

ASA の証明書認証で AnyConnect VPN 電話を設定して下さい

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[電話機の証明書タイプ](#)

[設定](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料は IP フォンを on Cisco 実行する AnyConnect クライアントに証明書認証を提供する (ASA) および CallManagerデバイスを適応型セキュリティ アプライアンス (ASA) ソフトウェア設定する方法を示す設定 例を提供したものです。この設定が完了すると、Cisco IP Phone で、通信を保護するための証明書を使用できるようにする ASA への VPN 接続を確立できます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- AnyConnect Premium SSL のライセンス
- AnyConnect for Cisco VPN Phone のライセンス

ASA バージョンに応じて、ASA リリース 8.0.x では「AnyConnect for Linksys phonet」または ASA Release 8.2.x 以降では「AAnyConnect for Cisco VPN Phone」と表示されます。

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 : リリース 8.0(4) 以降
- IP Phone のモデル : 7942/7962/7945/7965/7975
- 電話機 : リリース 9.1(1) ファームウェアを実行する 8961/9951/9971
- Phone : リリース 9.0(2)SR1S : Skinny Call Control Protocol (SCCP) 以降
- Cisco Unified Communications Manager (CUCM) : リリース 8.0.1.100000-4 以降

この設定例で使用しているリリースには次のものが含まれています。

- ASA : リリース 9.1(1)
- CallManager リリース 8.5.1.10000-26

使用している CUCM のバージョンでサポートされる電話機の完全なリストについては、次の手順を実行してください。

1. この URL : [https:// <CUCM Server IP Address>:8443/cucreports/systemReports.do](https://<CUCM Server IP Address>:8443/cucreports/systemReports.do) を開きます。
2. [Unified CM Phone Feature List] > [Generate a new report] > [Feature: Virtual Private Network] の順に選択します。

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。

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。

電話機の証明書タイプ

シスコでは、電話機で次の証明書タイプを使用します。

- 製造元でインストールされる証明書 (MIC) : MIC はすべての 7941、7961、および新しいモデルの Cisco IP Phone に含まれます。MIC はシスコの認証局 (CA) によって署名された 2048 ビット キー証明書です。MIC がある場合、ローカルで有効な証明書 (LSC) をインストールする必要はありません。CUCM で MIC の証明書を信頼するためには、証明書信頼ストアに前もってインストールされた CA 証明書 CAP-RTP-001、CAP-RTP-002、および Cisco_Manufacturing_CA を使用します。
- LSC : LSC は、認証または暗号化のデバイス セキュリティ モードを設定した後から CUCM と電話機間の接続を保護します。LSC は、CUCM Certificate Authority Proxy Function (CAPF) 秘密キーで署名された Cisco IP Phone の公開キーを処理します。これは、管理者が手動でプロビジョニングした Cisco IP Phone だけが CTL ファイルをダウンロードして確認できるため、推奨方式です (MIC の使用とは異なります)。注: セキュリティのリスクが高まっているため、LSC のインストールで MIC は単独で使用し、継続的に使用しないことをシスコは推奨します。Transport Layer Security (TLS) の認証またはその他の目的で MIC を使用するために Cisco IP Phone を設定するお客様は、ご自身の責任において行ってください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

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。

設定

このドキュメントでは、以下の設定について説明します。

- ASA の設定
- CallManager の設定
- CallManager での VPN の設定
- IP Phone への証明書のインストール

ASA の設定

ASA の設定は、AnyConnect のクライアント コンピュータを ASA に接続するときとほとんど同じです。ただし、次の制約事項が適用されます。

- トンネル グループには、グループ URL が必要です。この URL は、VPN ゲートウェイ URL にある CM で設定されます。
- グループ ポリシーは、スプリット トンネルに含まれません。

この設定は、ASA デバイスのセキュア ソケット レイヤ (SSL) トラストポイントに設定およびインストールされた ASA (自己署名またはサードパーティ) 証明書を使用します。詳細は、次のドキュメントを参照してください。

- [デジタル証明書の設定](#)
- [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](#)
- [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](#)

ASA の関連する設定は次のとおりです。

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client
```

```
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable
```

```
ssl trust-point SSL outside
```

CallManager 設定

証明書を ASA からエクスポートし、電話機 VPN 信頼の証明書として CallManager にこの証明書をインポートするには、次の手順を実行してください。

1. CUCM を使用して生成された証明書を登録します。
2. SSL に使用されている証明書を確認します。

```
ASA(config)#show run ssl
ssl trust-point SSL outside
```
3. 証明書をエクスポートします。

```
ASA(config)#crypto ca export SSL identity-certificate
```

プライバシー強化メール (PEM) でエンコードされた ID 証明書は次のとおりです。

```
ASA(config)#crypto ca export SSL identity-certificate
```
4. 端末からのテキストをコピーし、.pem ファイルとして保存します。
5. CallManager にログインし、[Unified OS Administration] > [Security] > [Certificate Management] > [Upload Certificate] > [Select Phone-VPN-trust] の順に選択し、前の手順で保存した証明書ファイルをアップロードします。

CallManager での VPN 設定

1. Cisco Unified CM の管理ページに移動します。
2. メニューバーで、[Advanced Features] > [VPN] > [VPN Gateway] の順に選択します。
3. [VPN Gateway Configuration] ウィンドウで、次の手順を実行してください。[VPN Map Name] フィールドで、名前を入力します。これは、どんな名前にもできます。[VPN Gateway Description] フィールドに説明を入力します (任意選択)。[VPN Gateway URL] フィールドに ASA で定義されたグループ URL を入力します。この [Location] フィールド内の [VPN Certificates] で、信頼ストアからこの場所に移動するために以前の手順で CallManager にアップロードした証明書を選択します。
4. メニューバーで、[Advanced Features] > [VPN] > [VPN Group] の順に選択します。
5. [All Available VPN Gateways] フィールドで、以前に定義された VPN ゲートウェイを選択します。下矢印をクリックして選択したゲートウェイを移動し、この [VPN Group] フィールドの [Selected VPN Gateways] に移動します。
6. メニューバーで、[Advanced Features] > [VPN] > [VPN Profile] の順に選択します。
7. VPN のプロファイルを設定するには、アスタリスク (*) でマーキングされているすべてのフィールドを入力します。[Enable Auto Network Detect] : イネーブルにした場合、VPN の電話機は TFTP サーバの ping を行い応答がない場合は、VPN の接続を自動的に開始します。[Enable Host ID Check] : イネーブルにした場合、VPN の電話機は VPN のゲートウェイ URL の FQDN を、証明書の CN/SAN と比較します。これらが一致しない場合、またはアスタリスク (*) を使ったワイルドカードの証明書が使用されていた場合は、接続は失敗します。[Enable Password Persistence] : これによって VPN の電話機が次の VPN を行うときのためにユーザ名とパスワードをキャッシュすることができます。
8. 新しい VPN 設定を適用するには、[Common Phone Profile Configuration] ウィンドウで [Apply Config] をクリックします。「Standard Common Phone Profile」を使用するか、または新しいプロファイルを作成できます。
9. 特定の電話/ユーザの新しいプロファイルを作成した場合、[Phone Configuration] ウィンドウに移動します。[Common Phone Profile] フィールドで、[Standard Common Phone Profile] を選択します。
10. 新しい設定をダウンロードするために CallManager に電話を再び登録します。

証明書認証の設定

証明書認証を設定するには、CallManager および ASA で次の手順を実行してください。

1. メニューバーで、[Advanced Features] > [VPN] > [VPN Profile] の順に選択します。
2. [Client Authentication Method] フィールドが [Certificate] に設定されていることを確認します。
3. CallManager にログインします。メニューバーから、[Unified OS Administration] > [Security] > [Certificate Management] > [Find] を順に選択します。
4. 選択した証明書認証方法に対して正しい証明書をエクスポートします。MIC :
Cisco_Manufacturing_CA : MIC を使用して認証された IP Phone
LSC: Cisco Certificate Authority Proxy Function (CAPF) : LSC を使用して認証された IP Phone
5. Cisco_Manufacturing_CA または CAPF の証明書を見つけます。 .pem ファイルをダウンロードし、 .txt ファイルとして保存します。
6. ASA に新しいトラストポイントを作成し、以前に保存された証明書でこのトラストポイントを認証します。 Base 64 で符号化された CA 証明書から入力を促される場合、ダウンロードされた .pem ファイルの BEGIN 行から END 行までのテキスト選択し、貼り付けます。次に例を示します。

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

7. トンネルグループの認証が証明書認証に設定されていることを確認します。

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

IP Phone の証明書のインストール

IP Phone は MIC または LSC のいずれかで機能することができますが、それぞれの証明書で設定プロセスは異なります。

MIC のインストール

デフォルトでは、VPN をサポートするすべての電話には MIC がプレロードされています。 7960 および 7940 電話機には MIC が初期設定されていないため、安全に登録するために LSC の特別なインストール手順が必要です。

注: シスコでは、LSC のインストールのみに MIC を使用することを推奨します。シスコでは、CUCM との TLS 接続を認証する LSC をサポートします。。MIC ルート証明書は危険にさらされることがあるので、TLS の認証またはその他の目的で MIC を使用するために電話機を設定するお客様は、ご自身の責任において行ってください。シスコでは、MIC が危険にさらされることに責任を負いません。

LSC のインストール

1. CUCM で CAPF サービスを有効にします。
2. CAPF サービスがアクティブになった後、CUCM で LSC を生成するために電話手順を割り当てます。Cisco Unified CM の管理ページにログインし、[Device] > [Phone] の順に選択します。設定した電話機を選択します。
3. [Certificate Authority Proxy Function (CAPF) Information] セクションで、すべての設定が正

しく、動作が将来の日時に設定されていることを確認します。

4. [Authentication Mode] がヌル スtring または [Existing Certificate] に設定されている場合、これ以上の処置は必要ではありません。
5. [Authentication Mode] が文字列に設定されている場合、電話機のコンソールで手動で [Settings] > [Security Configuration] > [*#] > [LSC] > [Update] の順に選択します。

確認

このセクションでは、設定が正常に機能していることを確認します。

ASA による確認

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXXX
```

```
Index : 57
```

```
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
```

```
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
```

```
DTLS-Tunnel: (1)AES128
```

```
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
```

```
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
```

```
Bytes Rx : 270069Pkts Tx : 5645
```

```
Pkts Rx : 5650Pkts Tx Drop : 0
```

```
Pkts Rx Drop : 0Group Policy :
```

```
GroupPolicy_SSL Tunnel Group : SSL
```

```
Login Time : 01:40:44 UTC Tue Feb 5 2013
```

```
Duration : 23h:00m:28s
```

```
Inactivity : 0h:00m:00s
```

```
NAC Result : Unknown
```

```
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
```

```
SSL-Tunnel Tunnels: 1
```

```
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
```

```
Tunnel ID : 57.1
```

```
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
```

```
Encryption : AES128 Hashing : SHA1
```

```
Encapsulation: TLSv1.0 TCP Dst Port : 443
```

```
Auth Mode : Certificate
```

```
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
```

```
Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
```

```
Bytes Tx : 1759 Bytes Rx : 799
```

```
Pkts Tx : 2 Pkts Rx : 1
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
SSL-Tunnel:
```

```
Tunnel ID : 57.2
```

```
Public IP : 172.16.250.15
```

```
Encryption : AES128 Hashing : SHA1
```

```
Encapsulation: TLSv1.0 TCP Src Port : 50529
```

```
TCP Dst Port : 443 Auth Mode : Certificate
```

```
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
```

Client Type : SSL VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 835 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 57.3
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 51096
UDP Dst Port : 443 Auth Mode : Certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)
Bytes Tx : 303255 Bytes Rx : 269270
Pkts Tx : 5642 Pkts Rx : 5649
Pkts Tx Drop : 0 Pkts Rx Drop : 0

CUCM による確認

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。

関連するバグ

- Cisco Bug ID [CSCtf09529](#)、8961、9951、9971 電話機への CUCM での VPN 機能のサポートの追加
- Cisco [Bug ID CSCuc71462](#)、IP Phone VPN フェールオーバーに 8 分間かかる
- Cisco [Bug ID CSCtz42052](#)、非デフォルトのポート番号の IP Phone SSL VPN サポート
- Cisco [Bug ID CSCth96551](#)、電話機の VPN のユーザとパスワードでログイン中は、サポートされない ASCII 文字があります。
- Cisco バグ ID [CSCuj71475](#)、IP Phone VPN のために必要とされる TFTP 手動エントリ
- Cisco バグ ID [CSCum10683](#)、IP 電話記録抜けていた、送信されたか、または受信された呼び出し

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)