Безопасная магистраль SIP между CUCM и примером конфигурации VCS

Содержание

Введение

Этот документ описывает, как установить безопасное соединение Протокола SIP между Cisco Unified Communications Manager (CUCM) и сервером Video Communication Server (VCS) Cisco TelePresence.

CUCM и VCS близко интегрированы. Поскольку оконечные точки видео могут быть зарегистрированы или на CUCM или на VCS, магистрали SIP должны существовать между устройствами.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communications Manager
- Сервер передачи видеоданных Cisco TelePresence
- Сертификаты

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования. Данный пример использует версию программного обеспечения X7.2.2 VCS Cisco и версию 9 CUCM. x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Гарантируйте, что сертификаты допустимы, добавьте сертификаты к CUCM и серверам VCS так, чтобы они доверяли сертификатам друг друга, затем установили магистраль SIP.

Схема сети

Получите сертификат VCS

По умолчанию все системы VCS идут с временным сертификатом. На странице администратора перейдите к**> Certificate management Обслуживания> Серверный сертификат**. Нажмите **сертификат Show server**, и новое окно открывается необработанными данными сертификата:

Это - пример необработанных данных сертификата:

```
-----BEGIN CERTIFICATE-----
MIIDHzCCAoigAwIBAgIBATANBgkqhkiG9w0BAQUFADCBmjFDMEEGA1UECgw6VGVt
cG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1
Njk5NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYw
LTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wHhcN
MTMwOTMwMDcxNzIwWhcNMTQwOTMwMDcxNzIwWjCBmjFDMEEGA1UECgw6VGVtcG9y
YXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5YTAtMTFlMy1hNTE4LTAwNTA1Njk5
NWI0YjFDMEEGA1UECww6VGVtcG9yYXJ5IENlcnRpZmljYXRlIDU4Nzc0NWYwLTI5
YTAtMTFlMy1hNTE4LTAwNTA1Njk5NWI0YjEOMAwGA1UEAwwFY2lzY28wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAKWvob+Y1zrKoAB5BvPsGR7aVfmTYPipL0I/
L21fyyjoO5qv9lzDCgy7PFZPxkD1d/DNLIgp1jjUqdfFV+64r8OkESwBO+4DFlut
tWZLQ1uKzzdsmvZ/b41mEtosElHNxH7rDYQsqdRA4ngNDJVlOgVFCEV4c7ZvAV4S
E8m9YNY9AgMBAAGjczBxMAkGA1UdEwQCMAAwJAYJYIZIAYb4QgENBBcWFVRlbXBv
cmFyeSBDZXJ0aWZpY2F0ZTAdBgNVHQ4EFgQU+knGYkeeiWqAjORhzQqRCHba+nEw
HwYDVR0jBBgwFoAUpHCEOXsBH1AzZN153S/Lv6cxNDIwDQYJKoZIhvcNAQEFBQAD
gYEAZklIMSfi49p1jIYqYdOAIjOiashYVfqGUUMFr4V1hokM90ByGGTbx8jx6Y/S
p1SyT4ilU5uiY0DD18EkLzt8y3jFNPmHYAw/f2fB9J3mDAqbiQdmbLAeD2RRUsy7
1Zc3zTl6WL6hsj+90GAsI/TGthQ2n7yUWPl6CevopbJe1iA=
-----END CERTIFICATE-----
```

Можно декодировать сертификат и видеть данные сертификата с помощью OpenSSL на локальном компьютере или использовании онлайнового декодера сертификата, такого как Покупатель SSL :

Генерируйте и загрузите подписанный сертификат VCS

Поскольку каждый сервер VCS имеет сертификат с тем же Общим именем, необходимо поместить новые сертификаты на сервер. Можно принять решение использовать подписанные сертификаты или сертификаты, подписанные Центром сертификации (CA). Посмотрите Создание Сертификата Cisco TelePresence и Использование С Руководством по развертыванию VCS Cisco для подробных данных этой процедуры.

Эта процедура описывает, как использовать сам VCS для генерации подписанного сертификата, затем загрузите тот сертификат:

1. Войдите как root к VCS, запустите OpenSSL и генерируйте секретный ключ:

```
~ # openssl
OpenSSL> genrsa -out privatekey.pem 1024
Generating RSA private key, 1024 bit long modulus
.................................++++++
..............++++++
e is 65537 (0x10001)
```

2. Используйте этот секретный ключ для генерации запроса подписи сертификата (CSR):

```
OpenSSL> req -new -key privatekey.pem -out certcsr.pem
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BE
State or Province Name (full name) [Some-State]:Vlaams-Brabant
Locality Name (eg, city) []:Diegem
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:radius.anatomy.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
OpenSSL> exit
```

3. Генерируйте подписанный сертификат:

```
~ # openssl x509 -req -days 360 -in certcsr.pem -signkey privatekey.pem -out vcscert.pem
Signature ok
subject=/C=BE/ST=Vlaams-Brabant/L=Diegem/O=Cisco/OU=TAC/CN=radius.anatomy.com
Getting Private key
~ #
```

4. Подтвердите, что сертификаты теперь доступны:

```
~ # ls -ltr *.pem
-rw-r--r-- 1 root root 891 Nov 1 09:23 privatekey.pem
-rw-r--r-- 1 root root 664 Nov 1 09:26 certcsr.pem
-rw-r--r-- 1 root root 879 Nov 1 09:40 vcscert.pem
```

5. Загрузите сертификаты WinSCP и загрузите их на веб-странице, таким образом, VCS может использовать сертификаты; вам нужно и секретный ключ и генерируемый

сертификат:

6. Повторите эту процедуру для всех серверов VCS.

Добавьте подписанный сертификат с сервера CUCM на сервер VCS

Добавьте сертификаты от серверов CUCM так, чтобы VCS доверял им. В данном примере вы используете стандартные подписанные сертификаты от CUCM; CUCM генерирует подписанные сертификаты во время установки, таким образом, вы не должны создавать тех, как вы сделали на VCS.

Эта процедура описывает, как добавить подписанный сертификат с сервера CUCM на сервер VCS:

1. Загрузите сертификат CallManager.pem от CUCM. Войдите в Страницу администрирования операционной системы, перейдите к **Безопасности> Управление сертификатами**, затем выберите и загрузите самоподписанный сертификат CallManager.pem:

2. Добавьте этот сертификат как доверяемый сертификат CA на VCS.On VCS, перейдите к**> Certificate management Обслуживания> сертификат CA, которому Доверяют** и выберите **Show CA certificate**:

   Новое окно открывается всеми сертификатами, которым в настоящее время доверяют.

3. Скопируйте весь из в настоящее время надежные сертификаты к текстовому файлу. Откройте файл CallManager.pem в текстовом редакторе, скопируйте его содержание и добавьте что содержание к нижней части того же текстового файла после в настоящее время надежные сертификаты:

```
CallManagerPub
======================
-----BEGIN CERTIFICATE-----
MIICmDCCAgGgAwIBAgIQZo7WOmjKYy9JP228PpPvgTANBgkqhkiG9w0BAQUFADBe
MQswCQYDVQQGEwJCRTEOMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA1RBQzERMA8G
A1UEAxMITUZDbDFQdWIxDzANBgNVBAgTBkRpZWdlbTENMAsGA1UEBxMEUGVnMzAe
Fw0xMjA4MDExMDI4MzVaFw0xNzA3MzExMDI4MzRaMF4xCzAJBgNVBAYTAkJFMQ4w
DAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMREwDwYDVQQDEwhNRkNsMVB1YjEP
MA0GA1UECBMGRGllZ2VtMQ0wCwYDVQQHEwRQZWczMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQDmCOYMvRqZhAl+nFdHk0Y2PlNdACglvnRFwAq/rNgGrPCiwTgc
0cxqsGtGQLSN1UyIPDAE5NufROQPJ7whR95KGmYbGdwHfKeuig+MT2CGltfPe6ly
c/ZEDqHYvGlzJT5srWUfM9GdkTZfHI1iV6k/jvPtGigXDSCIqEjn1+3IEQIDAQAB
o1cwVTALBgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMC
BggrBgEFBQcDBTAdBgNVHQ4EFgQUK4jYX6O6BAnLCalbKEn6YV7BpkQwDQYJKoZI
hvcNAQEFBQADgYEAkEGDdRdMOtX4ClhEatQE3ptT6L6RRAyP8oDd3dIGEOYWhA2H
Aqrw77loieva297AwgcKbPxnd5lZ/aBJxvmF8TIiOSkjy+dJW0asZWfei9STxVGn
NSr1CyAt8UJh0DSUjGHtnv7yWse5BB9mBDR/rmWxIRrlIRzAJDeygLIq+wc=
```

-----END CERTIFICATE-----Если у вас есть несколька адресов серверов в кластере CUCM, добавьте всех их здесь.

4. Сохраните файл как CATrust.pem и нажмите **Upload CA certificate** для загрузки файла назад к VCS:

   VCS будет теперь доверять сертификатам, предлагаемым CUCM.

5. Повторите эту процедуру для всех серверов VCS.

Сертификат загрузки с сервера VCS на сервер CUCM

CUCM должен доверять сертификатам, предлагаемым VCS.

Эта процедура описывает, как загрузить сертификат VCS, который вы генерировали на CUCM как Трастовый CallManager сертификат:

1. На Странице администрирования операционной системы перейдите к **Безопасности> Управление сертификатами**, введите имя сертификата, перейдите к его местоположению и нажмите **Upload File**:

2. Загрузите сертификат от всех серверов VCS. Сделайте это на каждом сервере CUCM, который свяжется с VCS; это, как правило, - все узлы, которые выполняют Сервис CallManager.

Соединение SIP

Как только сертификаты проверены, и обе системы доверяют друг другу, настраивают Соседнюю Зону на VCS и магистраль SIP на CUCM. Посмотрите Cisco Unified Communications Manager Cisco TelePresence с VCS Cisco (магистраль SIP) Руководство по развертыванию для подробных данных этой процедуры.

Проверка

Подтвердите, что соединение SIP активно в Соседней Зоне на VCS:

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco Unified Communications Manager Cisco TelePresence с VCS Cisco (магистраль SIP) руководство по развертыванию
- Руководство администратора сервера передачи видеоданных Cisco TelePresence
- Создание сертификата Cisco TelePresence и использование с руководством по развертыванию VCS Cisco
- Руководство по администрированию операционной системы унифицированной связи Cisco
- Руководство по администрированию Cisco Unified Communications Manager
- Cisco Systems – техническая поддержка и документация