Настройте Транк TLS SIP на Диспетчере связи с подписанным сертификатом CA.

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Общие сведения
Настройка
Шаг 1. Используйте общественность CA или установленный CA на Windows Server 2003
Шаг 2. Проверьте имя хоста и параметры настройки
Шаг 3. Генерируйте и загрузите запрос подписи сертификата (CSR)
Шаг 4. . Подпишите CSR с центром сертификации Microsoft Windows 2003 года
Шаг 5. . Получите корневой сертификат от CA
Шаг 6. Загрузка CA корневой сертификат как доверие CallManager
Шаг 7. Загрузка CA подписывает Сертификат CSR CallManager как сертификат CallManager.
Шаг 8. Создайте профили безопасности магистрального SIP-канала
Шаг 9. Создайте магистрали SIP
Шаг 10. Создайте шаблоны маршрута
Проверка
Устранение неполадок
Соберите захват пакета на CUCM
Соберите трассировки CUCM
Соответствующие дискуссии сообщества технической поддержки Cisco

Введение

Этот документ описывает пошаговый процесс для настройки Транка Transport Layer Security (TLS) Протокола SIP на Диспетчере связи с а Подписанный сертификат Центра сертификации (CA).

После следующего этого документа сообщения SIP между двумя кластерами будут зашифрованы с помощью TLS.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с:

- Cisco Unified Communications Manager (CUCM)
- SIP

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Версия 9.1 (2) CUCM
- Версия 10.5 (2) CUCM
- Microsoft Windows server 2003 как CA

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.

Общие сведения

Как показано в этом образе, Подтверждение связи SSL с помощью Сертификатов.

Настройка

Шаг 1. Используйте общественность CA или установленный CA на Windows Server 2003

См. ссылку: Установите CA на Windows 2003 Sever

Шаг 2. Проверьте имя хоста и параметры настройки

Сертификаты основываются на названиях. Гарантируйте, что названия корректны перед началом.

```
From SSH CLI
admin:show cert own CallManager
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
Subject Name: CN=CUCMA, OU=cisco, O=cisco, L=cisco, ST=cisco, C=IN
```

Для изменения имени хоста обратитесь к ссылке: Имя хоста Изменения на CUCM

Шаг 3. Генерируйте и загрузите запрос подписи сертификата (CSR)

CUCM 9.1 (2)

Для генерации CSR перейдите к**> Certificate Management> Security Admin OC>, Генерируют CSR**

В **Поле имени Сертификата** выберите опцию **CallManager** от выпадающего списка.

Для загрузки CSR перейдите к**> Certificate Management> Security Admin OC> CSR Загрузки**

В **Поле имени Сертификата** выберите опцию **CallManager** от выпадающего списка.

CUCM 10.5 (2)

Для генерации CSR перейдите к**> Certificate Management> Security Admin OC>, Генерируют**

CSR

1. В поле **Certificate Purpose** выберите **CallManager** от выпадающего списка.

2. В поле **Key Length** выберите **1024** от выпадающего списка.
3. В поле **Hash Algorithm** выберите **SHA1** от выпадающего списка.

Для загрузки CSR перейдите к**> Certificate Management> Security Admin OC> CSR Загрузки**

В поле **Certificate Purpose** выберите опцию **CallManager** от выпадающего списка.

> **Примечание:** CSR CallManager генерируется с Ключами алгоритма цифровой подписи райвеста шамира адлемана (RSA) на 1024 бита.

Шаг 4. . Подпишите CSR с центром сертификации Microsoft Windows 2003 года

Это - произвольные данные для подписания CSR с CA. Microsoft Windows 2003 года

1. Откройте центр сертификации.

2. Щелкните правой кнопкой мыши значок **CA** и перейдите ко **Всем Задачам>, Отправляют новый запрос**

3. Выберите CSR и нажмите опцию **Open** (Применимый и в CSR (CUCM 9.1 (2) и в CUCM 10.5 (2))

4. Все открытые CSR отображаются в Папке Запросов В состоянии ожидания. Щелкните правой кнопкой мыши каждый CSR и перейдите ко **Всем Задачам> Проблема** для запуска сертификатов. (Применимый и в CSR (CUCM 9.1 (2) и в CUCM 10.5 (2))

5. Для загрузки сертификата выберите папку **Issued Certificates**.

Щелкните правой кнопкой мыши сертификат и нажмите опцию **Open**.

6. Сведения о сертификате отображены. Для загрузки сертификата выберите вкладку **Details** и нажмите **кнопку Copy to File …**

7. В **Окне мастера Экспорта Сертификата** нажмите**, Base-64 закодировал X.509 (.CER)** кнопка с зависимой фиксацией.

8. Назовите файл точно. Данный пример использует формат **CUCM1052.cer**.

Для CUCM 9.1 (2), выполните ту же процедуру.

Шаг 5. . Получите корневой сертификат от CA

Откройте окно **Certification Authority**.

Для загрузки узла CA

1. Щелкните правой кнопкой мыши значок CA и нажмите **Параметр свойств**.

2. Во вкладке Общие нажмите **View Certificate.**

3. В окне **Certificate** нажмите подробную ВКЛАДКУ.

4. Щелкните Copy to File...

Шаг 6. Загрузка CA корневой сертификат как доверие CallManager

Для загрузки Корневого сертификата CA войдите к**> Certificate Management> Security Admin OC> Сертификат/Цепочка сертификатов Загрузки**

> **Примечание:** Выполните эти шаги и в CUCMs (CUCM 9.1 (2) и в CUCM 10.5 (2))

Шаг 7. Загрузка CA подписывает Сертификат CSR CallManager как сертификат CallManager.

Для загрузки CSR CallManager знака CA, входа в систему к**> Certificate Management> Security Admin OC> Сертификат/Цепочка сертификатов Загрузки**

> **Примечание:** Выполните эти шаги и в CUCMs (CUCM 9.1 (2) и в CUCM 10.5 (2))

Шаг 8. Создайте профили безопасности магистрального SIP-канала

CUCM 9.1 (2)

Для создания Профиля безопасности магистрального SIP-канала перейдите к **Системному> Security> Профиль безопасности магистрального SIP-канала**.

Скопируйте существующий Non Безопасный Профиль магистрали SIP и дайте ему новое имя. В примере Non Безопасный Профиль магистрали SIP был переименован с Безопасным TLS Профиля магистрали SIP.

В X.509 Имя субъекта используют Общее имя (CN) CUCM 10.5 (2) (CA подписанный сертификат) как показано в этом образе.

CUCM 10.5 (2)

Перейдите к **Системному> Security> Профиль безопасности магистрального SIP-канала.**

Скопируйте существующий Non Безопасный Профиль магистрали SIP и дайте ему новое имя. В примере Non Безопасный Профиль магистрали SIP был переименован с Безопасным TLS Профиля магистрали SIP.

В X.509 Имя субъекта используют CN CUCM 9.1 (2) (CA подписанный сертификат), как выделено:

Оба Профили безопасности магистрального SIP-канала устанавливают входящий порт 5061, в котором каждый кластер слушает на порте TCP 5061 для новых входящих вызовов TLS SIP.

Шаг 9. Создайте магистрали SIP

После того, как Профили безопасности созданы, создают магистрали SIP и вносят изменения для ниже параметра конфигурации на магистрали SIP.

CUCM 9.1 (2)

1. На **Окне конфигурации магистрали SIP** проверьте флажок **SRTP Allowed** параметра конфигурации.

Это защищает Протокол RTP, который будет использоваться для перекличек этот транк. Этот флажок должен только быть установлен при использовании TLS SIP, потому что ключами для Безопасного протокола транспорта в реальном времени (SRTP) обмениваются в теле сообщения SIP. Сигнализация SIP должна быть защищена TLS, иначе любой с незащищенной сигнализацией SIP мог дешифровать соответствующий поток SRTP по транку.

2. На **Разделе сведений SIP Окна конфигурации магистрали SIP** добавьте **Адрес назначения (DA)**, **Порт назначения** и **Профиль безопасности магистрального SIP-канала.**

CUCM 10.5 (2)

1. На **Окне конфигурации магистрали SIP** проверьте флажок **SRTP Allowed** параметра конфигурации.

Это позволяет SRTP использоваться для перекличек этот транк. Этот флажок должен только быть установлен при использовании TLS SIP, потому что ключами для SRTP обмениваются в теле сообщения SIP. Сигнализация SIP должна быть защищена TLS, потому что любой с незащищенной сигнализацией SIP мог дешифровать соответствующий Безопасный поток RTP по транку.

2. На **Разделе сведений SIP Окна конфигурации магистрали SIP** добавьте **IP - адрес назначения**, **Порт назначения** и **Профиль безопасности**

Шаг 10. Создайте шаблоны маршрута

Самый простой метод должен создать Шаблон маршрута на каждом кластере, указав непосредственно к магистрали SIP. Группы маршрутов и Списки маршрутов могли также использоваться.

CUCM 9.1 (2) точки к **Шаблону маршрута** 9898 через магистраль SIP TLS к CUCM 10.5 (2)

CUCM 10.5 (2) точки к **Шаблону маршрута** 1018 через магистраль SIP TLS к CUCM 9.1 (2)

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Вызов TLS SIP может быть отлажен с этими шагами.

Соберите захват пакета на CUCM

Для проверки подключения между CUCM 9.1 (2) и CUCM 10.5 (2), возьмите захват пакета на серверах CUCM и наблюдайте за трафиком TLS SIP.

Трафик TLS SIP передан на порте TCP 5061, замечен как tls sip.

В следующем примере существует сеанс CLI SSH, установленный к CUCM 9.1 (2)

1. Захват пакета CLI на экране

Этот CLI распечатывает выходные данные на экране для трафика TLS SIP.

```
admin:utils network capture host ip 10.106.95.200
Executing command with options:
interface=eth0
ip=10.106.95.200
19:04:13.410944 IP CUCMA.42387 > 10.106.95.200.sip-tls: P 790302485:790303631(1146) ack
3661485150 win 182 <nop,nop,timestamp 2864697196 5629758>
19:04:13.450507 IP 10.106.95.200.sip-tls > CUCMA.42387: . ack 1146 win 249 <nop,nop,timestamp
6072188 2864697196>
19:04:13.465388 IP 10.106.95.200.sip-tls > CUCMA.42387: P 1:427(426) ack 1146 win 249
<nop,nop,timestamp 6072201 2864697196>
```

2. Перехваты CLI к файлу

Этот CLI делает захват пакета на основе хоста и создает файл, названный пакетами.

```
admin:utils network capture eth0 file packets count 100000 size all host ip 10.106.95.200
```

Перезапустите магистраль SIP на CUCM 9.1 (2) и выполните вызов от расширения 1018 (CUCM 9.1 (2)) к расширению 9898 (CUCM 10.5 (2))

Для загрузки файла от CLI выполните эту команду:

```
admin:file get activelog platform/cli/packets.cap
```

Перехват сделан в стандарте .cap формат. Данный пример использует Wireshark для открытия packets.cap файла, но может использоваться любое программное средство показа захвата пакета.

1. Протокол TCP Синхронизируется (SYN) для установления TCP - взаимодействия между CUCM 9.1 (2) (Клиент) и CUCM 10.5 (2) (Сервер).
2. CUCM 9.1 (2) передает Сообщение приветствия клиента для начала сеанса TLS.
3. CUCM 10.5 (2) передает Приветствие сервера, Серверный сертификат и Запрос сертификата для начала процесса обмена сертификата.
4. Сертификат, который клиентский CUCM 9.1 (2) передает для завершения обмена сертификата.
5. Данные прикладной программы, который является зашифрованной сигнализацией SIP, показывают, что был установлен сеанс TLS.

Далее проверьте, обмениваются ли корректными сертификатами. После Приветствие сервера, сервер CUCM 10.5 (2) передает свой сертификат к клиентскому CUCM 9.1 (2).

Серийный номер и подчиненная информация, которую имеет сервер CUCM 10.5 (2), представлены клиентскому CUCM 9.1 (2).The серийный номер, предмет, отправитель, и даты законности - все по сравнению с информацией на странице OS Admin Certificate

Management.

Сервер CUCM 10.5 (2) подарки его собственный сертификат для проверки, теперь это проверяет сертификат клиентского CUCM 9.1 (2). Проверка происходит в обоих направлениях.

Если существует несоответствие между сертификатами в захвате пакета и сертификатами в веб-странице Admin OC, то корректные сертификаты не загружены.

Корректные сертификаты должны быть загружены на страницу OS Admin Cert.

Соберите трассировки CUCM

Трассировки CUCM могут также быть полезными для определения, какими сообщениями обмениваются между CUCM 9.1 (2) и CUCM 10.5 (2) серверы и установлен ли должным образом сеанс SSL.

В примере были собраны трассировки от CUCM 9.1 (2).

Поток вызова:

Ext 1018 > CUCM 9.1 (2) > TPAHK TLS SIP> CUCM 10.5 (2)> Ext 9898

++ Анализ цифровой информации

```
04530161.009 |19:59:21.185 |AppInfo |Digit analysis: match(pi="2", fqcn="1018",
cn="1018",plv="5", pss="", TodFilteredPss="", dd="9898",dac="0")
04530161.010 |19:59:21.185 |AppInfo |Digit analysis: analysis results
04530161.011 |19:59:21.185 |AppInfo ||PretransformCallingPartyNumber=1018
|CallingPartyNumber=1018
|DialingPartition=
|DialingPattern=9898
|FullyQualifiedCalledPartyNumber=9898
```

++ TLS SIP используется на порту 5061 для этого вызова.

```
04530191.034 |19:59:21.189 |AppInfo |//SIP/SIPHandler/ccbId=0/scbId=0/SIP_PROCESS_ENQUEUE:
createConnMsg tls_security=3
04530204.002 |19:59:21.224 |AppInfo
|//SIP/Stack/Transport/0x0/sipConnectionManagerProcessConnCreated: gConnTab=0xb444c150,
addr=10.106.95.200, port=5061, connid=12, transport=TLS Over TCP
04530208.001 |19:59:21.224 |AppInfo |SIPTcp - wait_SdlSPISignal: Outgoing SIP TCP message to
10.106.95.200 on port 5061 index 12
[131,NET]
INVITE sip:9898@10.106.95.200:5061 SIP/2.0
Via: SIP/2.0/TLS 10.106.95.203:5061;branch=z9hG4bK144f49a43a
From: <sip:1018@10.106.95.203>;tag=34~4bd244e4-0988-4929-9df2-2824063695f5-19024196
To: <sip:9898@10.106.95.200>
Call-ID: 94fffc00-57415541-7-cb5f6a0a@10.106.95.203
User-Agent: Cisco-CUCM9.1
```

++ Сообщение Signal Distribution Layer (SDL) SIPCertificateInd предоставляет подробную информацию о Подчиненном CN и информации о соединении.

```
04530218.000 |19:59:21.323
|SdlSig  |SIPCertificateInd                    |wait                          |SIPHandler(1,100,7
2,1)          |SIPTcp(1,100,64,1)             |1,100,17,11.3^*^*                        |[T:N-
H:0,N:1,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```

```
04530219.000 |19:59:21.324
|SdlSig  |SIPCertificateInd                    |restart0                       |SIPD(1,100,74,16)
             |SIPHandler(1,100,72,1)          |1,100,17,11.3^*^*                      |[R:N-
H:0,N:0,L:0,V:0,Z:0,D:0] connIdx= 12 --remoteIP=10.106.95.200 --remotePort = 5061 --
X509SubjectName /C=IN/ST=cisco/L=cisco/O=cisco/OU=cisco/CN=CUCM10 --Cipher AES128-SHA --
SubjectAltname =
```