Решите проблемы сертификата для VPN SSL с CME

Содержание

Введение

Этот документ описывает методологию для устранения проблем регистрации IP-телефона к Communications Manager Express (CME) через VPN Уровня защищенных сокетов (SSL).

Предварительные условия

Требования

Cisco рекомендует иметь основное понимание сертификатов безопасности, пакетного программного средства получения и Communications Manager Express.

Используемые компоненты

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

- Выпуск 8.6 Communications Manager Express
- Выпуск 8.5.3 IP-телефона Cisco 7965

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.

Решите проблемы сертификата

Существует два метода для устанавливания VPN SSL между IP-телефоном в Интернете и CME в корпоративной сети.

- CME находится позади устройства адаптивной защиты Cisco (ASA), который действует как Головная станция VPN. В этом сценарии CME и ASA совместно используют тот же сертификат, и IP-телефон выполняет согласование о настройке безопасности с ASA.
- CME связан с Интернетом непосредственно и действует как Головная станция VPN. Это выполняет согласование о настройке безопасности с IP-телефоном непосредственно.

В обоих сценариях, устанавливая VPN SSL между IP-телефоном в Интернете и CME состоит из подобных шагов:

1. CME генерирует или получает сертификат безопасности.
2. CME "выдвигает" хэш сертификата в формате Base64 к телефону через файл config, который телефон загружает от CME через TFTP.
3. IP-телефон пытается войти с Головной станцией VPN и получает сертификат по протоколу Transport Layer Security (TLS).
4. IP-телефон извлекает хэш из сертификата и сравнивает его с хэшем, который это загрузило от CME ранее. Если хэш совпадает, то телефон доверяет Головной станции VPN и продолжает дальнейшее согласование VPN.

Проверка

Чтобы проверить, что CME выдвинул хэш к IP-телефону, проверьте файл конфигурации, который это генерировало для безопасного телефона. Для упрощения этого шага можно настроить CME, чтобы генерировать файл конфигурации на телефон и сохранить его во флэш-памяти:

```
R009-3945-1(config-telephony)#cnf-file perphone
R009-3945-1(config-telephony)#cnf-file location flash:
```

Чтобы гарантировать, что новая конфигурация генерируется, рекомендуется воссоздать файлы конфигурации:

```
R009-3945-1(config-telephony)#no create cnf-files
CNF files deleted
R009-3945-1(config-telephony)#create cnf-file
Creating CNF files
```

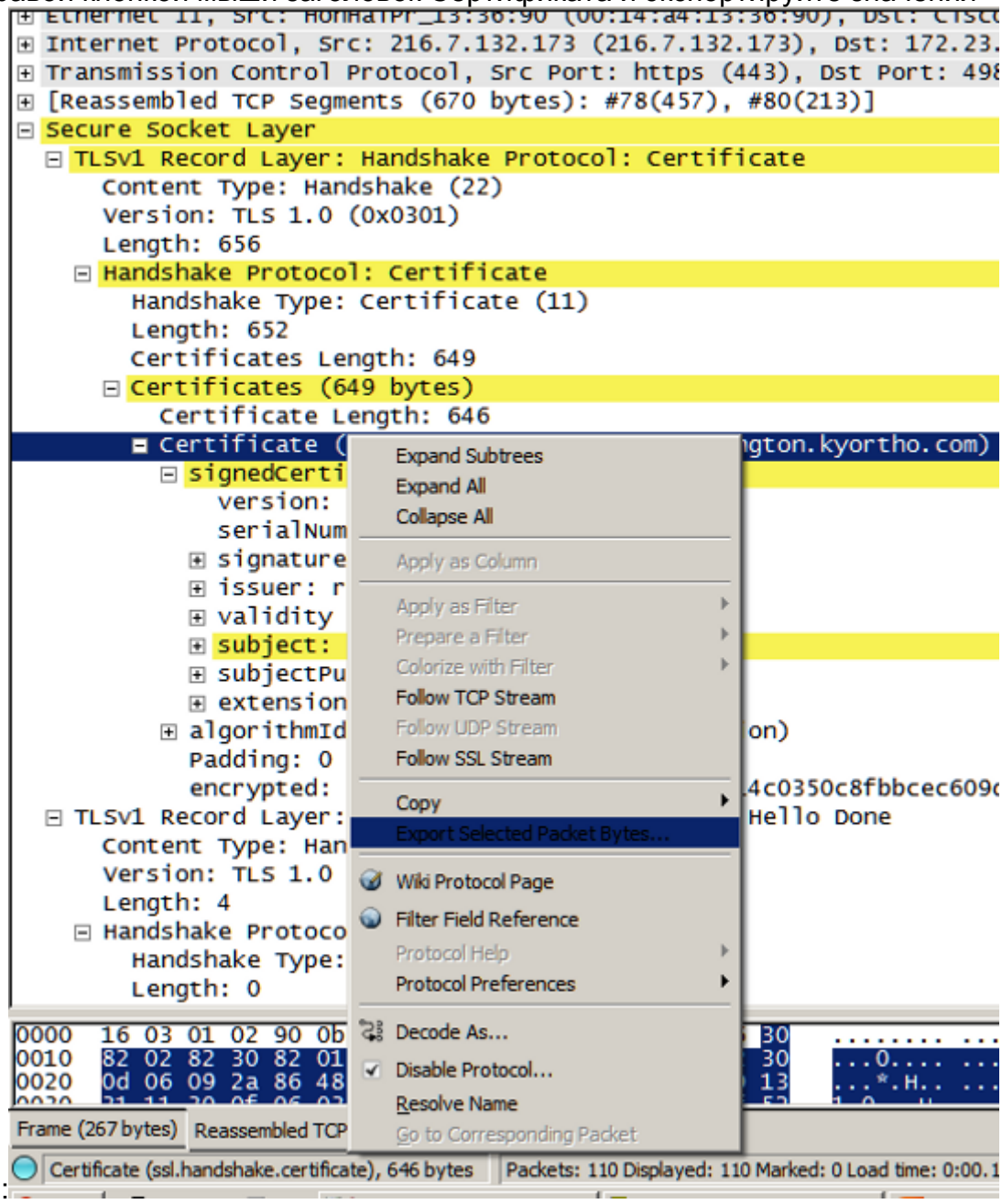
После соответствующего файла конфигурации в показах флэш-памяти (для ephone с настроенной группой vpn), необходимо видеть эту близость конец содержимого файла:

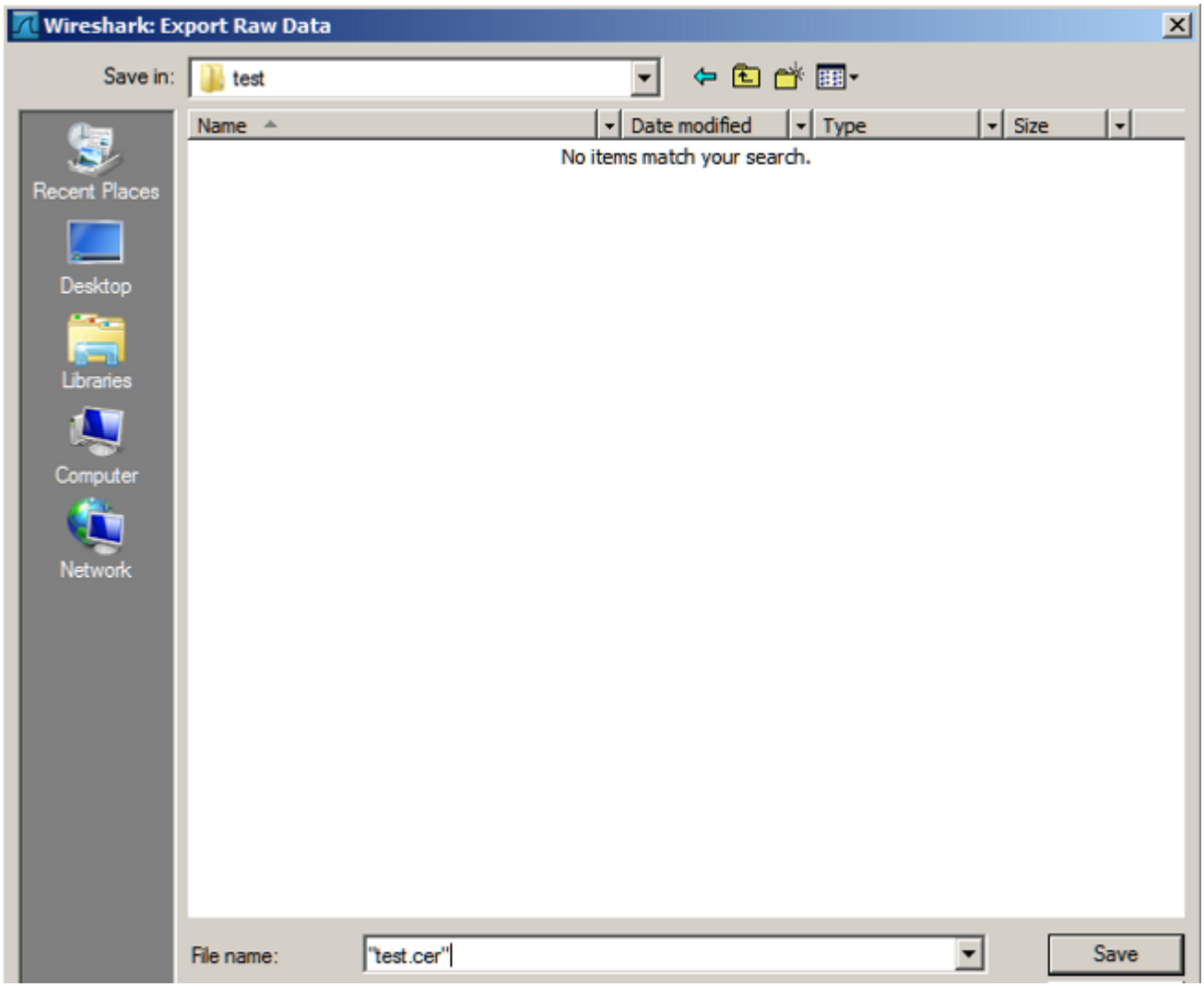
```
<vpnGroup>  <enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.201.160.201/SSLVPNphone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>fZ2xQHMBcWj/fSoNs5IkPbA2Pt8=</certHash1>
</credentials>
</vpnGroup>
```

Значение certHash1 является хэшем сертификата. Когда IP-телефон получит сертификат от Головной станции VPN во время настройки TLS, это ожидает, что хэш сертификата будет тем же как сохраненное значение хеш-функции. Если IP-телефон бросает "Плохой Сертификат" ошибка, могло бы случиться так, что не совпадают значения хеш-функции.

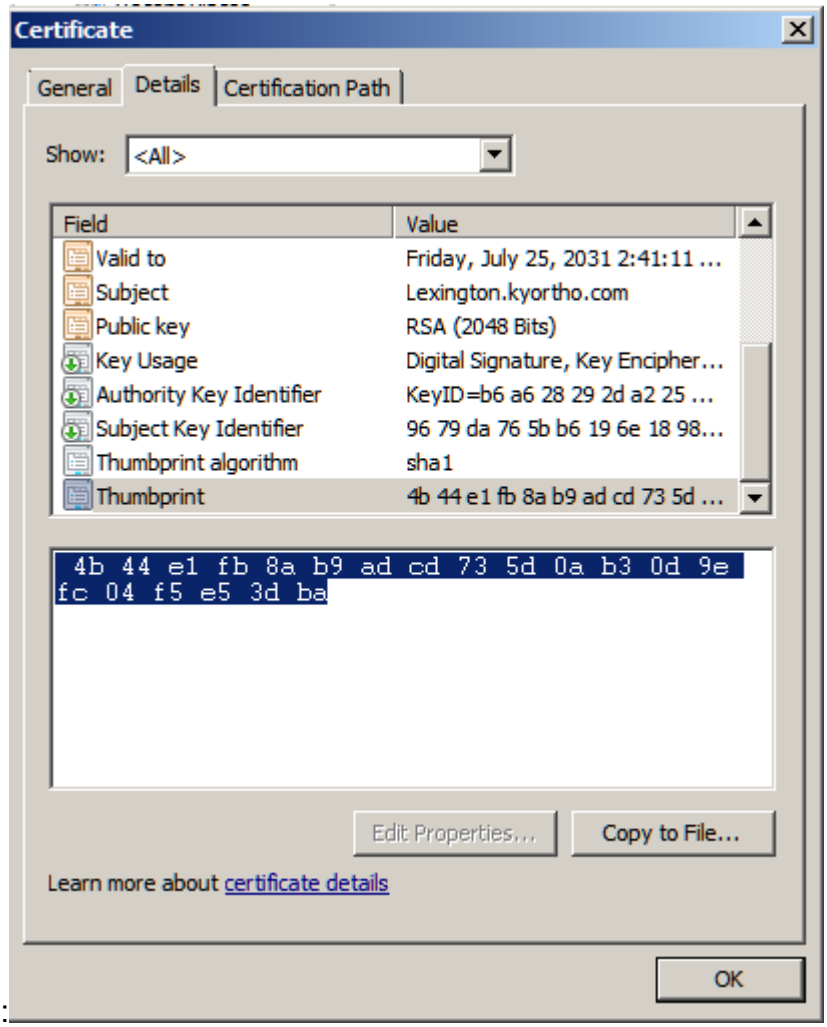
Для проверки выполните эти действия для извлечения значения хеш-функции из захвата пакета, собранного между IP-телефоном и Головной станцией VPN:

1. Найдите пакет от устройства Головной станции VPN до IP-телефона, который содержит сертификат. Это, как правило, находится в TLS Приветствие сервера пакет.
2. Разверните содержимое пакета и найдите заголовок:
   Уровень защищенных сокетов> Уровень Записи V1 TLS> Протокол подтверждения связи: Сертификат> Сертификаты> Сертификат.
3. Щелкните правой кнопкой мыши заголовок Сертификата и экспортируйте значения в.CER файл:





4. Откройте.CER файл, перейдите к вкладке Details, выберите Thumbprint и выберите значения. Значения являются хэшем в шестнадцатеричном



формате:

5. Затем, вы преобразовываете хэш от hex до Base64 с помощью любого онлайнового программного средства преобразования Hex к base64. Преобразованное значение может быть по сравнению со значением хеш-функции в файле конфигурации IP-телефона, если они не совпадают, тогда это означает, что хэш, полученный IP-телефоном, от другого сертификата, чем, что используется Головной станцией VPN для SSL.

Дополнительные сведения

- VPN-клиент SSL (SVC) Настройки для IP-телефонов SCCP
- Cisco Systems – техническая поддержка и документация

>