Содержание

Введение

Этот документ описывает основы Transport Layer Security (TLS) Протокола SIP и Безопасного протокола транспорта в реальном времени (SRTP) по Cisco Unified Border Element (CUBE) с примером конфигурации.

Засекреченная телефонная связь по CUBE может быть разделена на две части:

- Безопасная сигнализация? CUBE использует TLS для обеспечения сигнализации по SIP и Протокол IPSEC (Internet Protocol Security) (IPSec) для обеспечения сигнализации по H.323
- Безопасные среды? SRTP

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Файлы Списка надежных сертификатов (CTL) Cisco Unified Communications Manager (CUCM) созданы для Смешанного режима
- IP-телефоны зарегистрированы в Безопасном режиме (Шифрование)
- CUBE основной voip голосового сервиса и конфигурация адресуемой точки вызова сделан

Используемые компоненты

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

- CUCM 10.5
- CUBE? 3925E с IOS 15.3 (3) M3
- IP-коммуникатор Cisco (CIPC)

Общие сведения

- TLS - TLS и его предшественник, Уровень защищенных сокетов (SSL), являются криптографическими протоколами, которые предоставляют безопасность связи по Интернету.

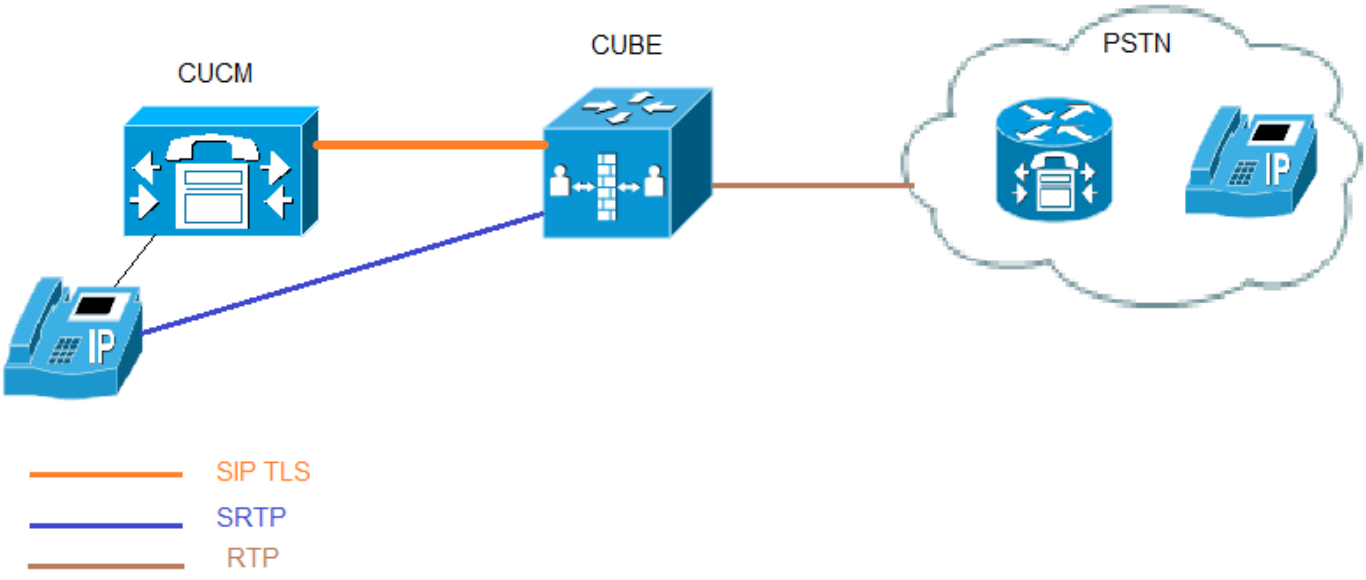
В эквивалентностях модели Взаимодействия открытых систем (OSI) TLS/SSL инициализируется на уровне 5 (уровень сеанса связи) и затем работает над уровнем 6 (уровень представления). И в моделях, TLS и в SSL работают от имени уровня базовой передачи, сегменты которого несут зашифрованные данные.

- Центр сертификации (CA) - Надежный объект, который выполняет сертификаты: Cisco или сторонний объект.
- Устройство аутентификации - Процесс, который проверяет идентичность устройства и гарантирует, что объект - то, чем это утверждает, что было перед соединением, сделан.
- Шифрование- Процесс перевода данных в шифрованный текст, который гарантирует конфиденциальность информации. Только целевой получатель может считать данные. Это требует алгоритма шифрования и ключа шифрования.
- Общественность/Секретные ключи - Ключи, которые используются в шифровании. Открытые ключи широко доступны, но секретные клавиши удерживаются их соответствующими владельцами. Асимметричное шифрование комбинирует оба типа.

Настройка

Схема сети

В этом образе, примере конфигурации для того, чтобы установить TLS SIP и SRTP между телефоном CUCM/IP и CUBE показан.
CUBE объединяется в сеть между SRTP и Протоколом RTP



Конфигурация CUBE

1. Настройте часы и включите сервер HTTP

Синхронизируйте часы в сервере CA и клиентских точках доверия (CUBE/OGW/TGW). В противном случае существуют проблемы с законностью

сертификатов, выполненных сервером CA.

Клиентские точки доверия используют HTTP для получения сертификата от CA.

1. Генерируйте криптографическую пару RSA

Этот шаг генерирует Секретные и Открытые ключи.

В данном примере CUBE является просто меткой. Это может быть что-либо.

1. Настройте IOS CA сервер

В данном примере CA Сервер называют кубом приблизительно

1. Создайте точки доверия PKI для куба для связи TLS.

В данном примере название точки доверия для CUBE является TLS CUBE. IP-адрес, используемый в enrollment url, должен быть локальным интерфейсом на CUBE. Имя субъекта, используемое в этом шаге, должно совпасть на Имени субъекта X.509 на Профиле безопасности магистрального SIP-канала CUCM. Оптимальный метод должен использовать имя хоста с доменным именем (если доменное имя включено).

Объединенные Открытые и секретные ключи криптосистемы RSA созданы в Шаге 2.

5. Аутентифицируйте точку доверия с сервером CA и примите сертификат CA.

```
Secure-CUBE(config)#crypto pki authenticate CUBE-TLS
Certificate has the following attributes:
      Fingerprint MD5: BCEBB5A1 1AC882F7 24BE476D 06537711
    Fingerprint SHA1: CE2FEEA5 42515B33 3EF6A8F6 7E31D6DF 8E32BEB6

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Secure-CUBE(config)#
```

1. Зарегистрируйте точку доверия с сервером CA.

В этом шаге CUBE получает подписанный сертификат от CA.

```
Secure-CUBE(config)#crypto pki enroll CUBE-TLS
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:


% The subject name in the certificate will include: CN=Secure-CUBE
% The fully-qualified domain name will not be included in the certificate
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CUBE-TLS' commandwill show the fingerprint.

Secure-CUBE(config)#
```

1. Создайте точку доверия для CUCM.

Если Группа CallManager имеет множественные Серверы CM, то точка доверия должна быть создана для всех серверов, иначе аварийное переключение не работает.

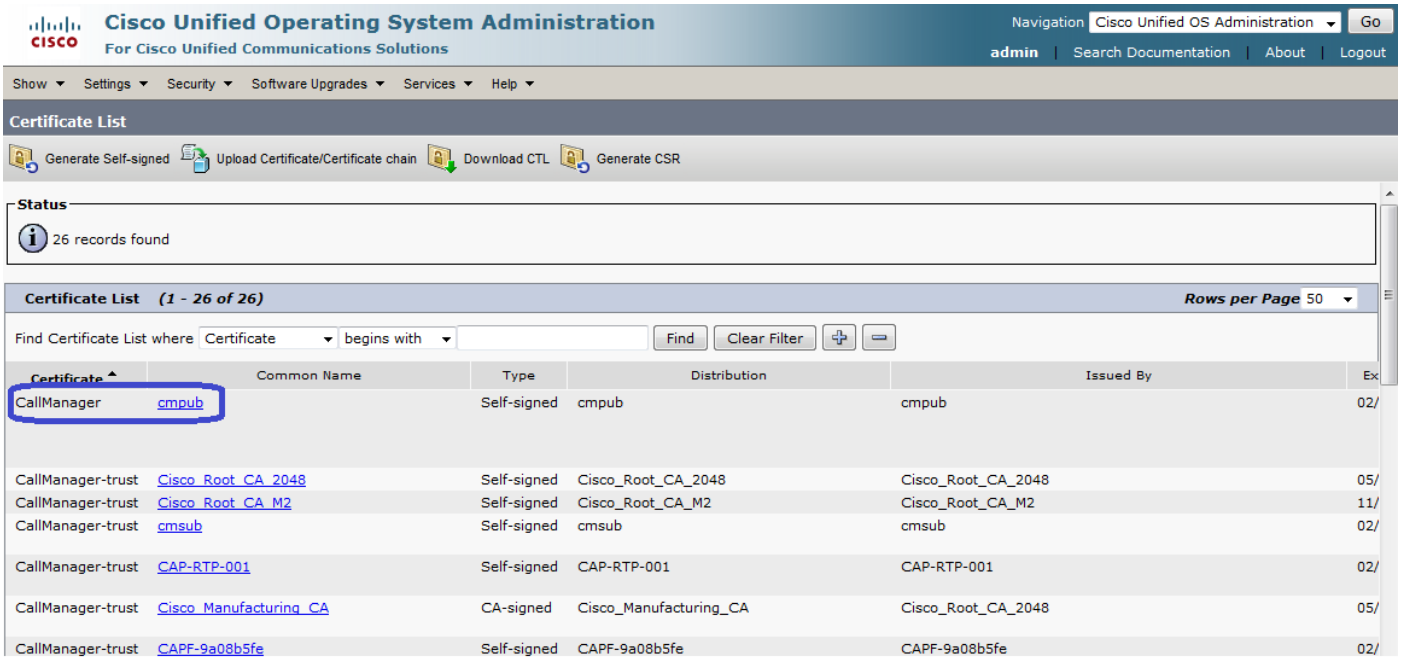
```
crypto pki trustpoint cucmpub
 enrollment terminal
 revocation-check none

crypto pki trustpoint cucmsub
```

```
enrollment terminal
revocation-check none
```

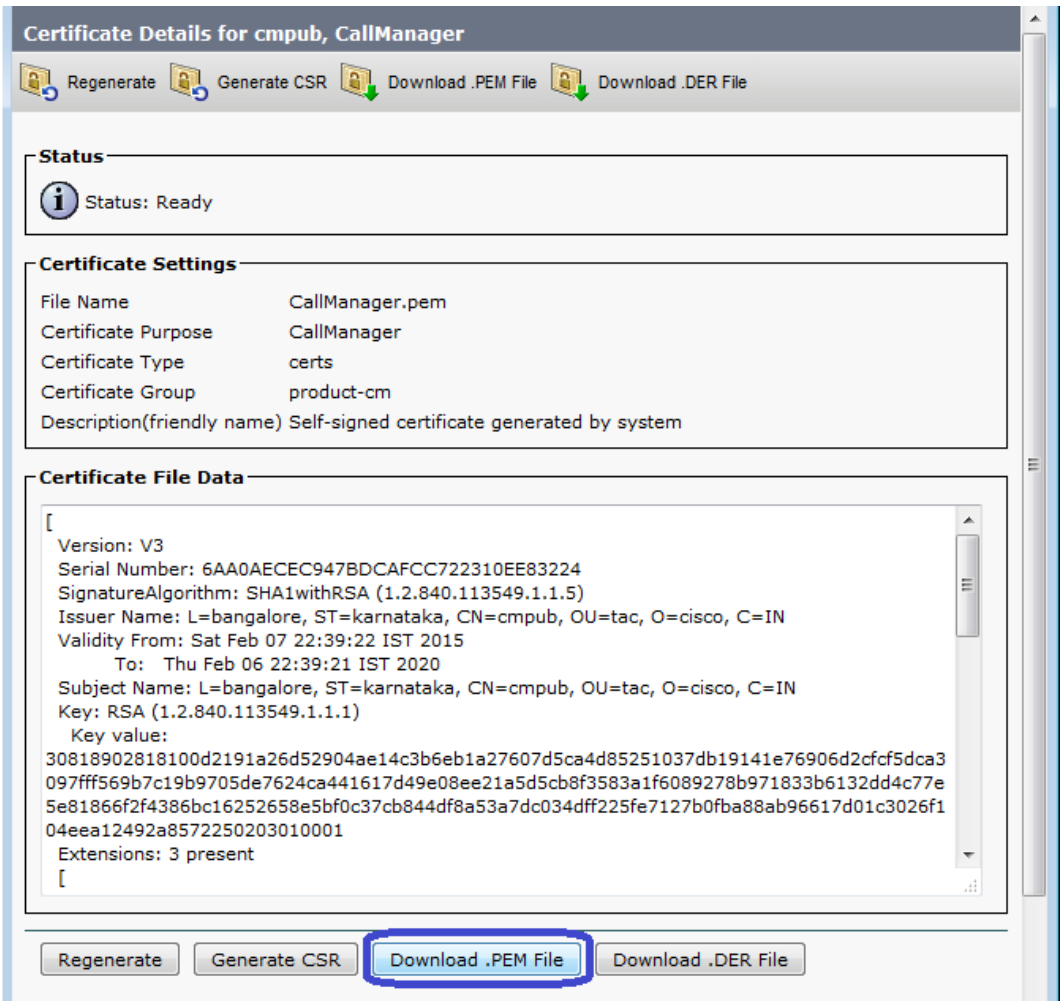
1. Зарегистрируйте сертификат CUCM к CUBE.

Шаг 1. Войдите в систему admin ОС CUCM.

Шаг 2. Перейдите к **Безопасности> Управление сертификатами>, Находят.**



Шаг 3. Нажмите сертификат **CallManager**, затем загрузите и сохраните файл.PEM как показано в этом образе.



Шаг 4. Откройте файл сертификата в CUBE и скопируйте содержание с СЕРТИФИКАТА BEGIN для ОКОНЧАНИЯ СЕРТИФИКАТА.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Шаг 6. Выполните ту же процедуру для других серверов CUCM.

1. Настройте TLS TCP как транспортный протокол.

Это может быть сделано или в глобальном или на уровне точки вызова.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01
```

```
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

1. Назначьте точку доверия для sip-ua, эта точка доверия используется для всего SIP, сигнализирующего между CUBE и CUCM

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

или точка доверия по умолчанию может быть настроена для всего SIP, сигнализирующего от CUBE.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
```

```
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

1. Включите SRTP.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

1. Для SRTP и сетевых технологий RTP, требуется безопасный перекодировщик.

Если версия IOS 15.2.2T (CUBE 9.0) или позже тогда, перекодировщик LTI может быть, настраивают для уменьшения конфигурации.

Перекодировщику LTI не нужна конфигурация точки доверия PKI для вызовов RTP SRTP

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
```

```
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Если IOS ниже 15.2.2T, то настройте перекодировщик sccp.

Перекодировщику Протокола SCCP была бы нужна точка доверия для сигнализации, однако, если то же маршрутизатор используется для хостинга перекодировщика тогда, та же точка доверия (TLS CUBE) может использоваться для CUBE, а также перекодировщика.

```
Secure-CUBE(config)#crypto pki authenticate cucmpub

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICojCCAgugAwIBAgIQaqCuzslHvcr8xyIxDugyJDANBgkqhkiG9w0BAQUFADBj
MQswCQYDVQQGEwJJTjEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY21wdWIxEjAQBgNVBAgTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMloXDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwN0YWMxDjAMBgNVBAMTBWNtcHVi
MRIwEAYDVQQIEwlrYXJuYXRha2ExEjAQBgNVBAcTCWJhbmdhbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUHn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iGl1cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAaNXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAwUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZl/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJJfXb3iKJPsMRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGXO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUIcumDASp
SkXO8/Ar
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint MD5: 92DA2B5B A888784D C53B6C29 2E2B6A3C
Fingerprint SHA1: 5D31BEF0 DF2DCA7E 64D40246 89E564DD 9A7F8A01

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

Secure-CUBE(config)#
```

Конфигурация CUCM

1. Сертификат IOS CUBE экспорта к CUCM.

Шаг 1. Сертификат IOS экспорта. Скопируйте самоподписанный сертификат CA и сохраните

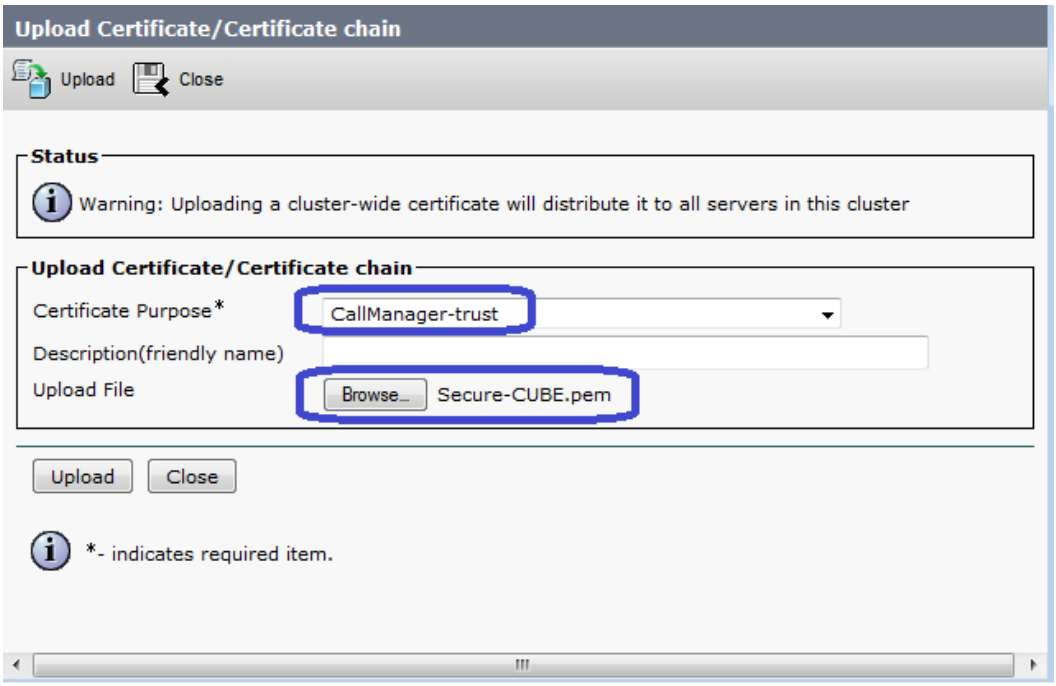
как файл.PEM, например, Безопасный-CUBE.pem

```
 Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVoXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtN3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr0lvbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH32lJ5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpoxpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAaNjMGEwDwYDVR0TAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCV7P+mlbpMfC/qh14z5/RzL
e5Bq6NUnxWByLR4gcFjmdSlE6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB7TCCAVagAwIBAgIBAjANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKWtfO
F9bBVYhVwQK8y2c5NMkJCY//pisg+oforvxalPKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTwk5jf9+YGIMVsivbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAf
BgNVHSMEGDAWgBSerO9rMr/upfOGShOIAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOWVf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXxAOTHhOsEbm/vfqk2vbYiHUO9AtDDI+kNecSuOGmd7fokJMP9K1xc1i2a
vrr2qwQYqRAh68BwTjWzR3mFAGbDZZwiywv1jJ92ra3EMAUc0sJZSLzGY0+BjO/E
dEW6JUIOx3NxP2SBN1NMAQ0=
-----END CERTIFICATE-----

Secure-CUBE(config)#
```

Шаг 2. Сертификат CA IOS загрузки на CUCM как доверие CallManager.

Шаг 3. Переместитесь к **CM по> Certificate Management> Security администрирования ОС> Сертификат/Цепочка сертификатов Загрузки**

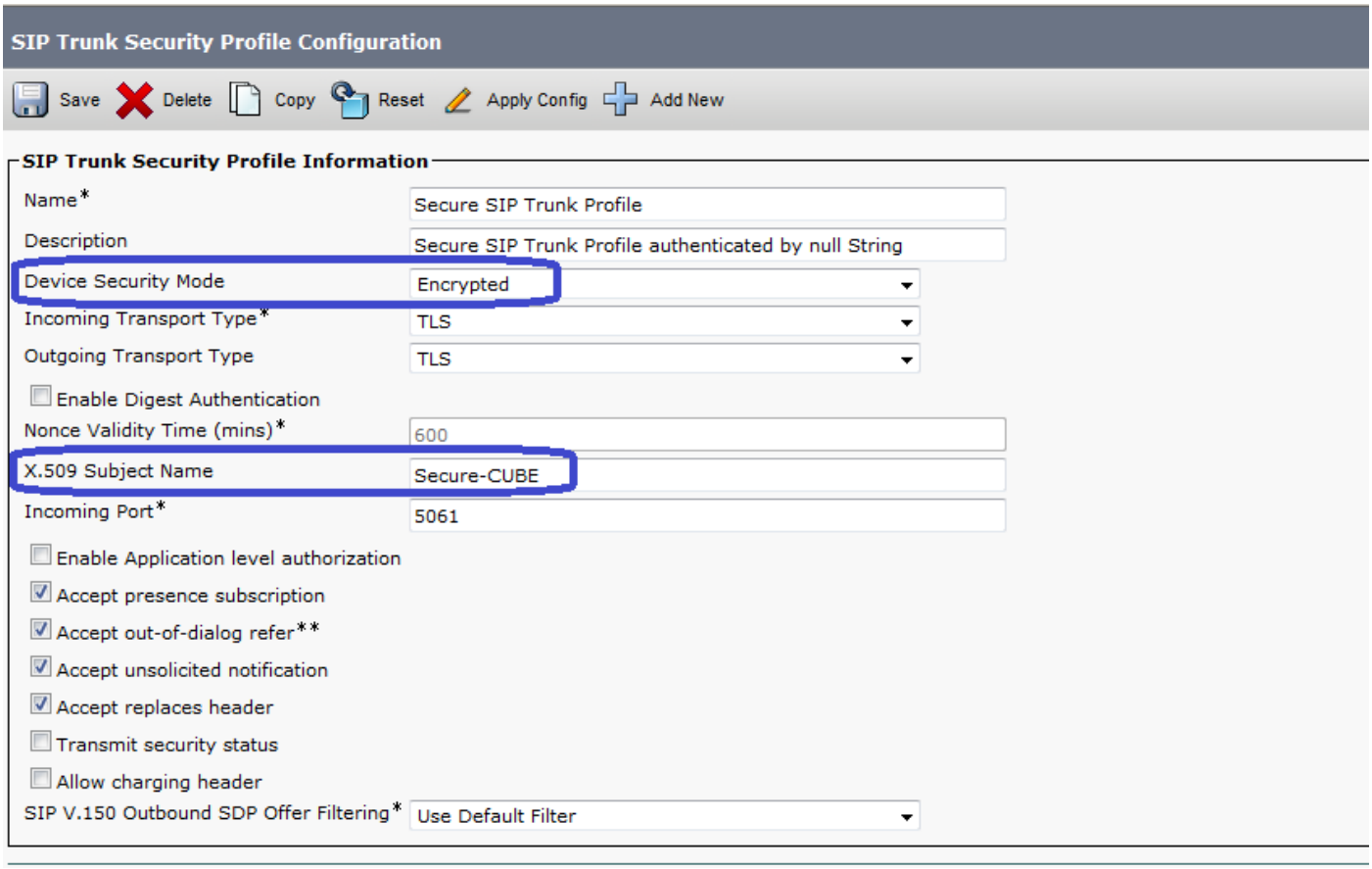
Шаг 4. Файл.PEM загрузки как показано в этом образе.



1. Создайте новый профиль безопасности магистрального SIP-канала

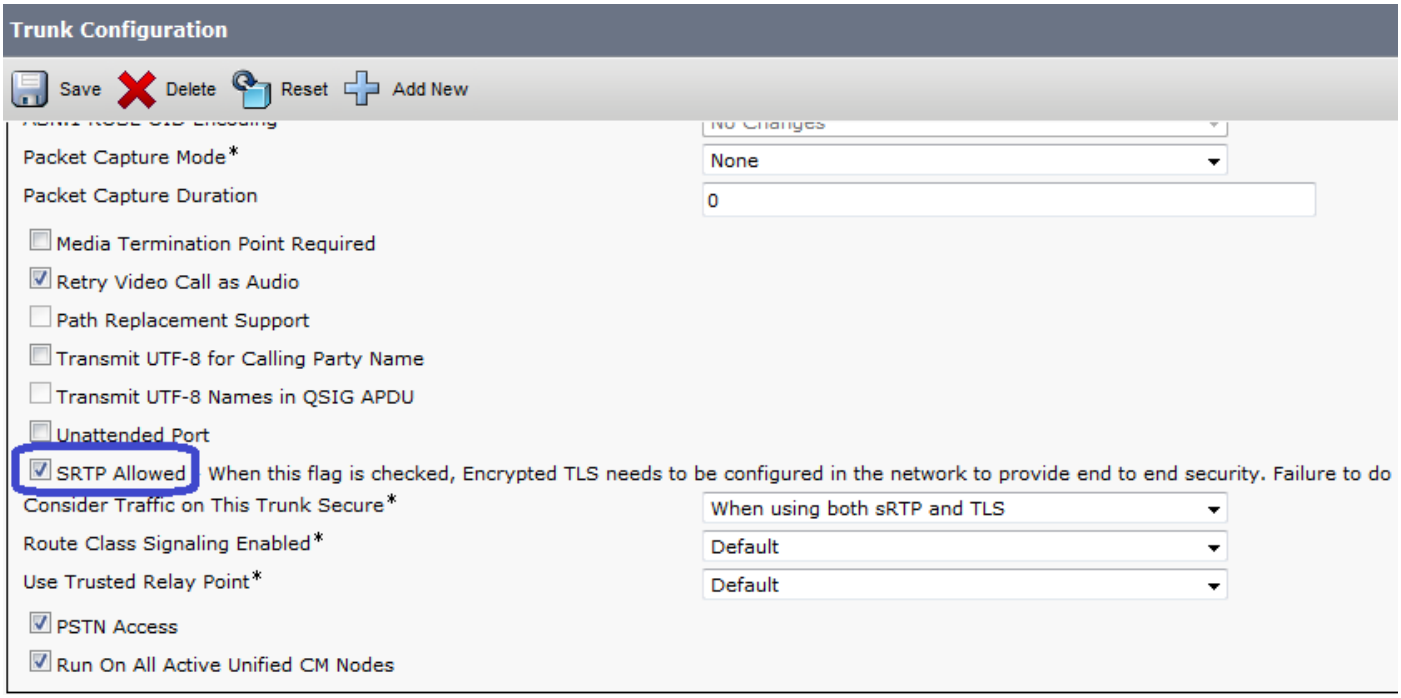
Шаг 1. На CM администрирование перешли к **Системному> Security> Профили безопасности магистрального SIP-канала> Файл.**

Шаг 2. Скопируйте существующий **Non Безопасный Профиль магистрали SIP** для создания нового безопасного профиля как показано в этом образе.

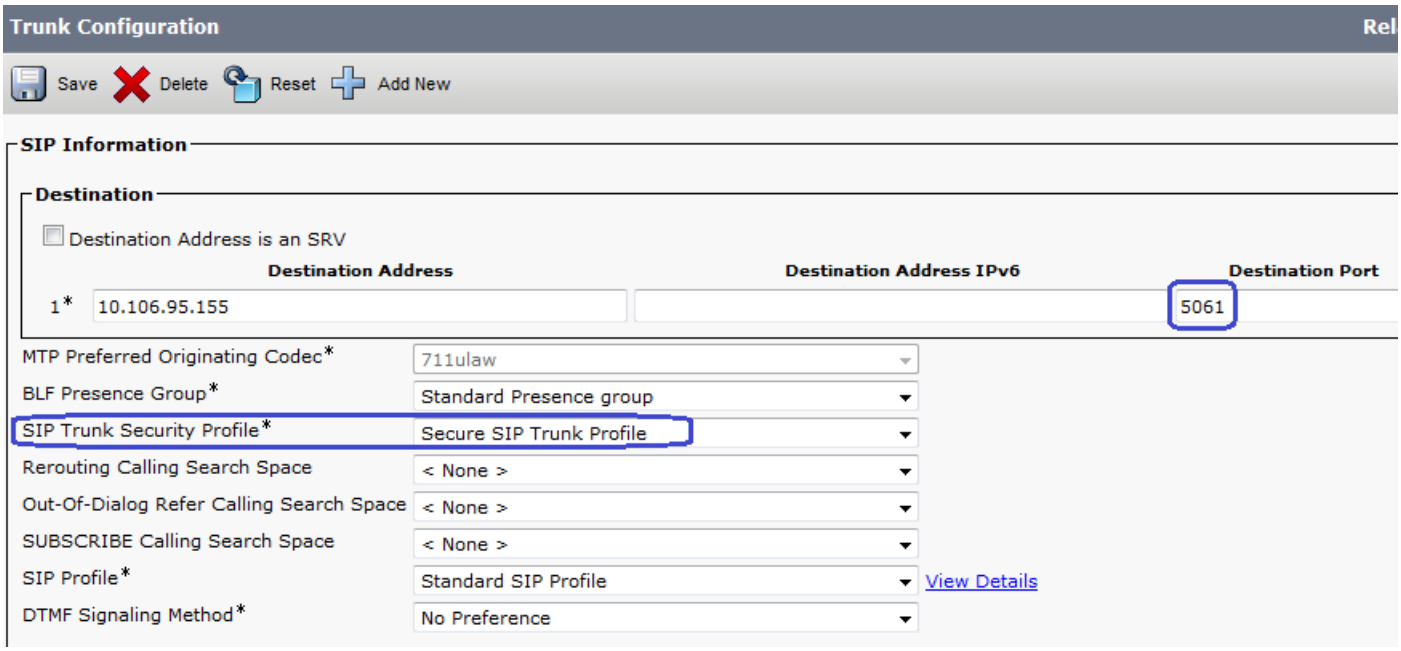


1. Создайте магистраль SIP к CUBE

Шаг 1. Включите SRTP на магистрали SIP как показано в этом образе.



Шаг 2. Настройте Порт назначения 5061 (TLS) и примените Новый Безопасный Профиль безопасности магистрального SIP-канала на магистраль SIP как показано в этом образе.



Проверка

```
Secure-CUBE#show sip-ua connections tcp tls detail
Total active connections : 2
No. of send failures : 0
No. of remote closures : 13
No. of conn. failures : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
** Tuples with no matching socket entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
to overcome this error condition
++ Tuples with mismatched address/port entry
- Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
to overcome this error condition

Remote-Agent:10.106.95.151, Connections-Count:2
Remote-Port Conn-Id Conn-State WriteQ-Size Local-Address
=========== ======= =========== =========== ===========
5061 16 Established 0 10.106.95.155
57396 17 Established 0 10.106.95.155


-------------- SIP Transport Layer Listen Sockets ---------------
Conn-Id Local-Address
=========== ============================
2 [10.106.95.155]:5061
```

Когда перекодировщик LTI используется, выходные данные краткого описания show call active voice перехвачены.

```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```

Также то, когда SRTP зашифровал вызов, сделано между Cisco IP Phone и CUBE или шлюзом, значок блокировки отображен на IP-телефоне.

Устранение неполадок

Эти отладки полезны для того, чтобы решить проблемы PKI/TLS/SIP/SRTP.


```
Secure-CUBE#show call active voice brief
Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 0
Multicast call-legs: 0
Total call-legs: 2
1283 : 33 357052840ms.1 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:3 Answer 3001 active
dur 00:00:08 tx:383/61280 rx:371/59360 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.106.95.132:17172 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00

1283 : 34 357052840ms.2 (23:57:23.929 IST Sun Feb 15 2015) +2270 pid:1 Originate 2001 active
dur 00:00:08 tx:371/60844 rx:383/62812 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.65.58.24:24584 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
```