

Настройте регистрации SIP, чтобы аутентифицировать и авторизовать на основе для каждого пользователя (MRA) для CUCM 11.5

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

Введение

Этот документ описывает улучшенное поведение в Cisco Unified Communications Manager (CUCM), который предоставляет дополнительный уровень аутентификации UserID в сообщениях РЕГИСТРА Протокола SIP по сравнению с существующим способом аутентификации только в Скоростной автомагистрали.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Администрирование CUCM и конфигурация
- SIP Portocol
- Скоростная автомагистраль сервера Video Communication Server (VCS)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Unified Communications Manager 11.5 и позже
- Скоростная автомагистраль сервера Video Communication Server (VCS)

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если ваша сеть является оперативной, Гарантируйте понимание потенциального воздействия любой команды.

Общие сведения

Когда устройство передает имя пользователя и пароль через Протокол HTTP, в прошлом регистрация устройства через Скоростную автомагистраль сервера Video Communication Server (VCS) работает. Скоростная автомагистраль тогда аутентифицирует имя пользователя и позволяет устройству продолжать регистрацию к CUCM без дальнейшей проверки.

Новое поведение состоит в том, что теперь CUCM проверяет СООБЩЕНИЕ REGISTER и гарантирует, что UserID имеет надлежащую ассоциацию к устройству. Через эту функцию UserID должен авторизовать, прежде чем это зарегистрируется в CUCM; поэтому, предоставляет следующий уровень защиты против устройства от внешнего / неизвестной сети. Это гарантирует, что РЕГИСТР SIP авторизуется, т.е. только допустимое устройство, привязанное к допустимому пользователю, должно зарегистрироваться. Если нет никакой ассоциации UserID к устройству тогда отказов в регистрации с 401 кодом ответа.

Фоновая история

- [CSCuu97283](#)
- [ID CVE-2015-6410 CVE](#)

Ограничения

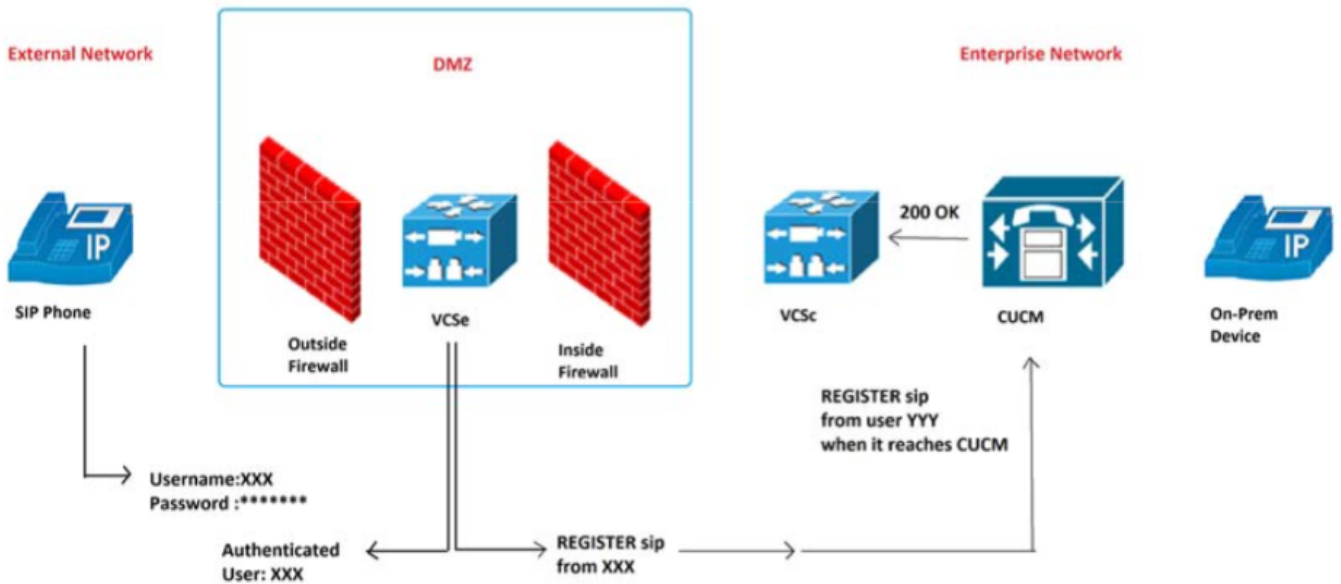
- Только SIP-телефоны влияния
- Собственная регистрация является незатронутой

Настройка

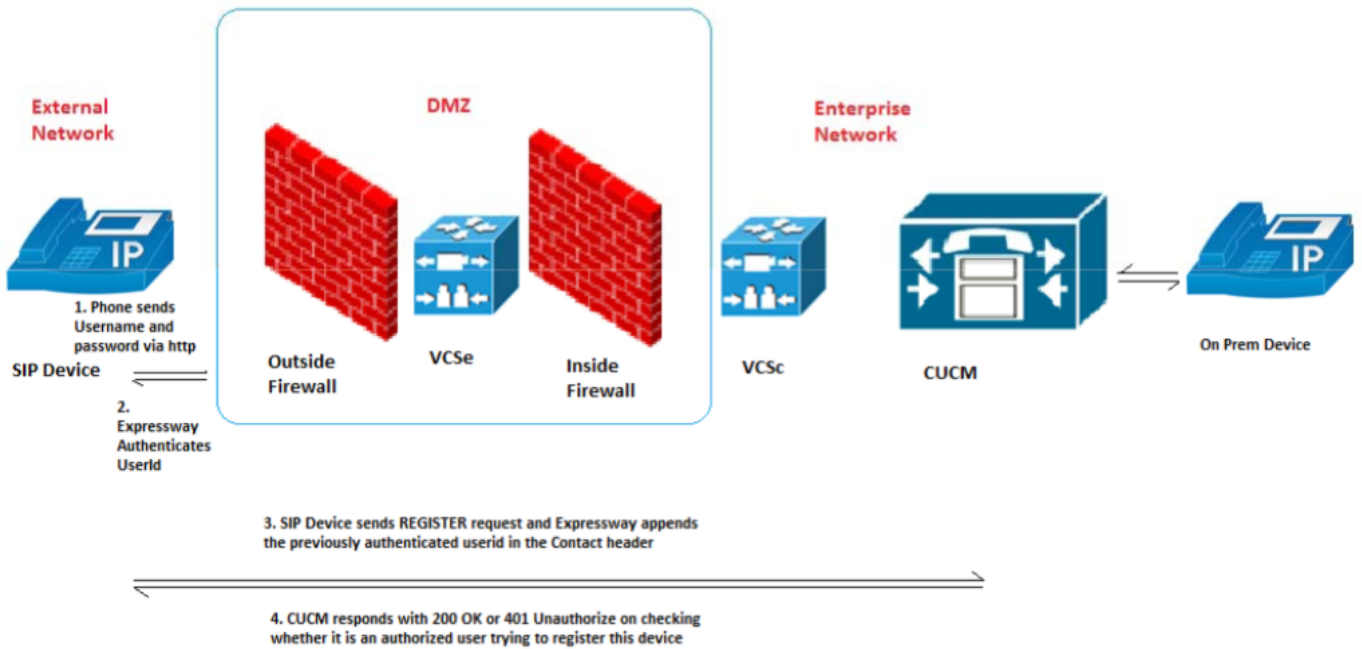
Схема сети

Используемые компоненты (Старый по сравнению с новой архитектурой)

Старый образ поведения:



Новый образ поведения:



Конфигурации

Новый параметр сервиса для переключения этой функции вкл\выкл: Система> Параметры сервиса> *server*> Cisco CallManager> Авторизация регистрации SIP Включена

Значения:

- Истинный - (по умолчанию)
- FALSE

Корректная ассоциация UserID к правильному устройству определяет, авторизует ли регистрация SIP или отклоняет.

Регистрационный запрос процесса авторизации придерживается этих сценариев:

Сценарий 1. Если UserID не присутствует в сообщении РЕГИСТРА, это должно авторизовать, и 200 ОК передаются.

Примечание: Это убеждается на - ргет совместимость и обратная совместимость с более старыми версиями Скоростной автомагистрали.

Сценарий 2. Если UserID присутствует в сообщении РЕГИСТРА тогда...

- Если поле идентификатора владельца соответствий UserID в Странице конфигурации телефона CUCM, ЗАТЕМ Авторизуйте и передайте 200 ОК
- Если ассоциация UserID соответствий UserID с устройством в Странице конфигурации Конечного пользователя CUCM, ЗАТЕМ Авторизуйте и передайте 200 ОК
- Если и поле идентификатора владельца является пробелом и сопоставлением устройств, конечному пользователю не существует, ЗАТЕМ Авторизует и передает 200 ОК
- ELSE, если никакое соответствие, ЗАТЕМ ОТКАЖИТЕ и передайте 401 Неавторизованный

Ситуация 3. Если сообщение РЕГИСТРА содержит несколько UserID других значений, ЗАТЕМ ОТКАЖИТЕ и передайте 401 Неавторизованный.

Примечание: Только Скоростная автомагистраль заполняет эти заголовки UserID

Таблица результатов вариантов использования

Номер	Контрольные примеры	Авторизация регистрации SIP включена	Ожидаемый результат
1	Параметр UserID в заголовке контакта не присутствует	TRUE	Авторизовать (200 ХОРОШО)
2	Параметр UserID в заголовке контакта совпадает с OwnerId на странице конфигурации телефона	TRUE	Авторизовать (200 ХОРОШО)
3	Параметр UserID в заголовке контакта совпадает с идентификатором пользователя, привязанным к устройству на странице EndUser.	TRUE	Авторизовать (200 ХОРОШО)
4	UserId в соответствиях заголовка контакта с ownerId на странице Phone Config, не совпадает с идентификатором пользователя, настроенным на странице EndUser	TRUE	Авторизовать (200 ХОРОШО)
5	UserId в соответствиях заголовка контакта с идентификатором пользователя на странице EndUser, не совпадает с OwnerId на странице Phone Config	TRUE	Авторизовать (200 ХОРОШО)
6	OwnerId на странице Phone Config является пробелом, и устройство не имеет никакого пользователя, привязанного на странице	TRUE	Авторизовать (200

7	EndUser OwnerId на странице Phone Config и идентификаторе пользователя, настроенном для устройства на странице EndUser, но никакого соответствия, найден	TRUE	ХОРОШО) 401 Неавторизованный
8	Несколько идентификаторов пользователя представляют в заголовке контакта.	TRUE	401 Неавторизованный
9	Множественный идентификатор пользователя настроен для устройства на странице EndUser	TRUE	Авторизуйте (200 Ok)
10	Невыход из идентификатора пользователя	TRUE	Авторизуйте (200 Ok) То же как Начальная
11	Регистр обновления	TRUE	буква РЕГИСТРИРУЕ Т сообщение
12	UserId в заголовке контакта является пустой строкой, OwnerId и UserId, не настроенным для устройства	TRUE	Авторизуйте (200 Ok)
13	UserId в заголовке контакта является пустой строкой, OwnerId/UserId, настроенный для устройства	TRUE	401 Неавторизованный
14	UserId присутствует в заголовке контакта, OwnerId/UserId, настроенный для устройства, но никакого найденного соответствия	FALSE	200 ХОРОШО
15	Несколько идентификаторов пользователя представляют в заголовке контакта	FALSE	200 ХОРОШО
16	UserId в заголовке контакта является пустой строкой, идентификатор пользователя ownerId/, настроенный для устройства	FALSE	200 ХОРОШО

Активируйте опцию через Диспетчера связи (CCM) Параметр сервиса. Это идет по умолчанию, и никакая дальнейшая конфигурация не требуется.

Send 181 Call Is Being Forwarded *	False	False
Delay Sending 181 until 180/183 message is received *	True	True
Fail Call Over SIP Trunk if MTP Allocation Fails *	False	False
Log Call-Related REFER/NOTIFY/SUBSCRIBE SIP Messages for Session Trace *	True	True
Port Received Timer for Outbound Call Setup *	2	2
SIP Registration Authorization Enabled *	True	True

There are hidden parameters in this group. Click on Advanced button to see hidden parameters.

Clusterwide Parameters (Feature - General)

Проверка

Свяжитесь с заголовком

CUCM проверяет заголовок Контакта сообщения РЕГИСТРА для модификации Скоростной автомагистралью

```
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"
```

Новый сигнал тревоги (AuthorizationErrorwithWarningLevel)

Когда существует Сбой авторизации регистрации SIP, новый Сигнал тревоги (AuthorizationErrorwithWarningLevel) теперь доступен

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 translation (NAT) error occurred because a firewall device is in the network path between two Unified CM nodes.
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.

Устранение неполадок

Ищите попытки авторизации в выходных данных отладки Трассировок CCM

Примеры Успешной авторизации:

Сценарий 1:

```
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"
```

Сценарий 2:

```
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"
```

Сбой проверки подлинности и Сигнальный пример:

```
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"
```