配置SIP註冊以對CUCM 11.5進行身份驗證和基於每個使用者的授權(MRA)

目錄

簡介

本檔案介紹Cisco Unified Communications Manager(CUCM)中的增強行為，與目前僅在Expressway上進行身份驗證的方法相比，CUCM在會話發起協定(SIP)REGISTER消息中提供額外的一層UserID身份驗證。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM管理和配置
- SIP通訊協定
- 視訊通訊伺服器(VCS)Expressway

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科整合通訊管理員11.5及更新版本
- 視訊通訊伺服器(VCS)Expressway

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

過去，通過影片通訊伺服器(VCS)Expressway進行裝置註冊時，裝置會通過超文本傳輸協定

(HTTP)傳送使用者名稱和密碼。 然後，Expressway驗證使用者名稱並允許裝置繼續向CUCM註冊，而無需進一步驗證。

新的行為是，現在CUCM檢查SIP REGISTER消息並確保UserID與裝置正確關聯。通過此功能，UserID應在註冊到CUCM之前獲得授權；因此，提供針對來自外部/未知網路的裝置的下一級保護。這可確保SIP REGISTER獲得授權，即只有與有效使用者關聯的有效裝置才應註冊。如果沒有UserID與裝置的關聯，則註冊將以401響應代碼拒絕。

背景歷史

- CSCuu97283
- CVE ID CVE-2015-6410

限制

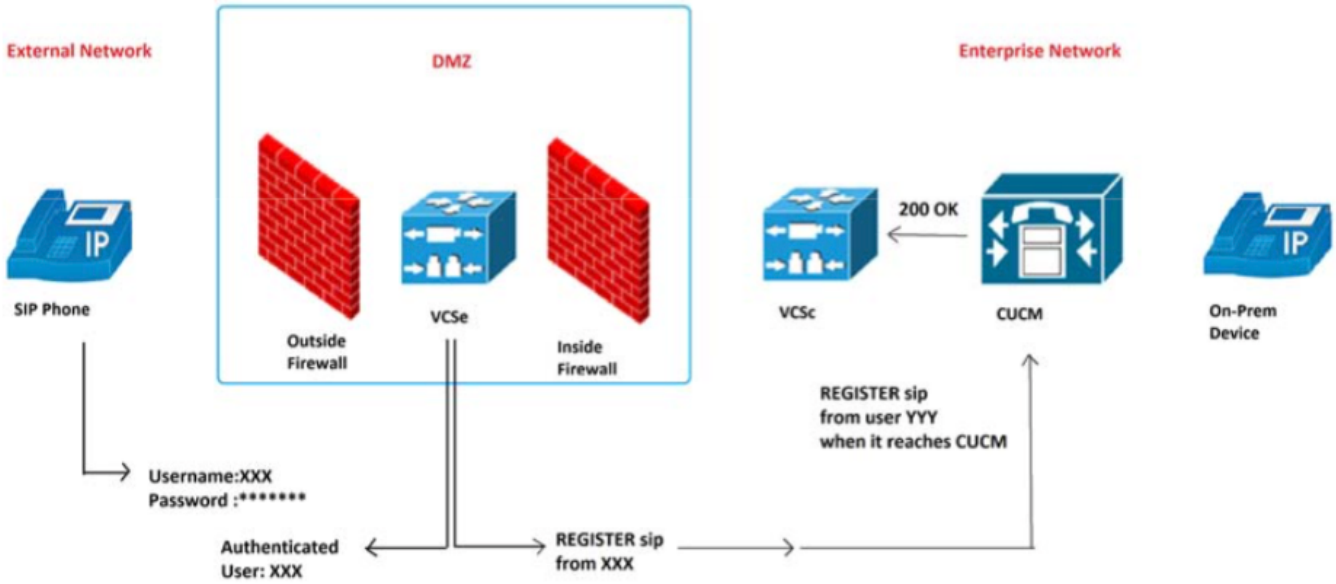
- 僅影響SIP電話
- 本地註冊不受影響

設定

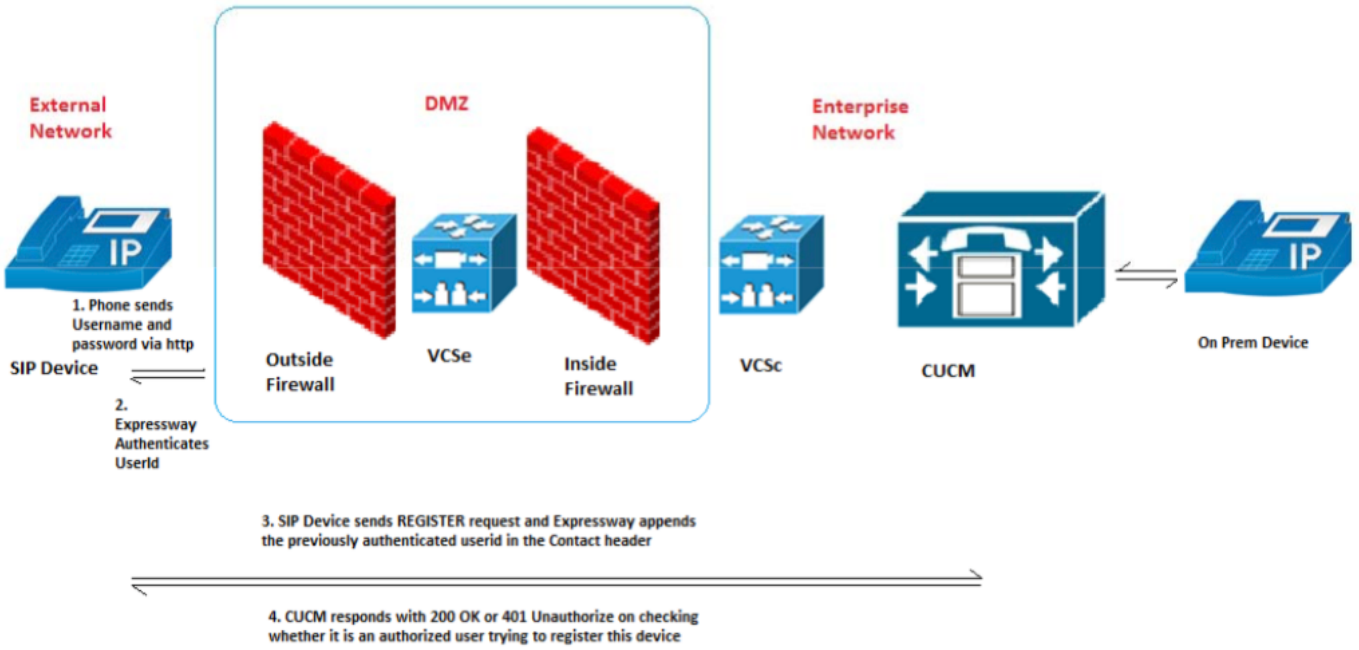
網路圖表

使用的元件（舊架構與新架構）

舊行為影象：



新行為影象：



組態

用於開啟/關閉此功能的新服務引數：System > Service Parameters > ***server > Cisco CallManager > SIP Registration Authorization Enabled***

值：

- True —（預設）
- 假

與正確裝置的正確UserID關聯可確定SIP註冊是否授權或拒絕。

註冊授權流程請求遵循以下方案：

案例1.如果REGISTER訊息中沒有UserID，則應授權，並傳送200 OK。

附註：這可確保與舊版Expressway的內部互操作性和向後相容性。

案例2.如果REGISTER消息中存在UserID，則……

- 如果UserID與「CUCM電話配置」頁中的owner-id欄位匹配，則授權並傳送200 OK
- 如果UserID與CUCM End User Configuration頁面中的裝置關聯UserID匹配，則授權並傳送200 OK
- 如果兩個所有者ID欄位都為空，且與終端使用者的裝置關聯不存在，則授權並傳送200確定
- 如果沒有匹配，則失敗，並傳送401未授權

場景3.如果REGISTER消息包含多個不同值的UserID，則返回FAIL並傳送401 Unauthorized。

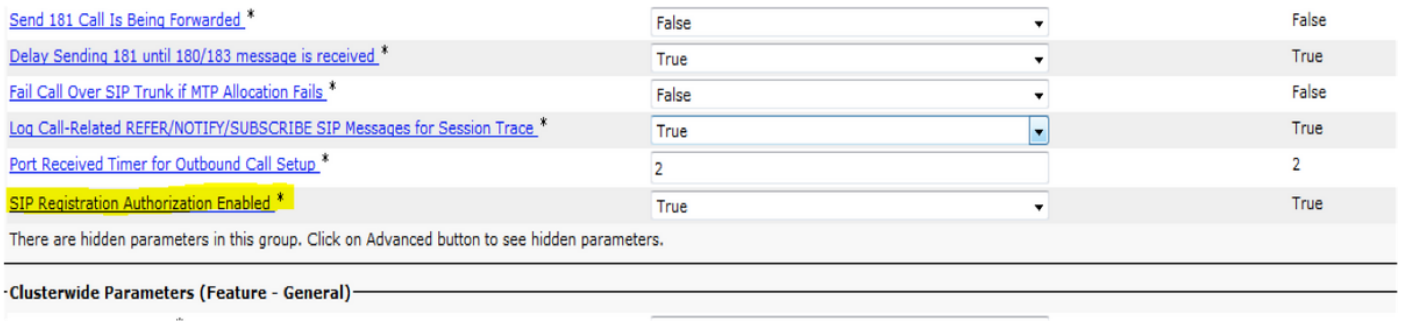
附註：只有Expressway填充這些UserID標頭

用例結果表

編號	測試案例	已啟用SIP註冊授權	預期結果
1	聯絡人標頭中的UserId引數不存在	正確	授權

			（200確定）
2	聯絡人標題中的UserId引數與電話配置頁面中的OwnerId匹配	正確	授權（200確定）
3	聯絡人標題中的userId引數與EndUser頁中裝置關聯的userId匹配。	正確	授權（200確定）
4	聯絡人頭中的UserId與「電話配置」頁中的ownerId匹配，與「終端使用者」頁中配置的userId不匹配	正確	授權（200確定）
5	聯絡人頭中的UserId與EndUser頁中的userId匹配，與Phone Config頁中的OwnerId不匹配	正確	授權（200確定）
6	「電話配置」頁中的OwnerId為空，裝置在「終端使用者」頁中沒有關聯使用者	正確	授權（200確定）
7	在Phone Config頁為OwnerId在EndUser頁為裝置配置的userId，但未找到匹配項	正確	401未授權
8	聯絡人頭中存在多個使用者ID。	正確	401未授權
9	在EndUser頁面中為裝置配置多個使用者ID	正確	授權(200 Ok)
10	取消轉義使用者ID	正確	授權(200 Ok)
11	刷新暫存器	正確	與初始註冊消息相同
12	聯絡人標頭中的UserId為空字串，沒有為裝置配置OwnerId和UserId	正確	授權(200 Ok)
13	聯絡人報頭中的UserId為空字串，為裝置配置的OwnerId/UserId	正確	401未授權
14	UserId存在於為裝置配置的OwnerId/UserId的聯絡人頭中，但找不到匹配項	假	200正常
15	聯絡人標頭中存在多個userId	假	200正常
16	為裝置配置的contact標頭中的userId為空字串ownerId /UserId	假	200正常

通過通訊管理器(CCM)服務引數啟用該功能。預設情況下，它會處於開啟狀態，無需進一步配置。



驗證

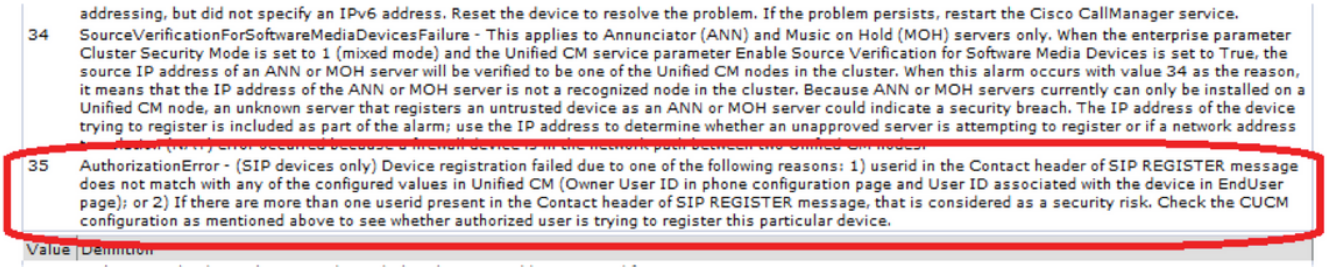
聯絡人標題

CUCM檢查REGISTER消息的聯絡人標題以由Expressway修改

```
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“
```

新警報(AuthorizationErrorwithWarningLevel)

現在，當SIP註冊授權失敗時，可以使用新的警報(AuthorizationErrorwithWarningLevel)



疑難排解

在CCM Traces調試輸出中查詢授權嘗試

成功的授權示例：

案例 1:

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

案例 2:

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

授權和警報失敗示例：

```
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=
```