Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Общие сведения](#)
[Условия](#)
[Описание](#)
[Транковая сторона и примеры стороны канала](#)
[Стратегия смягчения](#)
[Настройка](#)
[Конфигурация стороны канала](#)
[Конфигурация транковой стороны](#)
[Опции шифрования носителей](#)
[Нет](#)
[Обязательный](#)
[«Максимальные усилия»](#)
[Проверка](#)
[Устранение неполадок](#)
[Дополнительные сведения](#)
[Связанное чтение](#)
[Связанные RFC](#)

Введение

Этот документ описывает, как установить безопасный Протокол RTP между Сервером подключения Cisco Video (VCS) и Cisco Unified Communication Manager (CUCM).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- CUCM
- VCS Cisco или скоростная автомагистраль Cisco

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

обеспечения и оборудования:

- CUCM
- VCS Cisco или скоростная автомагистраль Cisco

  Примечание: Эта статья использует продукты Скоростной автомагистрали Cisco в целях пояснения (кроме, где сообщили), но информация также применяется, если ваши развертывания используют VCS Cisco.

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

Условия

- Вызовы Протокола SIP, направленные между CUCM и Скоростной автомагистралью
- Шифрование носителей наилучшим образом / дополнительное между Скоростной-автомагистралью-C и CUCM

Описание

Были трудности, сообщил для конфигурации шифрования носителей оптимального уровня для вызовов SIP, которые маршрутизируются между CUCM и VCS/скоростной автомагистралью. Распространенная ошибка конфигурации влияет на сигнализацию зашифрованных сред через Безопасный протокол транспорта в реальном времени (SRTP), который вызывает сбой наилучшим образом зашифрованных вызовов, когда транспорт между CUCM и Скоростной автомагистралью не безопасен.

Если транспорт не безопасен, то сигнализация шифрования носителей могла быть считана eavesdropper. В этом случае сигнальная информация шифрования носителей разделена из Протокола описания сеанса (SDP). Однако возможно настроить CUCM, чтобы передать (и ожидать получать) шифрование носителей, сигнализирующее по необеспеченному соединению. Можно обойти эту неверную конфигурацию одним из двух способов, зависящих от того, являются ли вызовы маршрутизировавшей транковой стороной или стороной канала к CUCM.

Транковая сторона и примеры стороны канала

Транковая сторона: магистраль SIP настроена на CUCM к Скоростной автомагистрали. Соответствующая соседняя зона настроена на Скоростной автомагистрали к CUCM. Вам был бы нужен транк, если бы вы хотели зарегистрированный в VCS (Скоростная автомагистраль не является регистратором, но VCS), оконечные точки для вызова CUCM-зарегистрированных оконечных точек. Другой пример должен был бы включить H.323,

взаимодействующий в ваших развертываниях.

Сторона канала: вызовы Стороны канала идут непосредственно в CUCM, не через транк. Если вся регистрация и управление вызовами предоставлены CUCM, ваши развертывания не могли бы потребовать транка к Скоростной автомагистрали. Например, если Скоростная автомагистраль развернута просто для Мобильного и Удаленного доступа (MRA), это проксирует вызовы стороны канала от внешних оконечных точек до CUCM.

Стратегия смягчения

Если существует магистраль SIP между CUCM и Скоростной автомагистралью, сценарий нормализации на CUCM переписывает SDP соответственно так, чтобы наилучшим образом не было отклонено требование шифрования. Этот сценарий автоматически установлен с более поздними версиями CUCM, но если вы наилучшим образом зашифровали отклоненные требования, Cisco рекомендует, чтобы вы загрузили и установили последний сценарий vc-interop для своей версии CUCM.

Если вызов пойдет сторона канала в CUCM, то CUCM ожидает видеть `x-cisco-srtp-fallback` заголовок, если шифрование носителей является дополнительным. Если CUCM не видит этот заголовок, он рассматривает вызов быть обязательным шифрованием. Поддержка этого заголовка была добавлена к Скоростной автомагистрали в версии X8.2, таким образом, Cisco рекомендует X8.2 или позже для MRA (край совместной работы).

Настройка

Конфигурация стороны канала

[CUCM] <-наилучшим образом-> [Скоростная-автомагистраль-C] <-обязательный-> [Скоростная-автомагистраль-E] <-обязательный-> [Оконечная точка]

Для включения наилучшим образом шифрования вызовов стороны канала от Скоростной-автомагистрали-C до CUCM:

- Используйте поддерживаемые развертывания / решение (например, MRA)
- Используйте Смешанную безопасность Режима на CUCM
- Гарантируйте, что Скоростная автомагистраль и CUCM доверяют друг другу (Центр сертификации (CA), который подписывается, сертификатам каждой стороны должна доверять другая сторона),
- Используйте версию X8.2 или позже Скоростной автомагистрали
- Используйте безопасные телефонные профили на CUCM с набором Режима безопасности устройства к Аутентифицируемому или Зашифрованному - для этих режимов, типом передачи является Transport Layer Security (TLS)

Конфигурация транковой стороны

- Используйте поддерживаемые развертывания / решение
- Используйте Смешанную безопасность Режима на CUCM

- Гарантируйте, что Скоростная автомагистраль и CUCM доверяют друг другу (CA, который подписывается, сертификатам каждой стороны должна доверять другая сторона),
- Выберите оптимальный уровень в качестве режима шифрования, и TLS как транспорт на соседней зоне от Скоростной автомагистрали до CUCM (эти значения автоматически предварительно заполнены в случае стороны канала),
- Выберите TLS как входящий и исходящий транспорт на Профиле безопасности магистрального SIP-канала
- Проверьте Позволенный SRTP (см. оператор Caution) на магистрали SIP от CUCM до Скоростной автомагистрали
- Проверьте для и применитесь при необходимости, корректный сценарий нормализации для ваших версий CUCM и Скоростной автомагистрали

Внимание: При проверке флажка SRTP Allowed Cisco строго рекомендует использовать зашифрованный профиль TLS так, чтобы ключи и другая связанная с безопасностью информация не становились представленными во время согласований вызова. При использовании незащищенного профиля SRTP будет все еще работать. Однако ключи будут представлены в сигнализации и трассировках. В этом случае необходимо гарантировать безопасность сети между CUCM и стороной - получателем транка.

Опции шифрования носителей

Нет

Шифрование не позволено. Вызовы, которые требуют шифрования, должны отказать, потому что они не могут быть безопасными. CUCM и Скоростная автомагистраль последовательны в сигнализации для этого случая.

CUCM и Скоростная автомагистраль оба использования `m=RTP/AVP` для описания сред в SDP. Нет никаких крипто-атрибутов (нет `a=crypto...` линии в разделах сред SDP).

Обязательный

Шифрование носителей требуется. Незашифрованные вызовы должны всегда отказывать; никакая нейтрализация не позволена. CUCM и Скоростная автомагистраль последовательны в сигнализации для этого случая.

CUCM и Скоростная автомагистраль оба использования `m=RTP/SAVP` для описания сред в SDP. SDP имеет крипто-атрибуты (`a=crypto...` линии в разделах сред SDP).

«Максимальные усилия»

Зашифрованы вызовы, которые могут быть зашифрованы. Если шифрование не может быть установлено, вызовы могли бы и должны переключиться на незашифрованные среды. CUCM и Скоростная автомагистраль противоречивы в этом случае.

Если транспортом является Протокол TCP или Протокол UDP, скоростная автомагистраль всегда отказывается от шифрования. Если вы хотите шифрование носителей, необходимо защитить транспорт между CUCM и Скоростной автомагистралью.

SDP (поскольку CUCM пишет его): Зашифрованные среды описаны как `m=RTP/SAVP` и `a=crypto` линии записаны в SDP. Это - корректная сигнализация для шифрования носителей, но крипто-линии читаемы, если транспорт не безопасен.

Если CUCM видит `x-cisco-srtp-fallback` заголовок, это позволяет вызову переключиться на незашифрованный. Если этот заголовок отсутствует, CUCM предполагает, что вызов требует шифрования (не позволяет нейтрализацию).

С X8.2 Скоростная автомагистраль делает оптимальный уровень тот же путь, как CUCM делает в случае стороны канала.

SDP (поскольку Скоростная автомагистраль пишет транковую сторону): Зашифрованные среды описаны как `m=RTP/AVP` и `a=crypto` линии записаны в SDP.

Однако существует две причины, что a=crypto линии могли отсутствовать:

1. Когда транспортный переход к или от прокси SIP на Скоростной автомагистрали не безопасен, прокси разделяет крипто-линии для предотвращения их от воздействия на небезопасном переходе.
2. Сторона ответа разделяет крипто-линии, чтобы сигнализировать, что она не может или не делать шифрования.

Использование корректного сценария нормализации SIP на CUCM смягчает эту проблему.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

Связанное чтение

- Руководство по обеспечению безопасности Cisco Unified Communications Manager, выпуск 10.0 (1)
- Оптимизированная конференц-связь для Cisco Unified Communications Manager и руководства по решениям VCS Cisco (Выпуск 2.0)
- Cisco Unified Communications Manager со скоростной автомагистралью Cisco (магистраль SIP) руководство по развертыванию (для скоростной автомагистрали Cisco

X8.2 и унифицированный CM 8.6x и 9. x
- Cisco Unified Communications Manager с VCS Cisco (магистраль SIP) руководство по развертыванию (для Cisco VCS X8.2 и унифицированного CM 8.6.x и 9. x
- Унифицированная связь Мобильный и Удаленный доступ через Руководство по развертыванию VCS Cisco (Для Cisco VCS X8.2 и Cisco Унифицированный CM 9.1 (2) SU1 или позже)
- Унифицированная связь Мобильный и Удаленный доступ через Руководство по развертыванию Скоростной автомагистрали Cisco (Для Скоростной автомагистрали Cisco X8.2 и Cisco Унифицированный CM 9.1 (2) SU1 или позже)
- Cisco Systems – техническая поддержка и документация

Связанные RFC

- RFC 3261 SIP: Протокол инициализации сеанса (SIP)
- RFC 4566 SDP : протокол описания сеанса
- RFC 4568 SDP : описания безопасности