

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[Конфигурация CUBE](#)

[Конфигурация CUCM](#)

[Проверка](#)

[Устранение неполадок](#)

[Связанные обсуждения Сообщества Cisco Support](#)

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.

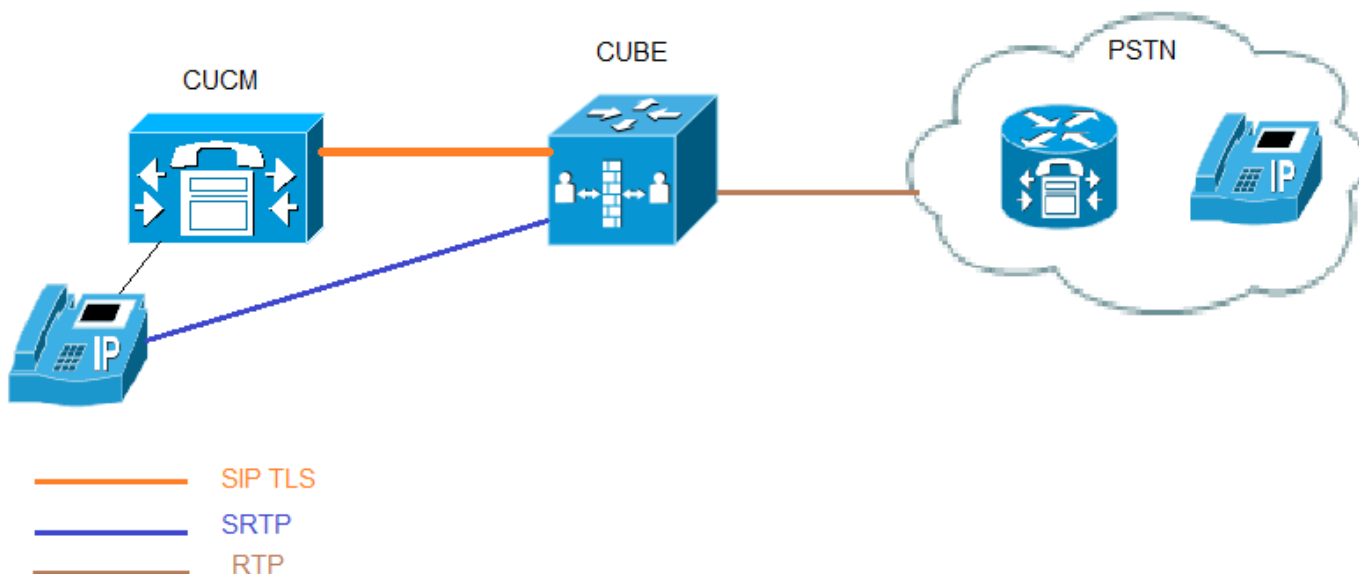
В эквивалентностях модели Взаимодействия открытых систем (OSI) TLS/SSL инициализируется на уровне 5 (уровень сеанса связи) и затем работает над уровнем 6 (уровень представления). И в моделях, TLS и в SSL работают от имени уровня базовой передачи, сегменты которого несут зашифрованные данные.

- 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 зашифрованный 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' command will 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.**

The screenshot shows the Cisco Unified Operating System Administration interface. The 'Certificate List' page displays a table of certificates. The first row, 'CallManager', is highlighted with a blue box. The table columns are: Certificate, Common Name, Type, Distribution, Issued By, and Expiration Date.

Certificate	Common Name	Type	Distribution	Issued By	Expiration Date
CallManager	cmpub	Self-signed	cmpub	cmpub	02/
CallManager-trust	Cisco_Root_CA_2048	Self-signed	Cisco_Root_CA_2048	Cisco_Root_CA_2048	05/
CallManager-trust	Cisco_Root_CA_M2	Self-signed	Cisco_Root_CA_M2	Cisco_Root_CA_M2	11/
CallManager-trust	cmsub	Self-signed	cmsub	cmsub	02/
CallManager-trust	CAP-RTP-001	Self-signed	CAP-RTP-001	CAP-RTP-001	02/
CallManager-trust	Cisco_Manufacturing_CA	CA-signed	Cisco_Manufacturing_CA	Cisco_Root_CA_2048	05/
CallManager-trust	CAPF-9a08b5fe	Self-signed	CAPF-9a08b5fe	CAPF-9a08b5fe	02/

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

The screenshot shows the 'Certificate Details for cmpub, CallManager' page. The 'Download .PEM File' button is highlighted with a blue box. The page displays the certificate's status, settings, and file data.

Status: Ready

Certificate Settings:

- File Name: CallManager.pem
- Certificate Purpose: CallManager
- Certificate Type: certs
- Certificate Group: product-cm
- Description(friendly name): Self-signed certificate generated by system

Certificate File Data:

```
[
Version: V3
Serial Number: 6AA0AECEC947BDCAFCC722310EE83224
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Validity From: Sat Feb 07 22:39:22 IST 2015
To: Thu Feb 06 22:39:21 IST 2020
Subject Name: L=bangalore, ST=karnataka, CN=cmpub, OU=tac, O=cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100d2191a26d52904ae14c3b6eb1a27607d5ca4d85251037db19141e76906d2cfcf5dca3
097fff569b7c19b9705de7624ca441617d49e08ee21a5d5cb8f3583a1f6089278b971833b6132dd4c77e
5e81866f2f4386bc16252658e5b0c37cb844df8a53a7dc034dff225fe7127b0fba88ab96617d01c3026f1
04eea12492a8572250203010001
Extensions: 3 present
]
```

Шаг 4. Вставьте файл сертификата в CUBE и выполните команду с СЕРТИФИКАТА BEGIN для ОКОНЧАНИЯ СЕРТИФИКАТА.

-----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
MQswCQYDVQQGEWJtjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxXjEjAQBgNVBAGTCWthcm5hdGFrYTESMBAGA1UEBxMjYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEWNoYXN0YXN0YXN0YXN0YXN0YXN0
MRIWEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBAcTCWJhbmdbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFcIUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAWUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/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
MQswCQYDVQQGEWJtjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTA3RhYzEOMAwG
A1UEAxMFY2l2dWIxXjEjAQBgNVBAGTCWthcm5hdGFrYTESMBAGA1UEBxMjYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyMl0XDTIwMDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAoTBWNpc2NvMQwwCgYDVQQLEWNoYXN0YXN0YXN0YXN0YXN0YXN0
MRIWEAYDVQQQIEwlrYXJlYXRha2ExEjAQBGNVBAcTCWJhbmdbG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEA0hkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbSz89dyjCX//Vpt8GblwXediTKRBYX1J4I7iG11cuPNYOh9giSeLlxgzthMt1M
d+XoGGby9DhrwWJSZY5b8MN8uETfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFcIUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAgYIKwYBBQUHAWUwHQYDVR0OBBYEFDGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIb3DQEBBQUAA4GBACb9gC0u/piCQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsA7Nk6QmpP5zXKJJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1Zfv
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkXO8/Ar
```

```
MRiWEAYDVQqIEwlrYXJuYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKcGyEAOhkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uEtfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQqgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFdGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/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 SSCP 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-----

```
MIICojCCAgugAwIBAgIQaaCuzslHvcr8xyIxDuGyJDANBgkqhkiG9w0BAQUFADEj
MQswCQYDVQQGEwJtjEOMAwGA1UEChMFY2l2Y28xDDAKBgNVBAsTAR3RhYzEOMAwG
A1UEAxMFY2l2dWIxExEjAQBGNVBAGTCWthcm5hdGFrYTESMBAGA1UEBxMJYmFuZ2Fs
b3JlMB4XDTE1MDIwNzE3MDkyM1oXDTE1MDIwNjE3MDkyMVowYzELMAkGA1UEBhMC
SU4xDjAMBGNVBAOTBWNpc2NvMQwwCgYDVQQLLEwN0YWMxDjAMBGNVBAMTBWntcHVi
MRiWEAYDVQqIEwlrYXJuYXRha2ExEjAQBGNVBACTCWJhbmhG9yZTCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwGyKcGyEAOhkaJtUpBK4Uw7brGidgfVyk2FJRA32xkUhn
aQbS89dyjCX//Vpt8GblwXeditKRBYX1J4I7iG11cuPNYOh9giSeLlxgzhMt1M
d+XoGGby9DhrwWJSZY5b8MN8uEtfilOn3ANN/yJf5xJ7D7qIq5ZhfQHDAm8QTuoS
SSqFciUCAwEAAANXMFUwCwYDVR0PBAQDAgK8MCcGA1UdJQqgMB4GCCsGAQUFBwMB
BggrBgEFBQcDAGYIKwYBBQUHAWUwHQYDVR0OBBYEFdGq0WCT/OnqwePSnhaknzR0
BconMA0GCSqGSIB3DQEBBQUAA4GBACb9gC0u/picQrv7BeLk2/qFmZ1/zVuXPDOn
wqz4yBMsa7Nk6QmpP5zXKJfXb3iKJPsmRWuUNEe+Df+sx0rUit3oGcF4ce/1ZfV
RKvt461TvA5r9HGxO+KaI8v7BaWeeROBfTboRpkvqRjFt6eIHEtn7+uUicumDASp
SkX08/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
LWNhMB4XDTE1MDIxMTEyNTYyMVowXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAtN3gRiUQ409jECyo
xVZzrpBRqj/HOqkVu3iRYp2C2PGRr01vbZvb6IZIh+m4K0Du7gBASUFDAOeidJIF
TCI3+MjUN3grnv1MH321J5tVzAPHj9z7GdD42+gZSoHqOMlFB8z4+VDPzpxpswI
3TFQHCFNbadF16P5VEFWv+0tHD8CAwEAAAnjMGEwDwYDVR0TAAQH/BAUwAwEB/zAO
BgNVHQ8BAf8EBAMCAyYwHwYDVR0jBBgwFoAUnqzvazK/7qXzhkoTiAEFCvsN8rww
HQYDVR0OBBYEFJ6s72syv+6l84ZKE4gBBQr7DfK8MA0GCSqGSIb3DQEBAUAA4GB
AEfnNrB4nls81vz0cqlpuTjID+KVyKRwYNP04zJYWCv7P+mlbpMfC/gh14z5/RzL
e5Bq6NUnxWByLR4gcFjmds1E6NqoNX9S5ryS3xQRkXr0MiXnVngSKELUn22JUw/q
CEnHng0AvcTRv/EBB2XlzYUxG0keiT8K+jv/g7+rmkF5
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIB7TCCAvaGAWIBAgIBAJANBgkqhkiG9w0BAQUFADASMRawDgYDVQQDEwdjdwJl
LWNhMB4XDTE1MDIxMTEzMDI1MFoXDTE4MDIxMDEyNTYyMVowFjEUMBIGA1UEAxML
U2VjdXJlLUNVQkUwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5C2JnKwtfO
F9bBVYhVwQK8y2c5NMkJKY//pisg+oforvxa1PKAXj/jqDkqtDTc3NAMf2A1rk25
f50aaBrNJmq4rfJB1wLyD2a/CzybJg+QB5sVCCHTkw5jf9+YGIMVsiVbrf4m+Lqi
OkZ5qxsMa5fEc/fejUsAE8yn4/mmgld/AgMBAAGjTzBNMAsGA1UdDwQEAwIFoDAf
BgNVHSMEGDAWgBSerO9rMr/upfOGShOIAQUK+w3yvDAdBgNVHQ4EFgQUsvUGSpaH
+XIOwVf50imcCHV8HjAwDQYJKoZIhvcNAQEFBQADgYEAYmRHLHxTgIogZYPScPmj
h69GLxXaOThH0sEbm/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.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* **CallManager-trust**

Description(friendly name)

Upload File **Browse...** Secure-CUBE.pem

Upload Close

i *- indicates required item.

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 магистралы SIP** для создания нового безопасного профиля как показано в этом образе.

SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

SIP Trunk Security Profile Information

Name*	Secure SIP Trunk Profile
Description	Secure SIP Trunk Profile authenticated by null String
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	Secure-CUBE
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

1. Создайте магистраль SIP к CUBE

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

Trunk Configuration

Save Delete Reset Add New

Packet Capture Mode* None

Packet Capture Duration 0

- Media Termination Point Required
- Retry Video Call as Audio
- Path Replacement Support
- Transmit UTF-8 for Calling Party Name
- Transmit UTF-8 Names in QSIG APDU
- Unattended Port
- SRTP Allowed When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do Consider Traffic on This Trunk Secure* When using both sRTP and TLS
- Route Class Signaling Enabled* Default
- Use Trusted Relay Point* Default
- PSTN Access
- Run On All Active Unified CM Nodes

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

Trunk Configuration Rel

Save **X** Delete Reset Add New

SIP Information

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.106.95.155		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile [View Details](#)

DTMF Signaling Method* No Preference

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
```