Phone のセッション開始プロトコル (SIP) はサポートしません。

注: 証明書を Unified CME から ASA またはルータにエクスポートする必要はありません。必要なことは、証明書を ASA またはルータ WebVPN ゲートウェイから Unified CME にエクスポートすることだけです。

証明書を WebVPN ゲートウェイからエクスポートするには、ASA/ルータのセクションを参照してください。サードパーティ証明書を使用する場合、すべての証明書チェーンを含める必要があります。証明書を Unified CME にインポートするには、証明書をルータにインポートしたときに使用した方法と同じ方法で行います。

```
CME(config)# crypto pki trustpoint certificate-name
CME(config-ca-trustpoint)# enrollment terminal
CME(config)# crypto ca authenticate certificate-name
```

SSL VPN を備えた UC 520 IP Phone の設定

Cisco Unified Communications 500 シリーズ モデル UC 520 IP Phone は、CUCM および CME コンフィギュレーションとは異なります。

- UC 520 IP Phone は CallManager および WebVPN の両方のゲートウェイなので、これらの間で証明書を設定する必要はありません。
- 自己署名証明書またはサードパーティ証明書で通常行うように、ルータで WebVPN を設定します。
- UC 520 IP Phone には、WebVPN クライアントが組み込まれています。これは、通常の PC と WebVPN の接続のように設定できます。ゲートウェイを入力して、ユーザ名/パスワードの組み合わせを入力します。
- UC 520 IP Phone は、Cisco Small Business IP Phone SPA 525G 電話と互換性があります。

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。