Содержание

Введение

Много администраторов сети принимают решение внедрить Cisco Unified Communications Manager Express (CME) с безопасностью. Вместо встроенного Центра сертификации IOS (IOS CA) администраторы сети могут принять решение интегрировать Безопасный CME со своей существующей инфраструктурой инфраструктуры открытого ключа (PKI). Этот документ описывает, как настроить Безопасный CME для работы с безопасной сигнализацией и средами, через сертификаты третьей стороны.

Предварительные условия

Требования

Этот документ предполагает, что Cisco Unified Communications Manager Express (CME) в вашей среде работает и полностью функциональный. Все телефоны, которые должны быть в рабочем состоянии на Безопасной Cisco Унифицированный CME , должны быть в состоянии к первому, успешно регистрируются к CME. См. Руководство системного администратора Cisco Unified Communications Manager Express для получения информации о том, как настроить CME.

Этот документ также предполагает, что включены и голос и характеристики безопасности.

Используемые компоненты

Сведения в этом документе основываются на Cisco Unified Communications Manager Express (CME).

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.

Условные обозначения

Сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Итоговые действия настройки

1. Создайте экземпляр IOS CA.
2. Создайте точки доверия для удержания сертификатов CA третьей стороны.
3. Генерируйте Запросы подписи сертификата (CSR) от точек доверия.
4. CSR знака с использованием Проверки подлинности сервера, и получают сертификацию CA.
5. Аутентифицируйте точки доверия с сертификатом CA и импортируйте соответствующие сертификаты идентификации.
6. Проверьте точки доверия сертификата третьей стороны.
7. Создайте IOS CA точка доверия CME.
8. Настройте клиента Списка надежных сертификатов (CTL).
9. Настройте сервер функции представительства сертифицирующей организации (CAPF).
10. Настройте сервис телефонии.
11. Настройте проверочный телефон.
12. Проверка.

Пример подробной конфигурации

1. Создайте экземпляр IOS CA. Экземпляр IOS CA производит подписанный сертификат, который используется для подписания логически значимого сертификата (LSC) телефона.
2. Создайте точки доверия, которые будут генерировать CSR для подписания третьей стороны. Эти точки доверия в конечном счете держат сертификат CA третьей стороны, а также сертификаты идентификации, которые являются результатом CSR.

3. Генерируйте CSR от точек доверия. **Команда crypto pki enroll** производит CSR, который предоставлен третьей стороне CA для подписания.

   Пример 1:
   Пример 2:
4. Используйте два CSR для генерации сертификатов с разрешениями Проверки подлинности сервера.

Примечания: Важно, что полная цепочка сертификатов получена для одного из этих двух сертификатов от CA. , цепочка сертификатов предоставляет и CA и сертификат идентификации от CA. подписанияГарантируйте, что сертификаты загружены в ядре 64 формата.Очень важно, чтобы сертификат CA использовался для аутентификации для каждой точки доверия и что сертификаты идентификации импортированы в каждую точку доверия в том заказе.

5. Аутентифицируйте точки доверия с сертификатами CA и импортируйте сертификаты идентификации SAST.

   Пример 1:

   Пример 2:
6. Однажды и CA и сертификаты идентификации загружены в соответствующие точки доверия, проверяют цепочку сертификатов для каждой точки доверия. Этот шаг гарантирует, что были успешно выполнены предыдущие шаги.

7. Создайте IOS CA точка доверия CME.

   Поскольку точка доверия IOS CA не может использоваться для аутентификации клиента (соединение безопасности транспортного уровня (TLS) с телефонами), необходимо создать другую точку доверия и поместить СЕРТИФИКАТ CA IOS в него.

   Эта точка доверия используется только для авторизации запроса IP-телефона о TLS подключение (таким образом, они могут зарегистрироваться должным образом).

8. Настройте клиента CTL.

   Примечание: Гарантируйте, что файл CTL был создан успешно:
9. Настройте сервер CAPF.

10. Настройте сервис телефонии.

11. Настройте проверочный телефон (ephone), чтобы обновить его сертификат и использовать режим шифрования. Как только конфигурация завершена, перезагрузила телефон и ждет его для регистрации.

    Примечание: Прежде чем телефон перезагружен, гарантируйте, что нет никакой конфигурации безопасности, уже представляют. Если конфигурация безопасности присутствует, это должно быть вручную удаленный или завершите сброс фабрики проверочного телефона до регистрации для Обеспечения Cisco Унифицированный CME.

    Для сброса телефона выполните эти команды:Как только телефон получил обновленный LSC, команда **пустой строки подлинного режима обновления свидетельства-oper** удалена.
12. Проверьте, что телефон зарегистрировался и в Аутентификации и в Шифровании.

Защитите Cisco, Унифицированный CME должен быть полностью функциональным с

сертификатами третьей стороны.

Дополнительные сведения

- Руководство системного администратора Cisco Unified Communications Manager
- Безопасный голос на центре технической поддержки Cisco Wiki
- Cisco Systems – техническая поддержка и документация