Configurez les enregistrements SIP pour qu'ils s'authentifient et qu'ils autorisent par utilisateur (MRA) pour CUCM 11.5

Contenu

Introduction

Ce document décrit le comportement amélioré dans Cisco Unified Communications Manager (CUCM) qui fournit une couche supplémentaire d'authentification UserID dans les messages SIP (Session Initiation Protocol) REGISTER par rapport à la méthode actuelle d'authentification uniquement sur Expressway.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Administration et configuration de CUCM
- Protocole SIP
- Expressway Video Communication Server (VCS)

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Unified Communications Manager 11.5 et versions ultérieures
- Expressway Video Communication Server (VCS)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Par le passé, l’enregistrement des périphériques via l’Expressway VCS (Video Communication Server) fonctionne lorsque le périphérique envoie un nom d’utilisateur et un mot de passe via le protocole HTTP (Hypertext Transfer Protocol). Expressway authentifie ensuite le nom d’utilisateur et permet au périphérique de poursuivre l’enregistrement vers CUCM sans vérification supplémentaire.

Le nouveau comportement est que CUCM vérifie maintenant le message SIP REGISTER et s'assure que l'ID utilisateur est correctement associé au périphérique. Grâce à cette fonctionnalité, l'ID utilisateur doit autoriser avant de s'enregistrer dans CUCM ; fournit donc le niveau de protection suivant contre le périphérique à partir d'un réseau externe/inconnu. Cela garantit que le SIP REGISTER est autorisé, c'est-à-dire que seul un périphérique valide associé à l'utilisateur valide doit s'enregistrer. S'il n'existe aucune association UserID au périphérique, l'enregistrement rejette avec le code de réponse 401.

Historique

- CSCuu97283
- ID CVE CVE-2015-6410

Limites

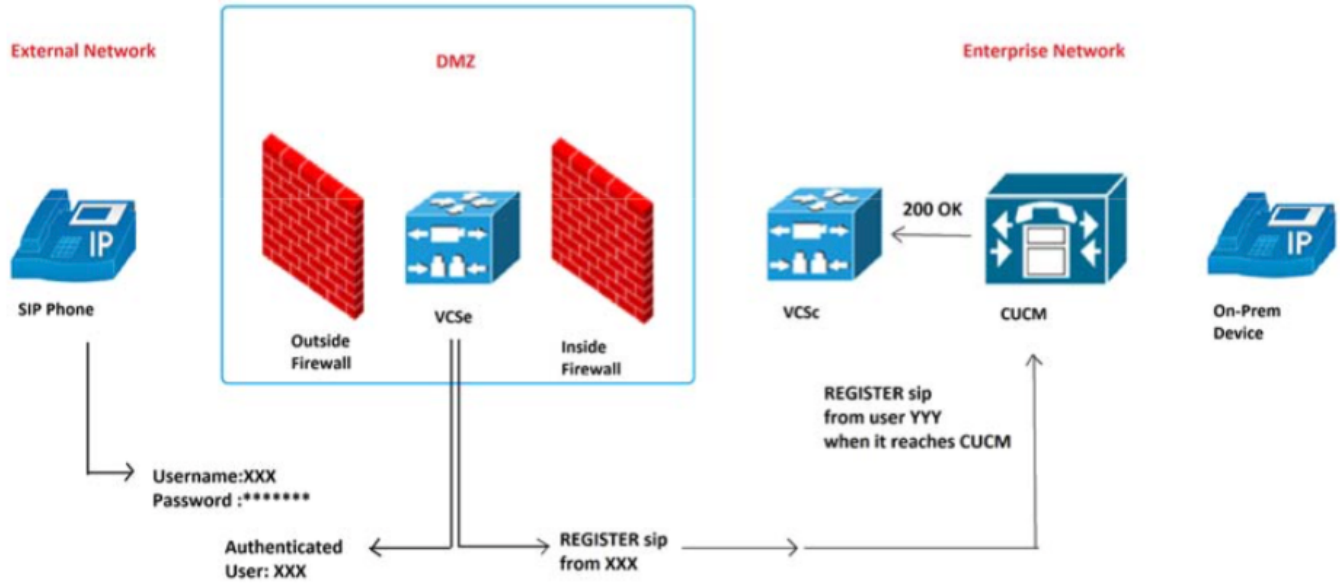
- Affecte uniquement les téléphones SIP
- Les inscriptions sur site ne sont pas affectées

Configuration

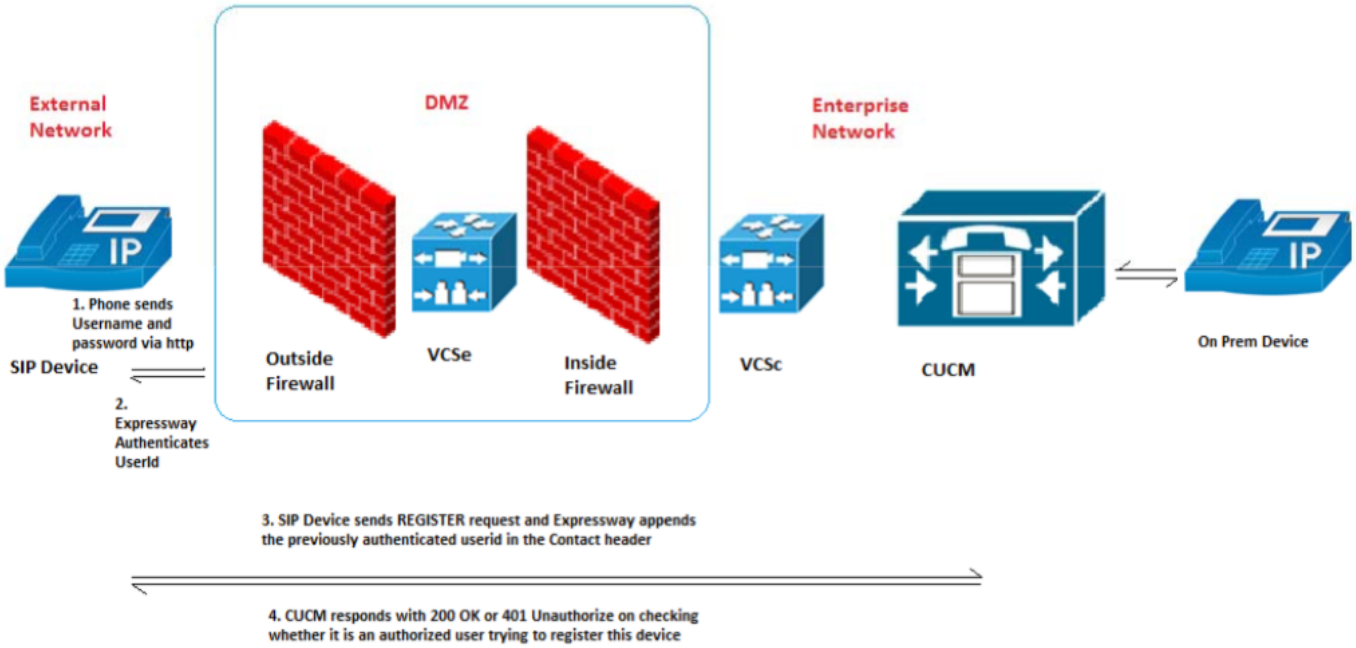
Diagramme du réseau

Composants utilisés (architecture ancienne ou nouvelle)

Ancienne image de comportement :



Nouvelle image de comportement :



Configurations

Nouveau paramètre de service pour activer/désactiver cette fonction : **System > Service Parameters > *server* > Cisco CallManager > SIP Registration Authorization Enabled**

Valeurs:

- True - (valeur par défaut)
- Faux

L'association UserID correcte au périphérique correct détermine si l'enregistrement SIP autorise ou rejette.

La demande d'autorisation d'enregistrement suit les scénarios suivants :

Scénario 1. Si UserID n'est pas présent dans le message REGISTER, il doit autoriser et 200 OK est envoyé.

Note: Cela garantit l'interopérabilité sur site et la rétrocompatibilité avec les anciennes versions d'Expressway.

Scénario 2. Si UserID est présent dans le message REGISTER, alors...

- IF UserID correspond au champ owner-id de la page Configuration du téléphone CUCM, PUIS Autoriser et envoyer 200 OK
- SI l'ID utilisateur correspond à l'association de l'ID utilisateur au périphérique dans la page Configuration de l'utilisateur final de CUCM, PUIS Autoriser et envoyer 200 OK
- Si le champ ID du propriétaire est vide et que l'association de périphérique à l'utilisateur final n'existe pas, ALORS Autoriser et envoyer 200 OK
- ELSE Si aucune correspondance, THEN FAIL et envoyer 401 Non autorisé

Scénario 3. Si le message REGISTER contient plus d'un UserID de valeurs différentes, THEN FAIL et send 401 Unallowed.

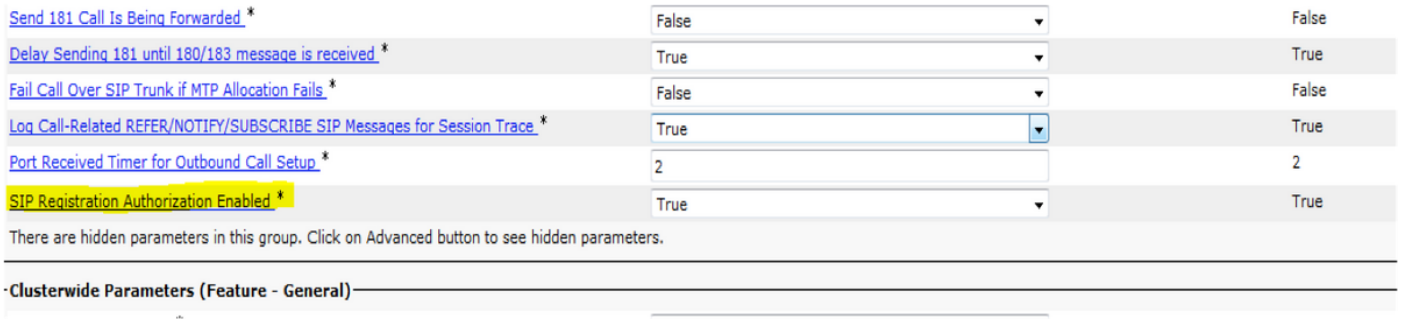
Note: Uniquement Expressway remplit ces en-têtes UserID

Tableau des résultats des cas d'utilisation

Nombre	Exemples de tests	Autorisation d'enregistrement SIP activée	Résultat attendu
1	Le paramètre UserId de l'en-tête du contact n'est pas présent	Vrai	Autoriser (200 OK)
2	Le paramètre UserId de l'en-tête du contact correspond à OwnerId dans la page de configuration du téléphone	Vrai	Autoriser (200 OK)
3	Le paramètre UserId de l'en-tête du contact correspond à l'ID utilisateur associé à un périphérique dans la page EndUser.	Vrai	Autoriser (200 OK)
4	L'ID utilisateur dans l'en-tête du contact correspond à l'ID propriétaire dans la page Configuration du téléphone, ne correspond pas à l'ID utilisateur configuré dans la page Utilisateur final.	Vrai	Autoriser (200 OK)
5	L'ID utilisateur dans l'en-tête du contact correspond à l'ID utilisateur dans la page Utilisateur final, ne correspond pas à l'ID propriétaire dans la page Configuration du téléphone	Vrai	Autoriser (200 OK)
6	OwnerId de la page de configuration du téléphone est vide et aucun utilisateur n'est associé au périphérique dans la page Utilisateur final.	Vrai	Autoriser (200 OK)
7	OwnerId dans la page Phone Config et userId configurés pour un périphérique dans la page EndUser, mais aucune correspondance trouvée	Vrai	401 Non autorisé

8	Plusieurs ID utilisateur présents dans l'en-tête du contact.	Vrai	401 Non autorisé
9	ID utilisateur multiple configuré pour un périphérique dans la page Utilisateur final	Vrai	Autoriser (200 Ok)
10	Suppression de l'ID utilisateur	Vrai	Autoriser (200 Ok)
11	Actualiser le registre	Vrai	Identique au message ENREGISTREMENT initial
12	UserId dans l'en-tête du contact est une chaîne vide, OwnerId et UserId non configurés pour le périphérique	Vrai	Autoriser (200 Ok)
13	L'ID utilisateur dans l'en-tête du contact est une chaîne vide, OwnerId/UserId configuré pour le périphérique	Vrai	401 Non autorisé
14	UserId est présent dans l'en-tête du contact, OwnerId/UserId configuré pour le périphérique, mais aucune correspondance trouvée	Faux	200 OK
15	Plusieurs ID utilisateur présents dans l'en-tête du contact	Faux	200 OK
16	UserId dans l'en-tête du contact est une chaîne vide, ownerId /UserId configuré pour le périphérique	Faux	200 OK

Activez la fonctionnalité via le paramètre de service de Communications Manager (CCM). Il est activé par défaut et aucune autre configuration n'est requise.



Vérification

En-tête du contact

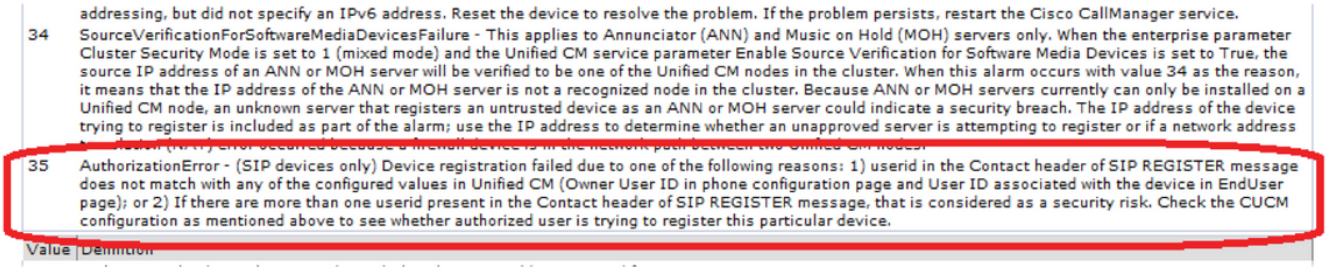
CUCM vérifie l'en-tête Contact du message REGISTER pour modification par Expressway

```
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"
```

Nouvelle alarme (AuthorizationErrorWarningLevel)

Une nouvelle alarme (AuthorizationErrorwithWarningLevel) est maintenant disponible en cas

d'échec d'autorisation d'enregistrement SIP



Value	Definition
34	addressing, but did not specify an IPv6 address. Reset the device to resolve the problem. If the problem persists, restart the Cisco CallManager service. SourceVerificationForSoftwareMediaDevicesFailure - This applies to Annunciator (ANN) and Music on Hold (MOH) servers only. When the enterprise parameter Cluster Security Mode is set to 1 (mixed mode) and the Unified CM service parameter Enable Source Verification for Software Media Devices is set to True, the source IP address of an ANN or MOH server will be verified to be one of the Unified CM nodes in the cluster. When this alarm occurs with value 34 as the reason, it means that the IP address of the ANN or MOH server is not a recognized node in the cluster. Because ANN or MOH servers currently can only be installed on a Unified CM node, an unknown server that registers an untrusted device as an ANN or MOH server could indicate a security breach. The IP address of the device trying to register is included as part of the alarm; use the IP address to determine whether an unapproved server is attempting to register or if a network address
35	AuthorizationError - (SIP devices only) Device registration failed due to one of the following reasons: 1) userid in the Contact header of SIP REGISTER message does not match with any of the configured values in Unified CM (Owner User ID in phone configuration page and User ID associated with the device in EndUser page); or 2) If there are more than one userid present in the Contact header of SIP REGISTER message, that is considered as a security risk. Check the CUCM configuration as mentioned above to see whether authorized user is trying to register this particular device.

Dépannage

Rechercher les tentatives d'autorisation dans la sortie de débogage de CCM Traces

Exemples d'autorisation réussis :

Scénario 1 :

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

Scénario 2 :

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

Exemple d'autorisation et d'alarme ayant échoué :

```
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=
```