在多维数据集的SIP TLS和SRTP-RTP互联网络使用IOS CA

目录

简介

本文描述基础会话初始化协议(SIP)传输层安全(TLS)和安全实时传输协议(SRTP)在Cisco Unified Border Element (多维数据集)与配置示例。

在多维数据集的安全语音通信可以分开成两部分：

- 安全信令–多维数据集使用TLS在SIP和Internet协议安全性(IPSec)获取发信号为了获取发信号的在H.323
- 安全梅迪亚– SRTP

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Unified Communications Manager (CUCM)证书信任列表(CTL)文件为Mixed-mode创建
- IP电话在安全模式(加密)注册
- 多维数据集基本语音服务voip和拨号对等配置被执行

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM 10.5
- 多维数据集–与IOS 15.3(3)M3的3925E
- Cisco IP Communicator (CIPC)

背景信息

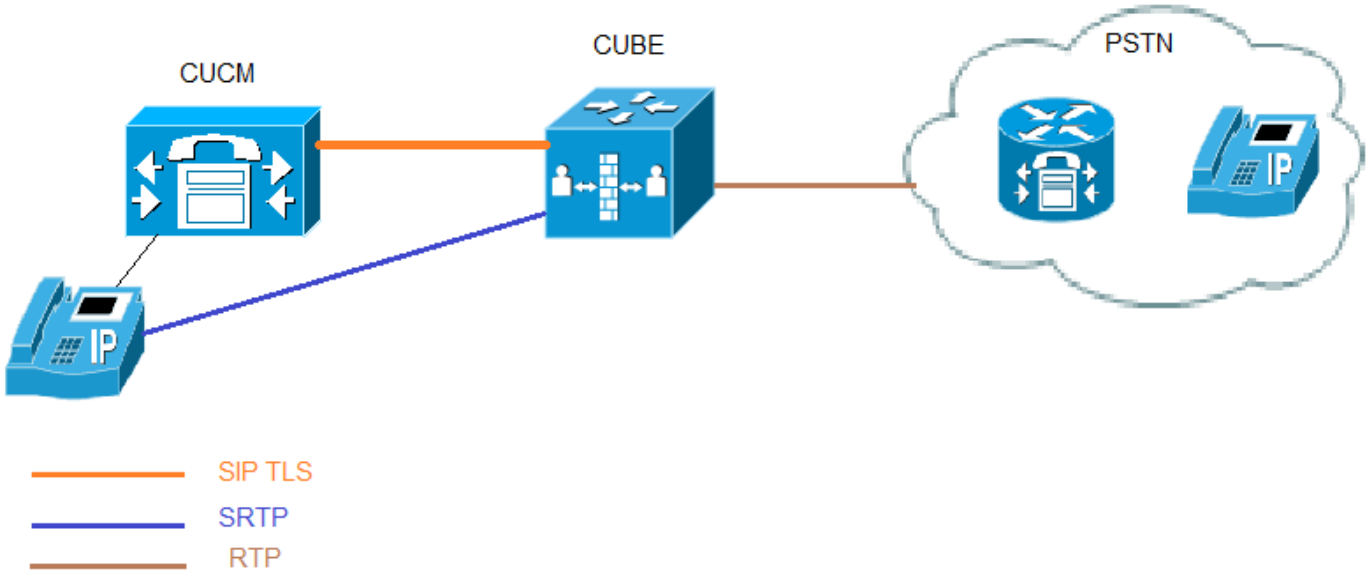
- TLS - TLS和其前身，安全套接字协议层(SSL)，是提供在互联网的通信安全性的加密协议。
  在开放式系统互联(OSI)型号当量， TLS/SSL初始化在第五层(会话层)然后工作在第六层(表示层)。在两个型号中， TLS和SSL代表基础传输层工作，分段传送已加密数据。

- Certificate Authority (CA) -发行证书的可信的实体：思科或一个第三方实体。
- 设备验证-处理验证设备标识并且保证实体是什么声称是，在联系被建立前。
- 加密-翻译数据进程到保证信息的机密性的密文里。只有预定接收方能读数据。它要求加密算法和加密密钥。
- 公共/Private密钥-在加密使用的密钥。公共密钥广泛可用的，但是专用密钥由他们的各自的所有者保持。不对称加密结合两个类型。

配置

网络图

在此镜像，设置的SIP TLS和SRTP配置示例在CUCM/IP电话和多维数据集之间显示。 在SRTP和实时传输协议(RTP)之间的多维数据集互联网络。多维数据集作为IOS CA和CUCM将使用自签名证书。



多维数据集配置

1. 配置时钟和enable (event) HTTP服务器
同步在CA服务器和客户端信任点(CUBE/OGW/TGW)的时钟。否则，有与CA服务器发出的证书的正确性的问题。

```
Secure-CUBE#clock set <hh:mm:ss> < Day of the month> <MONTH> <Year>
Or
Ntp server <IP Address>
```

客户端信任点使用HTTP接收从CA的证书。

```
Secure-CUBE(config)#ip http server
```

2. 生成RSA密钥对

此步骤生成私有和公共密钥。

在本例中，多维数据集是标签。它可以是任何。

```
Secure-CUBE(config)#crypto key generate rsa general-keys label CUBE modulus 1024
The name for the keys will be: CUBE
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
Secure-CUBE(config)#
```

3. 配置IOS CA服务器

在本例中， CA服务器被命名多维数据集CA。

```
crypto pki server cube-ca
database level complete
no database archive
grant auto
lifetime certificate 1800

Secure-CUBE(cs-server)#no shut
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit

Password:

Re-enter password:

% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

% Certificate Server enabled.

Secure-CUBE(cs-server)#
```

4. 创建多维数据集的PKI信任点TLS通信的。

在本例中，信任点名称对于多维数据集是CUBE-TLS。用于登记URL的IP地址必须是在多维数据集的本地接口。用于此步骤的主题名称在CUCM SIP中继安全配置文件的X.509主题名称必须配比。(如果域名启用)，最佳实践是使用主机名以域名。

关联在步骤创建的RSA密钥对2。

```
crypto pki trustpoint CUBE-TLS
enrollment url http://X.X.X.X:80
serial-number none
fqdn none
ip-address none
subject-name CN=Secure-CUBE
revocation-check none
rsakeypair CUBE
```

5.验证信任点用CA服务器并且接受CA证书。

```
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)#
```

6. 登记信任点用CA服务器。

在此步骤多维数据集接收从CA的一签名证书。

```
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)#
```

7. 创建CUCM的信任点。

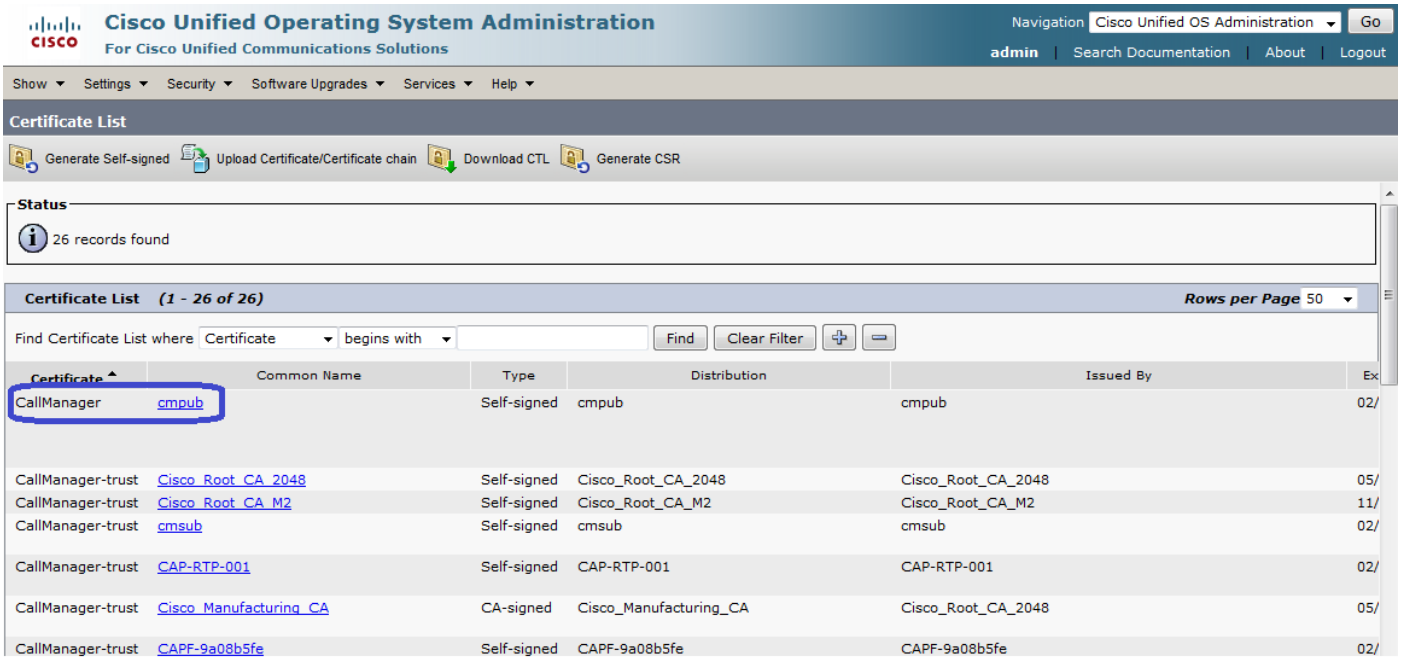
如果Callmanager组有多个CM服务器，则信任点需要为所有服务器创建，否则故障切换没有运作。

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

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

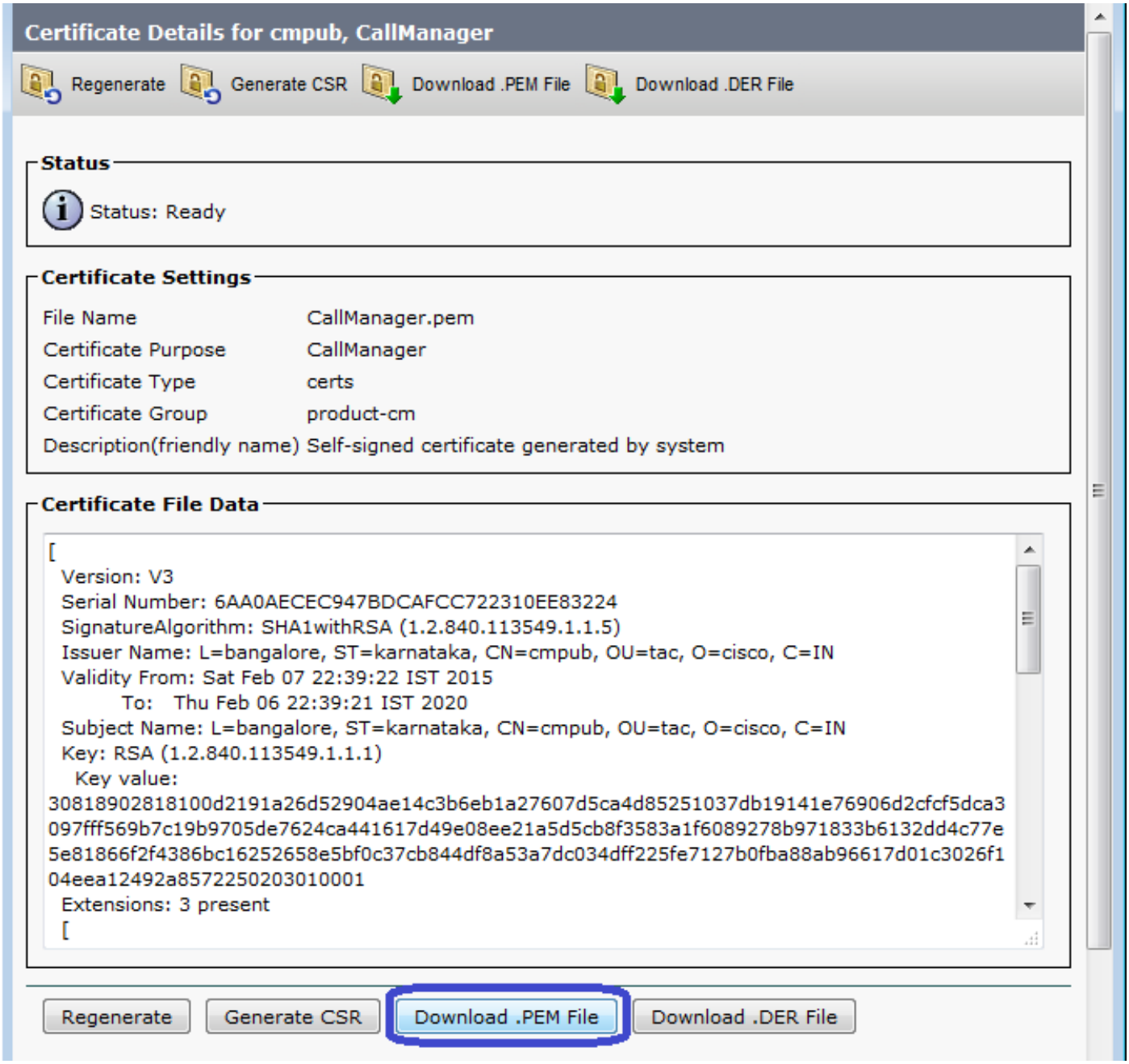
8. 登记CUCM证书求立方。

步骤1. CUCM OS的admin洛金。

步骤2.导航对**> Certificate Management >**



步骤3.如此镜像所显示，点击**CallManager**证书，然后下载并且保存.PEM文件。



步骤4.打开在记事本的文件并且复制内容从END

步骤5.粘贴在多维数据集的此证书如显示。

```
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)#
```

第六步：遵从其他CUCM服务器的同样步骤。

9. 配置TCP TLS作为传输协议。
这可以执行在全局或在dial-peer级别。

```
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)#
```

10. 为SIP UA分配信任点，此信任点使用在多维数据集和CUCM之间的所有SIP信令

```
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)#
```

或者默认信任点可以为从多维数据集的所有SIP信令配置。

```
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)#
```

11. Enable (event) 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)#
```

12. 对于SRTP和RTP互联网络，请巩固代码转换器要求。
如果IOS版本然后15.2.2T (多维数据集9.0)或以后， LTI代码转换器可以是配置最小化配置。

LTI代码转换器不需要SRTP-RTP呼叫的Pki trustpoint配置

```
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)#
```

如果IOS在15.2.2T之下，则请配置SCCP代码转换器。

内部呼叫控制协议(SCCP)代码转换器将需要发信号的信任点然而，如果同一路由器用于主机代码转换器同样信任点(CUBE-TLS)可以然后用于多维数据集以及代码转换器。

```
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)#
```

CUCM配置

1. 出口多维数据集对CUCM的IOS证书。

步骤1.出口IOS证书。复制自已签署的CA证书并且保存作为例如.PEM文件，安全CUBE.pem

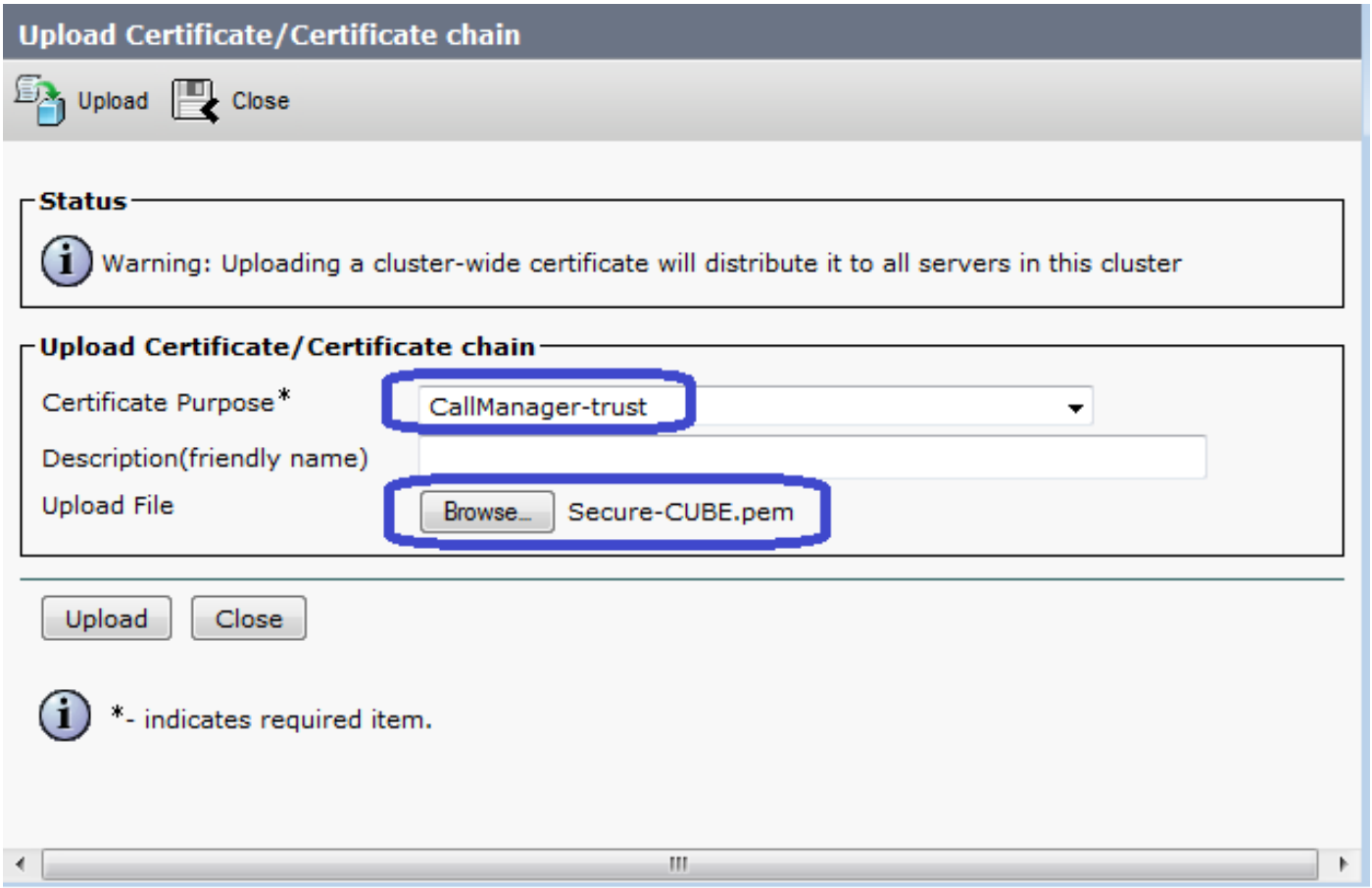
```
 Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVoXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
Y3ViZS1jYTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAtN3gRiUQ409jECyo
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)#
```

步骤2.加载在CUCM的IOS CA证书作为CallManager托拉斯。

步骤3.导航到**CM OS> Security > Certificate Management >/**

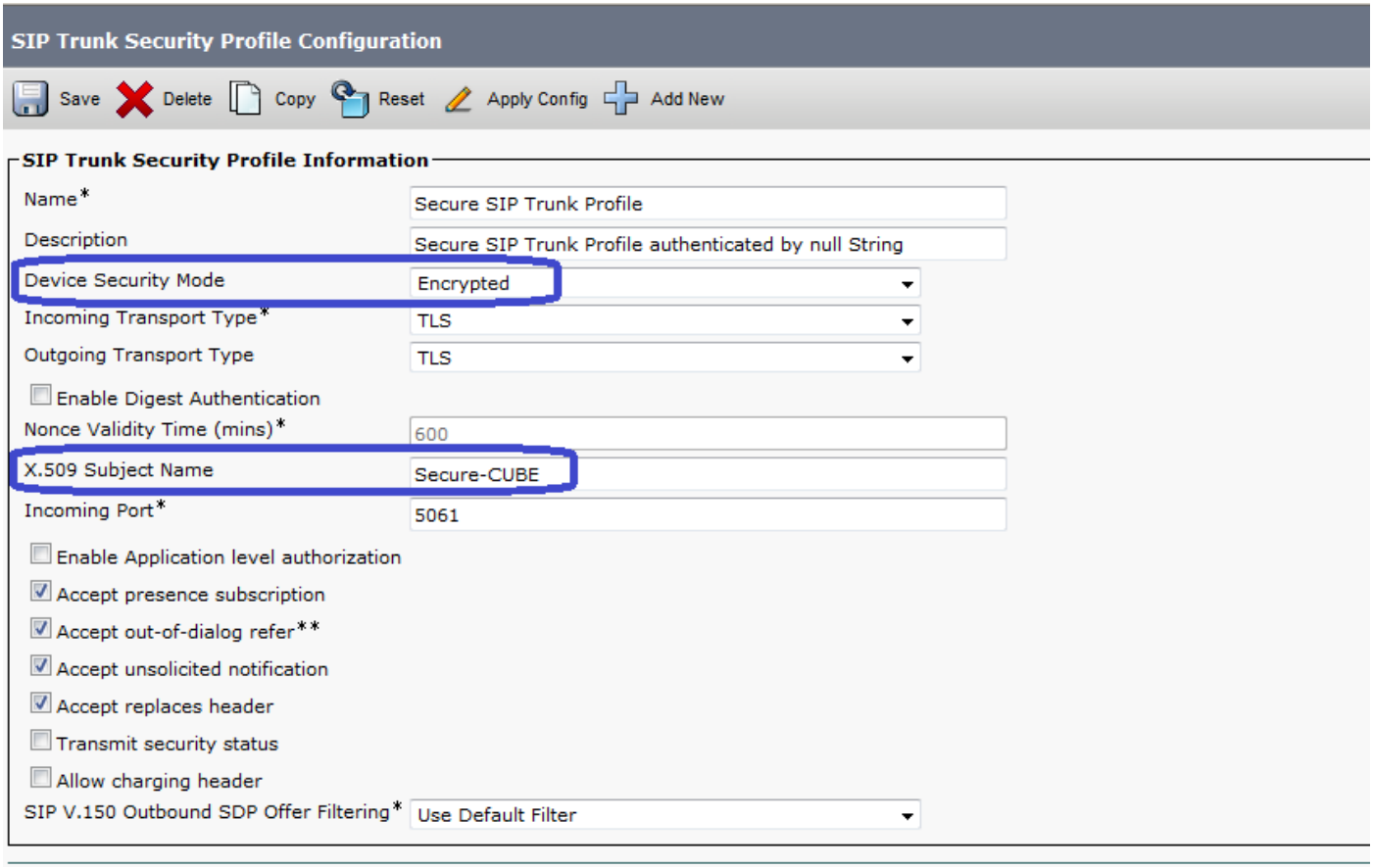
步骤4.加载如此镜像所显示的.PEM文件。



2. 创建新的SIP中继安全配置文件

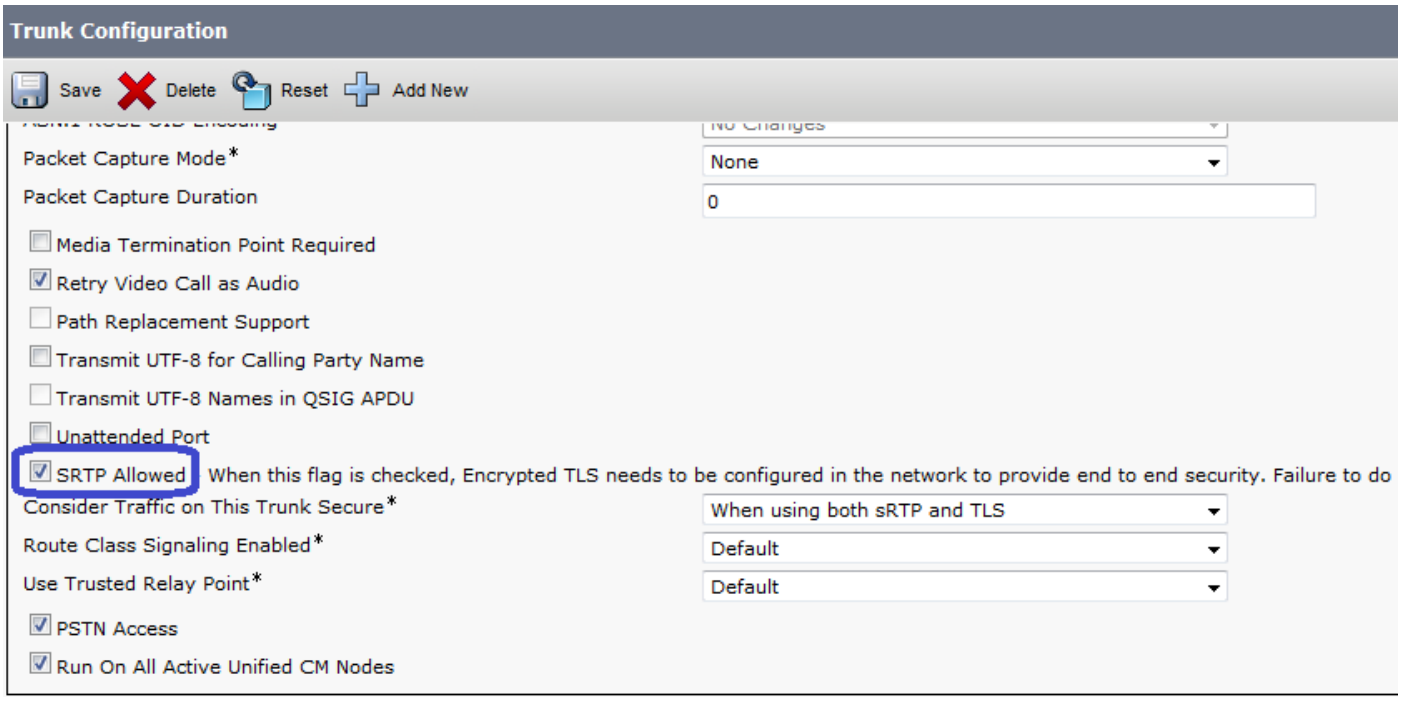
步骤1:在CM管理请导航到**> Security > SIP>**

步骤2.如此镜像所显示，复制存在**非安全SIP中继配置文件**为了创建新建的安全配置文件。

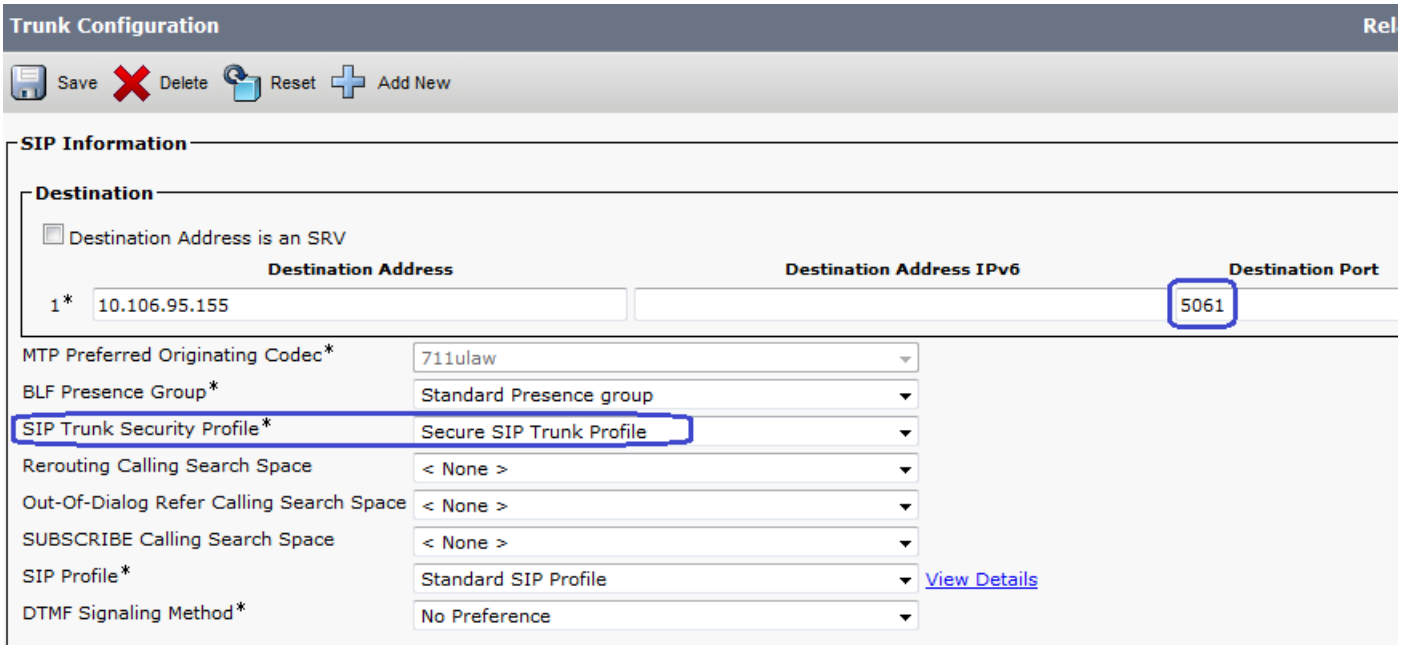


3. 创建SIP中继对多维数据集

步骤1.在SIP中继的Enable (event) SRTP如此镜像所显示。



步骤2.配置目的地端口5061 (TLS)如此镜像所显示，并且应用在SIP中继的新的安全SIP中继安全配置文件。



验证

```
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
```

当使用时， show call active voice brief输出捕获LTI代码转换器。

```
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
```

并且，当SRTP加密的呼叫被做在Cisco IP电话之间和多维数据集或者网关时，锁图标在IP电话显示。

故障排除

这些调试为排除故障PKI/TLS/SIP/SRTP问题是有用。

```
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
```