CUCM 11.5のユーザ単位(MRA)で認証および認可するためのSIP登録の設定

内容

概要

このドキュメントでは、Session Initiation Protocol(SIP)REGISTERメッセージのUserID認証の追加レイヤを提供するCisco Unified Communications Manager(CUCM)の拡張機能と、Expresswayでの現在の認証方式のみの拡張レイヤ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。

- CUCMの管理と設定
- SIPプロトコル
- Video Communication Server(VCS)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いています。

- Cisco Unified Communications Manager 11.5 以降
- Video Communication Server(VCS)Expressway

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

以前は、Video Communication Server(VCS)Expresswayを介したデバイス登録は、デバイスがハイパーテキスト転送プロトコル(HTTP)を介してユーザ名とパスワードを送信すると機能していました。 次に、Expresswayがユーザ名を認証し、デバイスがCUCMに対する登録を続行できるようにします。それ以上の検証は行われません。

新しい動作は、CUCMがSIP REGISTERメッセージをチェックし、ユーザIDがデバイスに適切に関連付けられていることを確認することです。この機能を使用して、UserIDをCUCMに登録する前に認可する必要があります。したがって、は、外部/不明ネットワークからのデバイスに対する次のレベルの保護を提供します。これにより、SIP REGISTERが承認されます。つまり、有効なユーザーに関連付けられた有効なデバイスのみが登録されます。デバイスにUserIDの関連付けがない場合、401応答コードで登録が拒否されます。

背景履歴

- CSCuu97283
- CVE ID CVE-2015-6410

制限

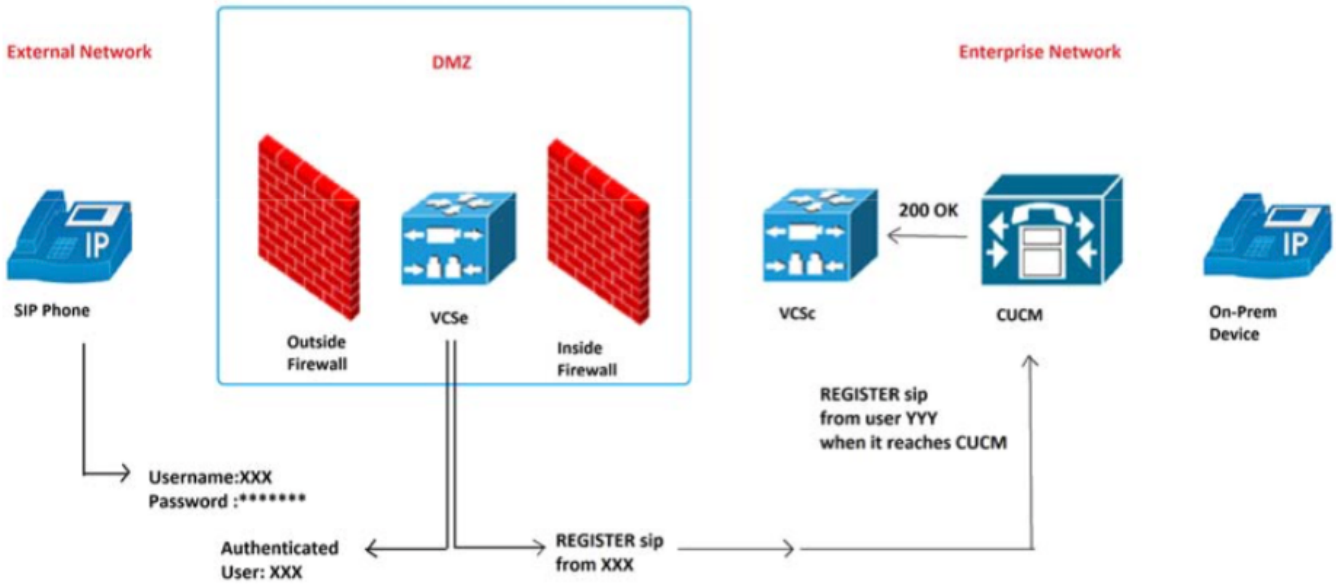
- SIP電話にのみ影響
- オンプレミス登録には影響はありません

設定

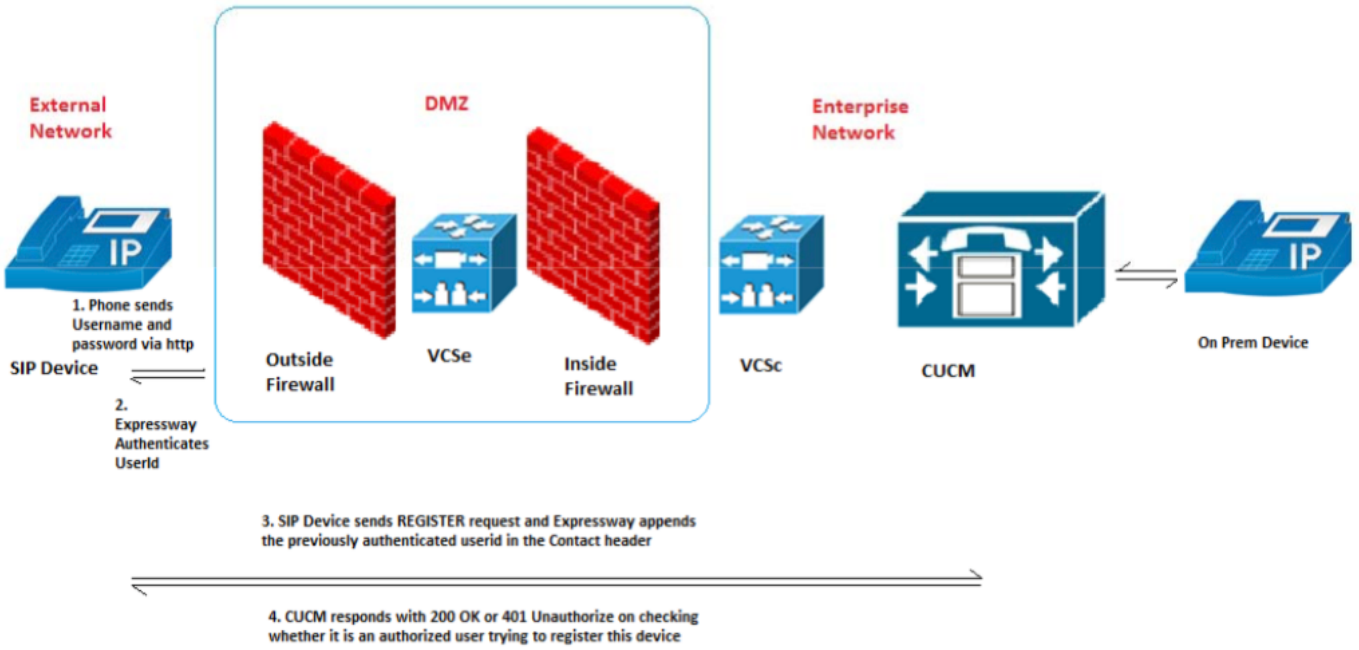
ネットワーク図

使用コンポーネント（旧アーキテクチャと新アーキテクチャ）

古い動作イメージ：



新しい動作イメージ：



設定

この機能のオン/オフを切り替える新しいサービスパラメータ：[System] > [Service Parameters] > [*server] > [Cisco CallManager] > [SIP Registration Authorization Enabled]*

値：

- True（デフォルト）
- False

正しいUserIDと正しいデバイスとの関連付けによって、SIP登録が許可または拒否されるかどうかが決まります。

登録承認プロセス要求は、次のシナリオに従います。

シナリオ1. UserIDがREGISTERメッセージに存在しない場合は、認証が必要で、200 OKが送信されます。

注：これにより、オンプレミスの相互運用性と、古いバージョンのExpresswayとの下位互換性が保証されます。

シナリオ2. REGISTERメッセージにUserIDが存在する場合…

- IF UserIDがCUCM Phone Configurationページのowner-idフィールドと一致した場合、AuthorizeおよびSend 200 OK
- IF UserIDがCUCM End User Configurationページのデバイスとの UserID関連付けと一致した場合、Authorize and send 200 OK
- 両方のowner-idフィールドが空白で、エンドユーザへのデバイスの関連付けが存在しない場合は、THEN Authorize and send 200 OK
- ELSE if no match, then FAIL and send 401 Unauthorized

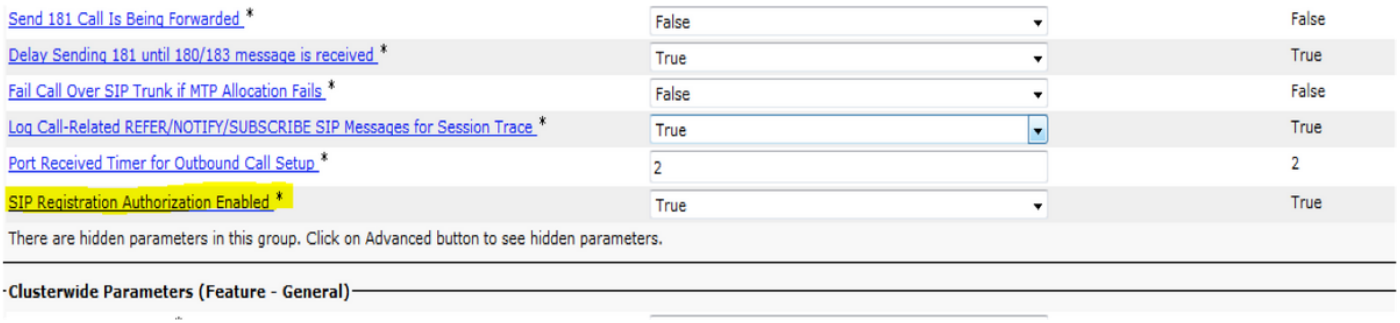
シナリオ3. REGISTERメッセージに複数の異なる値のUserIDが含まれている場合、THEN FAILと送信401 Unauthorized。

注：Expresswayのみがこれらの UserIDヘッダーを入力します

ユースケース結果テーブル

番号	テストケース	SIP登録許可の有効化	予想される結果
1	連絡先ヘッダーにUserIdパラメーターがありません	正しい	承認 (200 OK)
0	連絡先ヘッダーのUserIdパラメータが、電話設定ページのOwnerIdと一致します	正しい	承認 (200 OK)
3	連絡先ヘッダーのUserIdパラメータが、EndUserページのデバイスに関連付けられたuseridと一致します。	正しい	承認 (200 OK)
4	連絡先ヘッダーのUserIdが[電話の設定(Phone Config)]ページのownerIdと一致し、EndUserページで設定されたuseridと一致しません	正しい	承認 (200 OK)
5	連絡先ヘッダーのUserIdがEndUserページのuseridと一致し、Phone ConfigページのOwnerIdと一致しません	正しい	承認 (200 OK)
6	[電話の設定(Phone Config)]ページの[オーナーID(OwnerId)]が空白で、[エンドユーザ(EndUser)]ページにデバイスにユーザが関連付けられていません	正しい	承認 (200 OK)
7	[電話の設定(Phone Config)]ページのOwnerIdと[エンドユーザ(EndUser)]ページのデバイスに対して設定されたuseridですが、一致するものがありません	正しい	401不正
8	連絡先ヘッダーに複数のユーザIDがあります。	正しい	401不正
9 ミリ秒	[EndUser]ページのデバイスに複数のuseridが設定されている	正しい	承認(200 Ok)
10	エスケープされていないユーザID	正しい	承認(200 Ok)
11	レジスタの更新	正しい	初期REGISTERメッセージと同じ
12	連絡先ヘッダーのUserIdが空の文字列です。OwnerIdとUserIdがデバイスに設定されていません	正しい	承認(200 Ok)
13	連絡先ヘッダーのUserIdが空の文字列です。デバイスにOwnerId/UserIdが設定されています	正しい	401不正
14	連絡先ヘッダーにUserIdが存在し、デバイスにOwnerId/UserIdが設定されていますが、一致するものがありません	False	200 OK
15	連絡先ヘッダーに複数のuseridが存在します	False	200 OK
16	連絡先ヘッダーのUserIdが空の文字列です。デバイスにownerId /UserIdが構成されています	False	200 OK

Communications Manager(CCM)サービスパラメータを使用して機能を有効にします。これはデフォルトでオンになっており、これ以上の設定は必要ありません。



確認

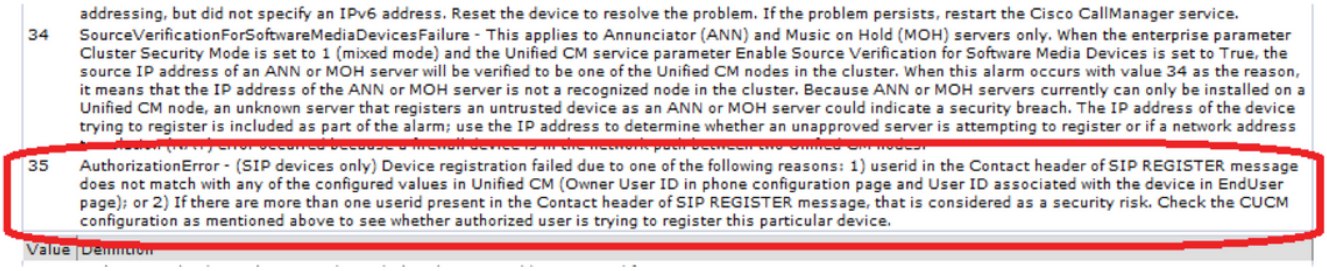
連絡先ヘッダー

CUCMは、Expresswayによる変更のためにREGISTERメッセージの連絡先ヘッダーをチェックします

```
Contact: <sip:ffeffb75-880e-f58f-a8ec-f5025d0f9136@10.50.179.6:5060;transport=tcp;orig-
hostport=192.168.0.121:55854>;+sip.instance="<urn:uuid:00000000-0000-0000-0000-
00506005457e>";+u.sip!model.ccm.cisco.com="604";+u.sip!userid.ccm.cisco.com="mjavie
r";+u.sip!serialno.ccm.cisco.com=A1AZ20D00153;audio=TRUE;video=TRUE;mobility="fixed";
duplex="full";description="TANDBERG-SIP“
```

新しいアラーム(AuthorizationError withWarningLevel)

SIP登録認証エラーが発生すると、新しいアラーム(AuthorizationError withWarningLevel)が使用可能になります



トラブルシュート

CCM Tracesのデバッグ出力で認証試行を探します。

成功した認可の例：

シナリオ１：

```
00013222.041 |15:46:20.792 |AppInfo |SIPStationD(7) - User Authorized - Phone Config page
```

シナリオ２：

```
00015642.041 |16:01:39.112 |AppInfo |SIPStationD(9) - User Authorized - EndUser page
```

失敗した認可とアラームの例：

00186341.041 |13:17:37.187 |AppInfo |SIPStationD(133) - User: shree is unauthorized to register a device
00186341.042 |13:17:37.187 |AppInfo |SIPStationD(133) - sendRegisterResp: non-200 response code 401, ccbId 2303, expires 4294967295, warning Authorization failure - Unauthorized user for this device 00186341.043 |13:17:37.188 |AppInfo |EndPointTransientConnection - An endpoint attempted to register but did not complete registration Connecting Port:5060 Device name: SEPCD1111000015 Device type:647 Reason Code:35 Protocol:SIP Device MAC address:CD1111000015 LastSignalReceived:SIPRegisterInd StationState:wait_register App ID:Cisco CallManager Cluster ID:10.77.29.71 Node ID:CuCM-71 00186341.044 |13:17:37.188 |AlarmWarn|AlarmClass: CallManager, AlarmName: EndPointTransientConnection, AlarmSeverity: Warning, AlarmMessage: , AlarmDescription: An endpoint attempted to register but did not complete registration, AlarmParameters: ConnectingPort:5060, DeviceName:SEPCD1111000015, DeviceType:647, Reason:35, Protocol:SIP, MACAddress:CD1111000015, LastSignalReceived:SIPRegisterInd, StationState:wait_register, AppID:Cisco CallManager, ClusterID:10.77.29.71, NodeID:CuCM-71, 00186346.000 |13:17:37.189 |SdlSig |SIPRegisterResp |wait |SIPHandler(1,100,80,1) |SIPStationD(1,100,74,133) |1,100,14,772.2^10.77.29.189^SEPCD1111000015 |[T:N-H:0,N:0,L:0,V:0,Z:0,D:0] ccbID= 2303 --TransType=1 --TransSecurity=0 PeerAddr= 10.77.29.189:5060 respCode= 401 action= 2 device=