

VPN電話の設定とトラブルシューティング

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ASA の設定](#)

[CUCM の設定](#)

[トラブルシューティング](#)

[収集するデータ](#)

[一般的な問題](#)

[ASA自己署名ID証明書の更新](#)

[ASAが楕円曲線\(EC\)暗号を選択](#)

[DTLS接続の失敗](#)

[証明書の更新後、電話機がASAに接続できない](#)

[電話機がDNS経由でASA URLを解決できない](#)

[電話機でVPNが有効にならない](#)

[電話機が登録されているが、通話履歴を表示できない](#)

[関連情報](#)

概要

このドキュメントでは、Cisco IP PhoneおよびCisco Unified Communications ManagerのVPN Phone機能を設定およびトラブルシューティング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。

- Cisco Unified Communications Manager (CUCM)
- Cisco Adaptive Security Appliance (ASA)
- AnyConnectバーチャルプライベートネットワーク(VPN)
- Cisco IP フォン

使用するコンポーネント

- 8861 14-0-1-0101-145
- ASAv 9.12(2)9

- CUCM 11.5.1.21900-40

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この記事のテスト環境には、8861、ASA v、およびCUCM 11.5.1が含まれますが、これらの製品には、さまざまなバリエーションがあります。使用している電話機モデルがVPN機能をサポートしていることを確認するには、CUCMの[Phone Feature List]を確認する必要があります。電話機能リストを使用するには、ブラウザでCUCMパブリッシャにアクセスし、[Cisco Unified Reporting] > [Unified CM Phone Feature List]に移動します。新しいレポートを生成し、ドロップダウンから電話機のモデルを選択します。次に、図に示すように、[List Features]セクションで[Virtual Private Network Client]を検索する必要があります。

Unified CM Phone Feature List

Provides a complete list of features available to products supported by Unified CM.
Created on Wed Apr 01 09:41:27 EDT 2020

Product:

Feature:

Unified CM Cluster Name

Cluster Name	Publisher Name/IP
cucm1251	cucm1251

List Features

Product	Protocol	Feature Name
Cisco 7962	SCCP	Security By Default
Cisco 7962	SCCP	Security Encryption
Cisco 7962	SCCP	Shared Line Appearance
Cisco 7962	SCCP	Show Speeddial Labels
Cisco 7962	SCCP	Single Button Barge
Cisco 7962	SCCP	Size Safe on Phone Template
Cisco 7962	SCCP	Support CAPF
Cisco 7962	SCCP	Trusted Device
Cisco 7962	SCCP	Use Generic Icon
Cisco 7962	SCCP	User Hold
Cisco 7962	SCCP	Video
Cisco 7962	SCCP	Virtual Private Network Client
Cisco 7962	SIP	7915 12-Button Line Expansion Module
Cisco 7962	SIP	7915 24-Button Line Expansion Module
Cisco 7962	SIP	7916 12-Button Line Expansion Module

設定

VPN電話では、ASAとCUCMで適切な設定が必要です。最初にどちらの製品から開始できますが、このドキュメントでは最初にASAの設定について説明します。

ASA の設定

手順1:ASAがVPN電話のAnyConnectをサポートするライセンスを取得していることを確認します。ASAでshow versionコマンドを使用すると、Anyconnect for Cisco VPN Phoneが有効になっていることを次のスニペットで確認できます。

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

この機能が有効になっていない場合は、ライセンスチームと協力して適切なライセンスを取得する必要があります。ASAがVPN電話をサポートしていることを確認したので、設定を開始できます。

注：設定セクションの下線が引かれたすべての項目は、変更可能な名前です。これらの名前のほとんどは設定内の他の場所で参照されるため、後で必要になるため、これらのセクションで使用する名前（グループポリシー、トンネルグループなど）を覚えておくことが重要です。

ステップ2:VPNクライアントのIPアドレスプールを作成します。これは、IP PhoneがASAに接続するときに、このプールからIPアドレスを受信するという点で、DHCPプールに似ています。プールは、ASAで次のコマンドを使用して作成できます。

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0
```

また、別のネットワークまたはサブネットマスクを使用する場合は、これを変更することもできます。プールを作成したら、グループポリシー（ASAとIP電話間の接続に関する一連のパラメータ）を設定する必要があります。

```
group-policy vpn-phone-policy internal
```

```
group-policy vpn-phone-policy属性
```

```
split-tunnel-policy tunnelall
```

vpn-tunnel-protocol ssl-client

ステップ3:AnyConnectが有効になっていない場合は、有効にする必要があります。 これを行うには、外部インターフェイスの名前を知っている必要があります。 通常、このインターフェイスの名前は**outside** (スニペットに示されているように) ですが、設定可能であるため、適切なインターフェイスがあることを確認してください。 `show ip`を実行して、インターフェイスのリストを表示します。

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

この環境では、外部インターフェイスの名前は**outside**であるため、これらのコマンドはそのインターフェイスでAnyConnectを有効にします。

webvpn

外部を有効にする
`anyconnect enable`

ステップ4：新しいトンネルグループを設定して、以前に作成したグループポリシーを、特定のURLに接続するすべてのクライアントに適用します。 スニペットの3行目と4行目の前に作成したIPアドレスプールとグループポリシーの名前に注目してください。 IPアドレスプールまたはグループポリシーの名前を変更した場合は、修正した名前ですべての値を置き換える必要があります。

```
tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
  address-pool vpn-phone-pool
  default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attributes
  認証証明書
  group-url https://asav.sckiewer.lab/phone enable
```

グループURLの名前ではなく、IPアドレスを使用できます。 これは通常、電話機がASAの完全修飾ドメイン名(FQDN)を解決できるDNSサーバにアクセスできない場合に行われます。 また、この例では証明書ベースの認証が使用されていることも確認できます。 ユーザ名/パスワード認証も使用できますが、このドキュメントの範囲外であるASAに関する要件が多くあります。

この例では、DNSサーバにAレコード**asav.sckiewer.lab - 172.16.1.250**があり、`show ip`出力から**outside**という名前のインターフェイスに**172.16.1.250**が設定されていることがわかります。 設定は次のようになります。

crypto ca trustpoint asa-identity-cert

登録セルフ

`subject-name CN=asav.sckiewer.lab`

crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert outside

注意すべき点がいくつかあります。

1. asa-identity-certという名前の新しいトラストポイントが作成され、サブジェクト名が適用されました。これにより、このトラストポイントから生成された証明書は、指定されたサブジェクト名を使用します
2. 次に、「crypto ca enroll asa-identity-cert」コマンドを使用すると、ASAは自己署名証明書を生成し、そのトラストポイントに保存できます
3. 最後に、ASAはトラストポイント内の証明書を、外部インターフェイスに接続するすべてのデバイスに提示します

ステップ5:ASAがIP Phoneの証明書を信頼できるように、必要なトラストポイントを作成します。まず、IPフォンで製造元でインストールされる証明書(MIC)またはローカルで有効な証明書(LSC)が使用されているかどうかを確認する必要があります。デフォルトでは、LSCがインストールされていない限り、すべての電話機がセキュア接続にMICを使用します。CUCM 11.5.1以降では、[Unified CM Administration] > [Device] > [Phone]で検索を実行して、LSCがインストールされているかどうかを確認できます。一方、古いバージョンのCUCMでは、各電話機のセキュリティ設定を物理的に確認する必要があります。CUCM 11.5.1では、フィルタを追加(またはデフォルトフィルタを変更)する必要があることに注意してください。[LSC Issued By]列にNAが含まれるデバイスは、LSCがインストールされていないため、MICを使用します。

Device Name(LINE) *	Description	Extension	Owner User ID	LSC Status	LSC Expires	LSC Issued By	LSC Issuer Expires By	CAPF Auth String	Device P
DCTAAAAAAAAAAAAAA				None	NA	NA	NA		SIP
SEP38EC183318E	Auto 3010	3010		None	NA	NA	NA		SIP
SEP821C78C8DCE	Auto 3006	43782		None	NA	NA	NA		SIP
SEP6C3E18F21868	Auto 3009	3009		Troubleshoot Success	02/17/2025	CAPF-0999930F	05/01/2024		SIP
SEP4A8439C31A7C	Auto 3013	3013		None	NA	NA	NA		SIP
UCCK_T006	INITIAL_INBOUND_CCG-1			None	NA	NA	NA		SCCP

電話機が図で強調表示されているように見える場合、ASAが電話機の証明書をセキュア接続に対して検証するために、CUCMパブリッシャのCAPF証明書をASAにアップロードする必要があります。LSCがインストールされていないデバイスを使用する場合は、Cisco Manufacturing CertificatesをASAにアップロードする必要があります。これらの証明書は、CUCMパブリッシャの[Cisco Unified OS Administration] > [Security] > [Certificate Management]にあります。

注：これらの証明書の一部が複数の信頼ストア (CallManager-trustおよびCAPF-trust) で確認できます。これらの正確な名前を持つ証明書を選択する必要がある限り、証明書をダウンロードする信頼ストアは関係ありません。

- Cisco_Root_CA_2048 <MIC SHA-1ルート
- Cisco_Manufacturing_CA <MIC SHA-1中間体
- Cisco_Root_CA_M2 <MIC SHA-256ルート
- Cisco_Manufacturing_CA_SHA2 <MIC SHA-256中間体
- CUCMパブリッシャ< LSCからのCAPF

Certificate	Common Name	Type	Distribution	Issued By
CAPF	CAPF-bf1846f2	Self-signed	CAPF-bf1846f2	CAPF-bf1846f2

Buttons: Generate Self-signed, Upload Certificate/Certificate chain, Generate CSR, Download CSR

MICに関しては、79xxシリーズや99xxシリーズなどの古い電話機モデルではSHA-1証明書チェーンを使用し、88xxシリーズなどの新しい電話機モデルではSHA-256証明書チェーンを使用します。電話機が使用する証明書チェーンをASAにアップロードする必要があります。

必要な証明書を手に入れたら、次のコマンドでトラストポイントを作成できます。

crypto ca trustpoint cert1

登録端末

crypto ca authenticate cert1

最初のコマンドは、**cert1**という名前のトラストポイントを作成します。**crypto ca authenticate**コマンドを使用すると、base64でエンコードされた証明書をCLIに貼り付けることができます。これらのコマンドは、ASA上の適切なトラストポイントを取得するために必要な回数だけ実行できますが、証明書ごとに新しいトラストポイント名を使用してください。

ステップ6：次のコマンドを発行して、ASA ID証明書のコピーを取得します。

crypto ca export asa-identity-cert identity-certificate

これにより、**asa-identity-cert**という名前のトラストポイントのID証明書がエクスポートされます。必ず名前を調整して、ステップ4で作成したトラストポイントと一致するようにします。

ASAの完全なラボ設定を次に示します。

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
    split-tunnel-policy tunnelall
    vpn-tunnel-protocol ssl-client

webvpn
    enable outside
    anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
    address-pool vpn-phone-pool
    default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
    authentication certificate
    group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

この時点でASAの設定は完了しており、CUCMの設定に進むことができます。収集したASA証明書のコピーと、トンネルグループセクションで設定したURLが必要です。

CUCM の設定

ステップ1:CUCMで、[Cisco Unified OS Administration] > [Security] > [Certificate Management]に移動し、ASA証明書をphone-vpn-trustとしてアップロードします。

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

Status

1 records found

Certificate List (1 - 1 of 1)

Find Certificate List where Certificate begins with phone-vpn Find Clear Filter + -




Certificate ^	Common Name	Type
Phone-VPN-trust	asav.sckiewer.lab	Self-signed

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR


ステップ2 :これが完了したら、[Cisco Unified CM Administration] > [Advanced Features] > [VPN] > [VPN Profile]に移動して、新しいプロファイルを作成します。このセクションには正しい設定も間違いもありません。各設定の目的を理解することが重要です。

1. **Enable Auto Network Detect** : この機能を有効にすると、電話機の電源がオンになると、電話機からTFTPサーバにpingが送信されます。このpingに対する応答を受信すると、VPNは有効になりません。このpingに対する応答を電話機が受信しない場合は、VPNを有効にします。この設定を有効にすると、VPNを手動で有効にすることはできません。
2. **ホストIDの確認** : このチェックボックスがオンの場合、電話機は設定ファイル (<https://asav.sckiewer.lab/phone>を使用)からVPN URLを検査し、ホスト名またはFQDNがASAが提示する証明書内の共通名(CN)またはSANエントリと一致することを確認します。
3. **認証方式**:ASAへの接続に使用される認証方式のタイプを制御します。このドキュメントの設定例では、証明書ベースの認証が使用されています。
4. **Password Persistence** : このオプションが有効になっている場合、ログインの失敗が発生するか、クライアントが手動でパスワードをクリアするか、電話機がリセットされるまで、クライアントのパスワードが電話機に保存されます。

VPN Profile Configuration

Save  Delete  Copy  Add New

Status

 Status: Ready

VPN Profile Information

Name*

Description

Enable Auto Network Detect

Tunnel Parameters

MTU*

Fail to Connect*


Enable Host ID Check

Client Authentication

Client Authentication Method*

Enable Password Persistence

Save Delete Copy Add New

ステップ3 : 次に、[Cisco Unified CM Administration] > [Advanced Features] > [VPN] > [VPN Gateway] に移動します。 VPNゲートウェイのURLがASA設定と一致していることを確認し、 に示すように、証明書を一番上のボックスから一番下のボックスに移動する必要があります。

VPN Gateway Configuration

Save

Status
 Status: Ready

VPN Gateway Information
 VPN Gateway Name* asav.sckiewer.lab
 VPN Gateway Description
 VPN Gateway URL* https://asav.sckiewer.lab/phone

VPN Gateway Certificates
 VPN Certificates in your Truststore
 VPN Certificates in this Location* SUBJECT: 2.5.4.5=#130b394144563639334c50454c+1.2.840.113549.1.9.2=#160d73636b69657765722d4153417

ステップ4：これが保存されたら、[Cisco Unified CM Administration] > [Advanced Features] > [VPN] > [VPN Group]に移動し、作成したゲートウェイを[Selected VPN Gateways in this VPN Group]ボックスに移動します。

VPN Group Configuration

Save

Status
 Status: Ready


VPN Group Information
 VPN Group Name* asav.sckiewer.lab
 VPN Group Description

VPN Gateway Information
 All Available VPN Gateways
 Selected VPN Gateways in this VPN Group asav.sckiewer.lab


ステップ5:VPN設定が完了したら、[Cisco Unified CM Administration] > [Device] > [Device Settings] > [Common Phone Profile]に移動します。ここで、目的のVPN電話で使用するプロファイルをコピーし、名前を変更して、VPNグループとVPNプロファイルを選択し、新しいプロファ

イルを保存する必要があります。

Common Phone Profile Configuration

 Save

Status

 Status: Ready

Common Phone Profile Information

Name*

Description

Local Phone Unlock Password

DND Option*

DND Incoming Call Alert*

Feature Control Policy

Wi-Fi Hotspot Profile [View Details](#)

Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User

Secure Shell Password

Phone Personalization Information

Phone Personalization*

Always Use Prime Line*

Always Use Prime Line for Voice Message*

Services Provisioning*

VPN Information

VPN Group

VPN Profile

ステップ6：最後に、この新しいプロファイルを電話機に適用し、内部ネットワーク上にある電話機をリセットする必要があります。これにより、電話機は、ASA証明書ハッシュやVPN URLなど、この新しい設定をすべて受信できます。

注：電話機をテストする前に、電話機に「代替TFTP」サーバが設定されていることを確認する必要があります。ASAは電話機にオプション150を提供しないため、TFTP IPを電話機に手動で設定する必要があります。

ステップ7:VPN電話をテストし、ASAに正常に接続して登録できることを確認します。 `show vpn-sessiondb anyconnect`を使用して、トンネルがASAでアップ状態であることを確認できます。

。

```
sckiewer-ASAv# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : CP-8841-SEP682C7B40B5CE
Index        : 3
Assigned IP   : 10.10.1.131      Public IP    : 192.168.1.52
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption    : AnyConnect-Parent: (1)AES256 SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 4275771          Bytes Rx     : 32476192
Group Policy  : VPN-Phone        Tunnel Group : VPN-Phone
Login Time    : 01:07:39 UTC Fri Mar 27 2020
Duration      : 4d 1h:56m:42s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A              VLAN         : none
Audt Sess ID  : 0e3051fa000030005e7d51db
Security Grp  : none
```

トラブルシュート

収集するデータ

VPN Phoneの問題をトラブルシューティングするには、次のデータが推奨されます。

- ASA Debugs: logging buffered debuglogging debug-tracedebug crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- 電話コンソールのログ(または電話がサポートしている場合はPRT – [詳細情報はこちら](#))

デバッグを有効にして問題を再現すると、デバッグ出力には常に711001が含まれるため、次のコマンドを使用して出力を表示できます。

```
show log | i 711001
```

一般的な問題

注：このセクションでは、VPN電話として導入されるより一般的な電話シリーズの1つであるため、ログスニペットは8861電話からのものです。他のモデルでは、ログに異なるメッセージを書き込むことができることを覚えておいてください。

ASA自己署名ID証明書の更新

ASA ID証明書の有効期限が切れる前に、新しい証明書を生成して電話機にプッシュする必要があります。VPN電話に影響を与えずに実行するには、次のプロセスを使用します。

ステップ1：新しいID証明書の新しいトラストポイントを作成します。

```
crypto ca trustpoint asa-identity-cert-2
```

登録セルフ

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

ステップ2：この時点で、ASAの新しいID証明書が作成されますが、どのインターフェイスでも使用されていません。この新しい証明書をエクスポートし、CUCMにアップロードする必要があります。

crypto ca export asa-identity-cert-2 identity-certificate

ステップ3：新しいID証明書を取得したら、Cisco Unified OS Administration > Security > Certificate Management > Uploadでphone-VPN-trustとしてCUCMノードのいずれかにアップロードします。

注：現在のphone-VPN-trust証明書は、最初にアップロードされたCUCMノードにのみ存在します（一部の証明書のような他のノードには自動的に伝搬されません）。CUCMバージョンがCSCuo58506の影響を受ける場合は、新しいASA証明書を別のノードにアップロードする必要があります。

ステップ4：新しい証明書がクラスタ内のいずれかのノードにアップロードされたら、CUCM Publisherで[Cisco Unified CM Administration] > [Advanced Features] > [VPN] > [VPN Gateway]に移動します

ステップ5：適切なゲートウェイを選択します。

ステップ6：一番上のボックスで証明書（アップロードしたばかりの証明書）を選択し、下矢印を選択して下に移動します（これにより、TFTPはその証明書をVPN Phoneの設定ファイルに追加できます）。

ステップ7：完了したら、すべてのVPN電話をリセットします。プロセスのこの時点で、ASAは古い証明書を提示するため、電話機は接続できませんが、新しい証明書と古い証明書の両方を含む新しい設定ファイルを取得します。

ステップ8：これで、新しい証明書をASAに適用できます。これを行うには、新しいトラストポイントの名前と外部インターフェイスの名前が必要です。次に、この情報を使用して次のコマンドを実行します。

ssl trust-point asa-identity-cert-2 outside

注：ブラウザでwebvpn URLに移動して、ASAが新しい証明書を提示することを確認できます。外部の電話機がアドレスに到達するには、そのアドレスがパブリックに到達可能である必要があるため、PCもアドレスに到達できます。その後、ASAがブラウザに提示する証明書を確認し、新しい証明書であることを確認できます。

ステップ9：新しい証明書を使用するようにASAを設定したら、テスト用の電話機をリセットし、ASAに接続して登録できることを確認します。電話機が正常に登録されると、すべての電話機をリセットし、ASAに接続して登録できることを確認できます。証明書の変更後、ASAに接続されている電話機は接続されたままになるため、このプロセスが推奨されます。最初に1台の電話機で証明書の更新をテストすると、設定の問題が多数の電話機に影響するリスクが低くなります。最初のVPN電話がASAに接続できない場合、他の電話が接続されたままの状態、トラブルシューティングのために電話またはASAからログを収集できます。

ステップ10：電話機が新しい証明書に接続して登録できることを確認したら、古い証明書をCUCMから削除できます。

ASAが楕円曲線(EC)暗号を選択

ASAは9.4(x)以降で楕円曲線(EC)暗号化をサポートしているため、ASAを9.4(x)以降にアップグレードした後に、以前に動作していたVPN電話で障害が発生することがよくあります。これは、ASAが新しい電話機モデルとのTLSハンドシェイク中にEC暗号を選択するために発生します。通常、前のASAバージョンがECをサポートしていなかったため、電話機が接続するインターフェイスに関連付けられたRSA証明書があります。この時点で、ASAはEC暗号を選択しているため、接続にRSA証明書を使用できないため、RSAではなくECアルゴリズムで作成する一時的な自己署名証明書を電話機に生成して送信します。この一時証明書は電話機で認識されないため、接続は失敗します。これは、88xxの電話ログでかなり簡単に確認できます。

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA
```

電話機のログには、「新しい暗号」行にEC暗号が含まれているため、ASAがこの接続に対してEC暗号を選択したことが示され、これが接続に失敗します。

AESを選択したシナリオでは、次のように表示されます。

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: AES256-SHA: AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-SHA: AES128-SHA
```

詳細については、CSCuu02848を参照して[ください](#)。

この問題を解決するには、電話機が使用するTLSバージョンのASAでEC暗号を無効にします。各電話機モデルがサポートするTLSバージョンの詳細については、次のサイトを参照してください。

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

Version	Phone Models			
	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware

** With 12.5 firmware

<https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone->

環境に関連するTLSバージョンがわかっただら、ASAで次のコマンドを実行して、それらのバージョンのEC暗号を無効にできます。

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"  
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"  
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"  
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-SHA256:AES128-SHA256:AES256-SHA"
```

IP電話はデフォルトでDTLS(Datagram Transport Layer Security)を使用するため、DTLSのcipher文と電話機に関連するTLSバージョンを実行する必要があることに注意してください。また、これらの変更はASAでのグローバルな変更であるため、これらのTLSバージョンを使用する他のAnyConnectクライアントによってEC暗号がネゴシエートされないことを理解することが重要です。

DTLS接続の失敗

場合によっては、VPN電話がDTLSを使用してASAへの接続を確立できません。電話機がDTLSを使用しようとしたが失敗した場合、電話機はDTLSが有効であることを認識しているため、DTLSを何度も試行し続けます。これは88xx電話機のログに表示されます。

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:  
fatal:illegal parameter  
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000  
status: 0x0 error: 0x0  
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal  
parameter  
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1,  
error 1  
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)  
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL  
routines:ssl3_get_server_hello:old session cipher not returned  
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,  
cleanup  
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:  
warning:close notify  
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed  
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect  
failed  
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success  
DTLS fail
```

これは、「[ASA Selecting Elliptic Curve \(EC\) Cipher](#)」セクションで説明したのと同じ問題が原因である可能性があり、DTLSでEC暗号を無効にする必要があります。その他にも、DTLSを無効にして、VPN電話が代わりにTLSを使用するようにすることもできます。これは、すべてのトラフィックがUDPではなくTCPを使用してオーバーヘッドが増加することを意味するため、理想的ではありません。ただし、一部のシナリオでは、設定の大部分が問題なく、DTLS固有の問題であることを少なくとも確認できるため、これは適切なテストです。これをテストする場合は、管理者が通常VPN電話に固有のグループポリシーを使用するため、グループポリシーレベルで行うのが最善です。これにより、他のクライアントに影響を与えずに変更をテストできます。

group-policy vpn-phone-policy属性

webvpn

anyconnect ssl dtls none

DTLS接続の成功を妨げるもう1つの一般的な設定の問題は、電話機が同じ暗号でTLSおよびDTLS接続を確立できない場合です。 ログの抜粋の例：

```
%%%% TLS Ciphers Offered
```

```
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

```
%%%% DTLS Ciphers Offered
```

```
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
```

```
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA
```

```
%%%% DTLS connection failure
```

```
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093, to abort connect
```

```
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

スニペットの最初の行で提供されるTLS暗号を確認できます。 両側でサポートされている最も安全なオプションが選択されています (ログには選択が表示されませんが、ログスニペットから少なくともAES-256であると推測できます)。 また、提供されるDTLS暗号化はAES128のみであることも確認できます。 選択したTLS暗号はDTLSで使用できないため、接続は失敗します。 このシナリオの修正は、ASA設定で同じ暗号をTLSおよびDTLSに使用できるようにすることです。

証明書の更新後、電話機がASAに接続できない

新しいASA ID証明書をphone-vpn-trustとしてCUCMにアップロードして、電話機がこの新しい証明書のハッシュを取得できるようにすることが非常に重要です。 このプロセスに従わない場合は、アップデート後にVPN PhoneがASAに接続しようとする、電話機に信頼できない証明書が提示されるため、接続が失敗します。 ASA証明書の更新後、証明書が変更されても電話機が切断されないため、数日または数週間後に発生する可能性があります。 ASAが電話機からキープアライブを受信し続ける限り、VPNトンネルはアップしたままです。 そのため、ASA証明書が更新されているものの、新しい証明書が最初にCUCMに配置されていないことを確認した場合は、次の2つのオプションがあります。

1. 古いASA ID証明書がまだ有効である場合は、ASAを古い証明書に戻し、このドキュメントで説明されている手順に従って証明書を更新します。 新しい証明書をすでに生成している場合は、証明書の生成セクションをスキップできます。
2. 古いASA ID証明書の有効期限が切れた場合は、新しいASA証明書をCUCMにアップロードし、電話機を内部ネットワークに戻して、新しい証明書ハッシュで更新された設定ファイルを受信する必要があります。

電話機がDNS経由でASA URLを解決できない

一部のシナリオでは、管理者がIPアドレスではなくホスト名を使用してVPN URLを設定します。 この処理を行う場合、電話機は名前をIPアドレスに解決するためにDNSサーバを持つ必要があります。 このスニペットでは、電話機が2つのDNSサーバ(192.168.1.1と192.168.1.2)で名前を解決しようとしたが、応答を受信しなかったことがわかります。 30秒後、電話機に「 DnsLookupErr:」が出力されます

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

これは通常、次のいずれかを示します。

1. 電話機に無効なDNSサーバがあります
2. 電話機がDHCP経由でDNSサーバを受信しなかったか、手動で設定されていない

この問題を解決するには、次の2つのオプションがあります。

1. 電話機の設定をチェックして、外部のDHCPサーバからDNSサーバを受信するか、電話機のDNSサーバがASA設定で使用される名前を解決できることを確認します
2. DNSが不要になるように、ASA設定とCUCMのURLをIPアドレスに変更します

電話機でVPNが有効にならない

このドキュメントで前述したように、Auto Network Detect (自動検出; 自動ネットワーク検出)により、電話機はTFTPサーバにpingを実行し、応答を確認します。電話機が内部ネットワークにある場合、VPNなしでTFTPサーバに到達できるため、電話機がpingに対する応答を受信すると、VPNは有効になりません。電話機が内部ネットワーク上にない場合、pingは失敗するため、電話機はVPNを有効にしてASAに接続します。クライアントのホームネットワークは、DHCP経由で電話にオプション150を提供するように設定されず、ASAもオプション150を提供できないため、「代替TFTP」がVPN電話の要件であることに注意してください。

ログでは、いくつかの点を確認します。

1. 電話機はCUCM TFTPサーバのIPにpingを実行しますか。
2. 電話機はpingに対する応答を受信しますか。
3. pingに対する応答を受信しない電話機はVPNを有効にしますか。

これらの項目をこの順序で表示することが重要です。電話機が誤ったIPに対してpingを実行し、応答を受信するシナリオでは、電話機がVPNを有効にしないため、ASAでデバッグを有効にしても意味がありません。不要なログ分析を防止できるように、これら3つの点をこの順序で検証します。pingが失敗し、その後VPNが有効になると、88xx電話ログに次のように表示されます。


```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

電話機が登録されているが、通話履歴を表示できない

電話機で代替TFTPが有効になっており、正しいTFTP IPが設定されていることを確認します。代替TFTPはVPN電話の要件です。これは、ASAがオプション150を提供できないためです。

関連情報

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