Configuración de registros SIP para autenticar y autorizar por usuario (MRA) para CUCM 11.5

Contenido

Introducción

Este documento describe el comportamiento mejorado en Cisco Unified Communications Manager (CUCM) que proporciona una capa adicional de autenticación de ID de usuario en los mensajes REGISTER del protocolo de inicio de sesión (SIP) frente al método actual de autenticación sólo en Expressway.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administración y configuración de CUCM
- Protocolo SIP
- Expressway de Video Communication Server (VCS)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Unified Communications Manager 11.5 y posterior
- Expressway de 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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En el pasado, el registro de dispositivos a través de Video Communication Server (VCS) Expressway funciona cuando el dispositivo envía el nombre de usuario y la contraseña a través del protocolo de transferencia de hipertexto (HTTP). Expressway luego autentica el nombre de usuario y permite al dispositivo continuar con el registro hacia CUCM sin más verificación.

El nuevo comportamiento es que ahora CUCM verifica el mensaje SIP REGISTER y asegura que el ID de usuario tenga una asociación adecuada con el dispositivo. A través de esta función, el ID de usuario debe autorizar antes de registrarse en CUCM; por lo tanto, proporciona el siguiente nivel de protección contra el dispositivo desde una red externa/desconocida. Esto garantiza que el REGISTRO SIP esté autorizado, es decir, solo un dispositivo válido asociado al usuario válido debe registrarse. Si no hay ninguna asociación UserID al dispositivo, el registro rechaza con el código de respuesta 401.

Historial de antecedentes

- CSCuu97283
- CVE ID CVE-2015-6410

Limitaciones

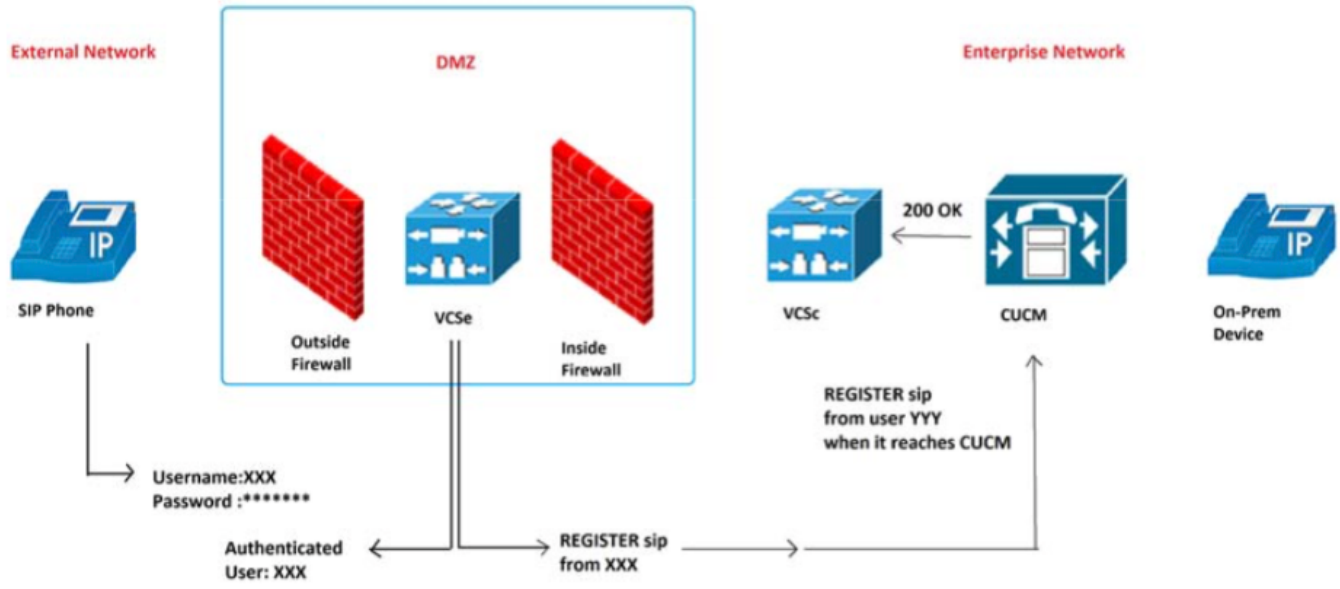
- Solo afecta a los teléfonos SIP
- Los registros in situ no se ven afectados

Configurar

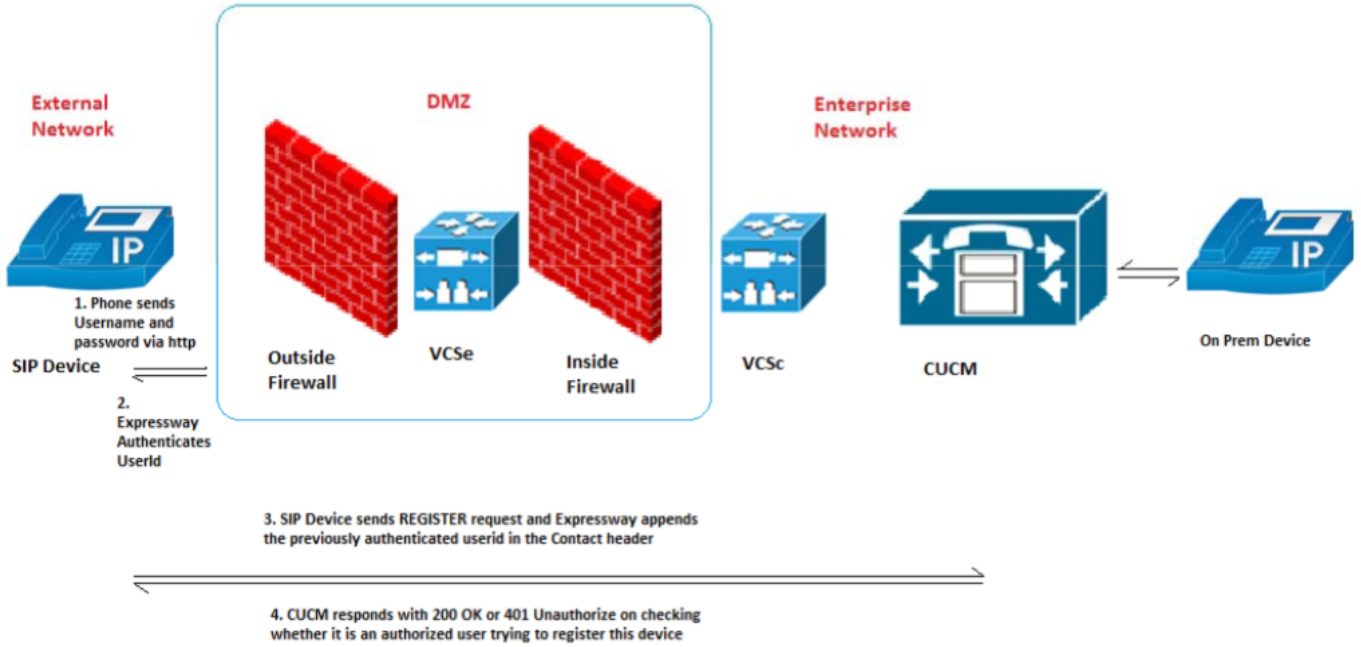
Diagrama de la red

Componentes utilizados (arquitectura antigua frente a nueva)

Imagen de comportamiento antiguo:



Nueva imagen de comportamiento:



Configuraciones

Nuevo parámetro de servicio para activar/desactivar esta función: **System > Service Parameters > *server* > Cisco CallManager > SIP Registration Authorization Enabled**

Valores:

- True (valor predeterminado)
- Falso

La asociación UserID correcta con el dispositivo correcto determina si el registro SIP autoriza o rechaza.

La solicitud del proceso de autorización de registro sigue estos escenarios:

Escenario 1. Si UserID no está presente en el mensaje REGISTER (Registro), debería autorizar y enviar 200 OK (Aceptar).

Nota: Esto garantiza la interoperabilidad in situ y la compatibilidad con versiones anteriores de Expressway.

Situación hipotética 2. Si UserID está presente en el mensaje REGISTER, entonces...

- SI UserID coincide con el campo owner-id en la página de configuración del teléfono de CUCM, LUEGO autorice y envíe 200 OK
- SI UserID coincide con la asociación UserID con el dispositivo en la página CUCM End User Configuration, LUEGO autorice y envíe 200 OK
- SI ambos campos owner-id están en blanco y la asociación del dispositivo al usuario final no existe, ENTONCES autorice y envíe 200 OK
- ELSE SI no hay coincidencia, LUEGO FALLA y envía 401 No autorizado

Situación hipotética 3. Si el mensaje REGISTER contiene más de un ID de usuario de valores

diferentes, LUEGO FALLE y envíe 401 Unauthorized.

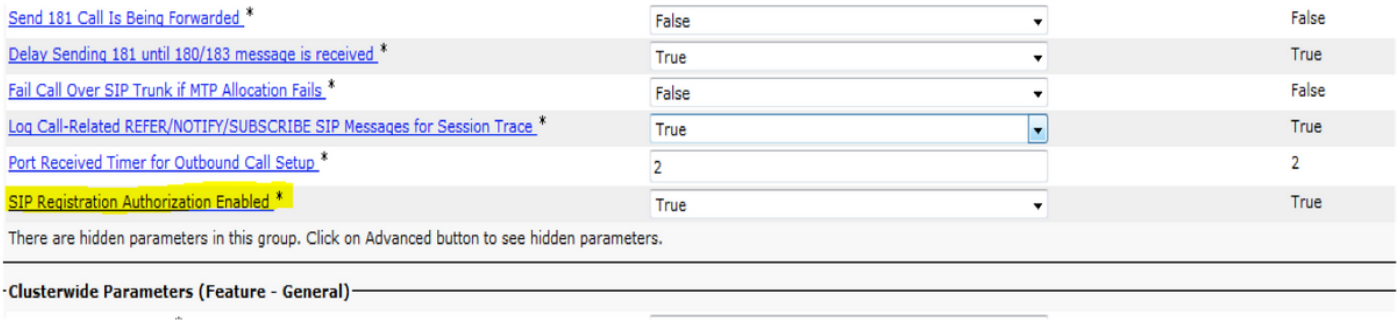
Nota: Solo Expressway rellena estos encabezados UserID

Tabla de resultados de casos prácticos

Número	Casos de prueba	Autorización de registro SIP habilitada	Resultado esperado
1	El parámetro UserId del encabezado del contacto no está presente	Verdadero	Autorizar (200 OK)
2	El parámetro UserId del encabezado del contacto coincide con OwnerId en la página de configuración del teléfono	Verdadero	Autorizar (200 OK)
3	El parámetro UserId del encabezado del contacto coincide con userId asociado a un dispositivo en la página EndUser.	Verdadero	Autorizar (200 OK)
4	El ID de usuario en el encabezado de contacto coincide con el ID de propietario en la página Configuración del teléfono, no coincide con el ID de usuario configurado en la página Usuario final	Verdadero	Autorizar (200 OK)
5	El ID de usuario en el encabezado de contacto coincide con el ID de usuario en la página Usuario final, no coincide con el IdPropietario en la página Configuración del teléfono	Verdadero	Autorizar (200 OK)
6	OwnerId en la página Phone Config está en blanco y el dispositivo no tiene ningún usuario asociado en la página EndUser	Verdadero	Autorizar (200 OK)
7	OwnerId en la página de configuración del teléfono y userId configurados para un dispositivo en la página Usuario final, pero no se ha encontrado ninguna coincidencia	Verdadero	401 No autorizado
8	Hay más de un ID de usuario presente en el encabezado del contacto.	Verdadero	401 No autorizado
9	ID de usuario múltiple configurado para un dispositivo en la página Usuario final	Verdadero	Autorizar (200 Ok)
10	ID de usuario ineludible	Verdadero	Autorizar (200 Ok)
11	Actualizar registro	Verdadero	Igual que el mensaje de REGISTRO inicial
12	El ID de usuario en el encabezado de contacto es una cadena vacía, el ID de propietario y el ID de usuario no están configurados para el dispositivo	Verdadero	Autorizar (200 Ok)
13	El ID de usuario en el encabezado del contacto es una cadena vacía, OwnerId/UserId configurado para el dispositivo	Verdadero	401 No autorizado
14	UserId está presente en el encabezado del contacto, OwnerId/UserId configurado para el dispositivo, pero no se ha encontrado ninguna coincidencia	Falso	200 OK

15	Hay más de un ID de usuario presente en el encabezado del contacto	Falso	200 OK
16	UserId en el encabezado del contacto es una cadena vacía, ownerId /UserId configurada para el dispositivo	Falso	200 OK

Active la función mediante el parámetro de servicio de Communications Manager (CCM). Está activado de forma predeterminada y no se requiere ninguna configuración adicional.



Verificación

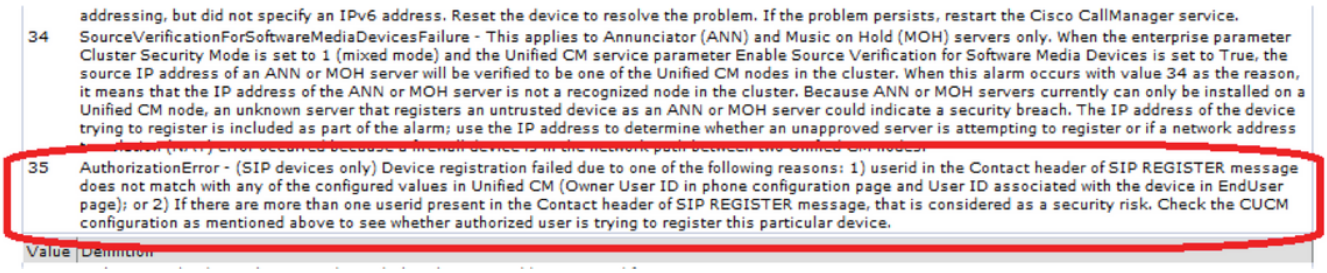
Encabezado de contacto

CUCM comprueba el encabezado de contacto del mensaje REGISTER para que Expressway lo modifique

```
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"
```

Nueva alarma (AuthorizationErrorwithWarningLevel)

Ahora hay disponible una nueva alarma (AuthorizationErrorwithWarningLevel) cuando se produce una falla en la autorización de registro SIP



Troubleshoot

Buscar intentos de autorización en la salida de depuración de seguimientos de CCM

Ejemplos de autorización correctos:

Escenario 1:

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

Escenario 2:

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

Ejemplo de autorización y alarma fallidas:

```
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=
```