SORVA o funcionamento entre redes TLS e SRTP-RTP no CUBO usando IO CA

Índice

Introdução

Este documento descreve os princípios do Transport Layer Security do Session Initiation Protocol (SIP) (TLS) e do protocolo de transporte em tempo real seguro (SRTP) sobre o Cisco Unified Border Element (CUBO) com um exemplo de configuração.

Uma comunicação de voz segura sobre o CUBO pode ser dividida em duas porções:

- Fixe a sinalização – O CUBO usa o TLS para fixar a sinalização sobre o SORVO e a segurança de protocolo do Internet (IPsec) a fim fixar a sinalização sobre H.323
- Fixe media – SRTP

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Os arquivos do certificate trust list do gerente das comunicações unificadas de Cisco (CUCM) (CTL) são criados para o Misturado-MODE
- Os Telefones IP são registrados no modo seguro (a criptografia)
- O voip e a configuração de dial peer básicos do serviço de voz do CUBO são feitos

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM 10.5
- CUBO – 3925E com IO 15.3(3)M3
- Cisco IP Communicator (CIPC)

Informações de Apoio

- TLS - O TLS e seu antecessor, o secure sockets layer (SSL), são os protocolos criptograficamente que fornecem a Segurança de comunicação sobre o Internet.

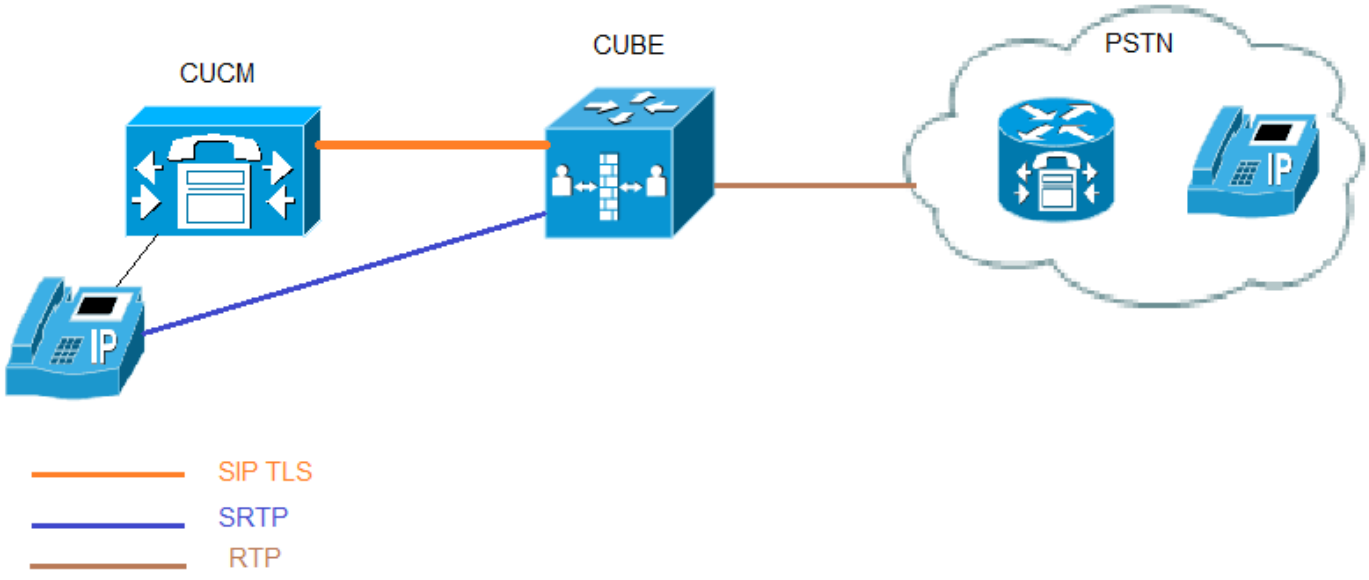
Em equivalências do modelo do Open Systems Interconnection (OSI), TLS/SSL é inicializado na camada 5 (a camada de sessão) e trabalha então na camada 6 (a camada de apresentação). Em ambos os modelos, o TLS e o SSL trabalham em nome da camada de transporte subjacente, cujos os segmentos levam dados criptografados.

- Certificate Authority (CA) - Entidade confiável essa Certificados das edições: Cisco ou uma entidade da terceira.
- Processo de autenticação do dispositivo que valida a identidade do dispositivo e se assegura de que a entidade seja o que reivindica ser antes que uma conexão estiver feita.
- Criptografia - Processo de traduzir dados no texto cifrado que assegura a confidencialidade da informação. Somente os receptores intencionados podem ler os dados. Exige um algoritmo de criptografia e uma chave de criptografia.
- Público/chaves privadas - Chaves que são usadas na criptografia. As chaves públicas são amplamente disponíveis, mas as chaves privadas são mantidas por seus proprietários respectivos. A criptografia assimétrica combina ambos os tipos.

Configurar

Diagrama de Rede

Nesta imagem, o exemplo de configuração para estabelecer o SORVO TLS e SRTP entre o telefone CUCM/IP e o CUBO é mostrado. Inter-redes do CUBO entre o SRTP e o Real-Time Transport Protocol (RTP). O CUBO atua como IO CA e CUCM usaria certificados auto-assinados.



Configuração do CUBO

1. Configurar o pulso de disparo e permita o Server do HTTP

Sincronize os pulsos de disparo no server de CA e nos pontos confiáveis do cliente (CUBE/OGW/TGW). Se não, há umas edições com a validez dos Certificados emitidos pelo server de CA.

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

Os pontos confiáveis do cliente usam o HTTP para receber o certificado de CA.

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

2. Gerencia um par de chave RSA

Esta etapa gerencie privado e chaves públicas.

Neste exemplo, o CUBO é apenas uma etiqueta. Pode ser qualquer coisa.

```
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. Configurar o server IO CA

Neste exemplo, o server de CA é nomeado cubo-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. Crie pontos confiáveis PKI para o cubo para uma comunicação TLS.

Neste exemplo, o nome do ponto confiável para o CUBO é CUBE-TLS. O endereço IP de Um ou Mais Servidores Cisco ICM NT usado no registro URL deve ser interface local no CUBO. O nome do sujeito usado nesta etapa deve combinar no nome do sujeito X.509 no perfil de segurança do tronco do SORVO CUCM. O melhor prática é usar o hostname com Domain Name (se o Domain Name é permitido).

Par de chaves do associado RSA criado em etapa 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. Autentique o ponto confiável com server de CA e aceite o certificado de 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)#
```

6. Registre o ponto confiável com server de CA.

Nesta etapa o CUBO recebe um certificado assinado de 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)#
```

7. Crie o ponto confiável para o CUCM.

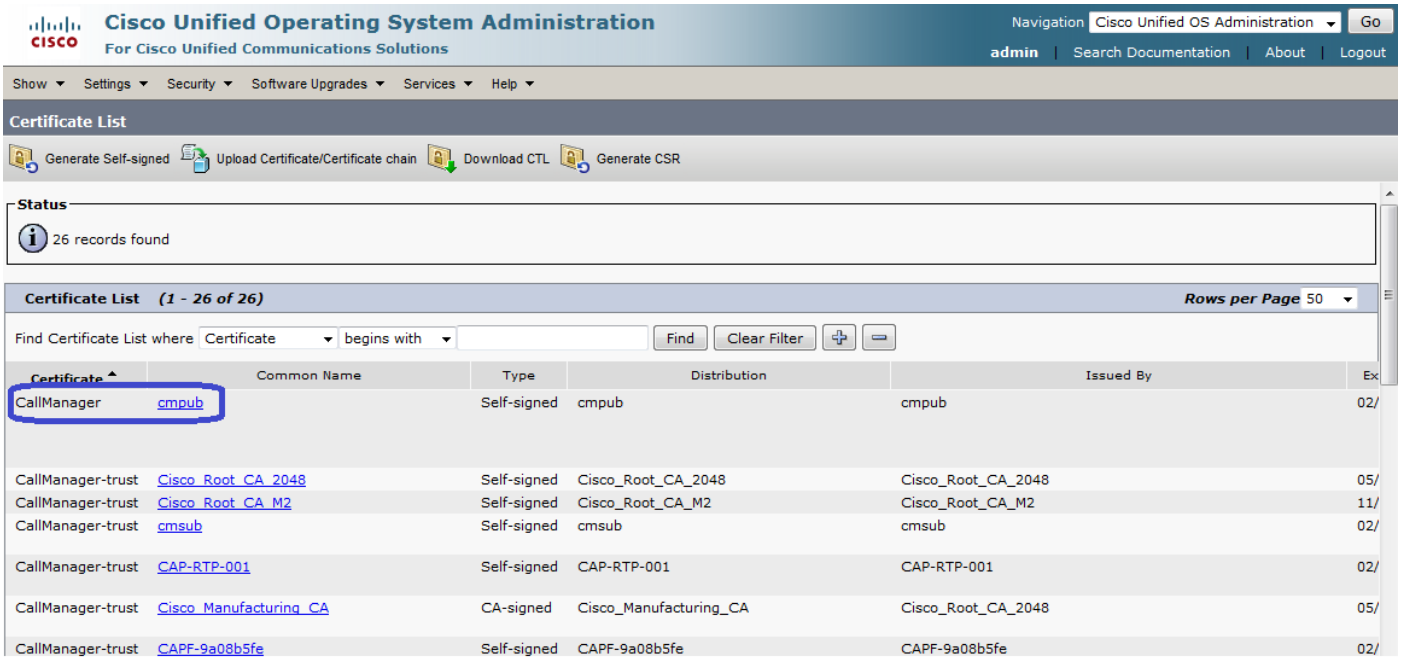
Se o grupo do CallManager tem servidores de CM múltiplos, a seguir o ponto confiável precisa de ser criado para todos os server, se não o Failover não trabalha.

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

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

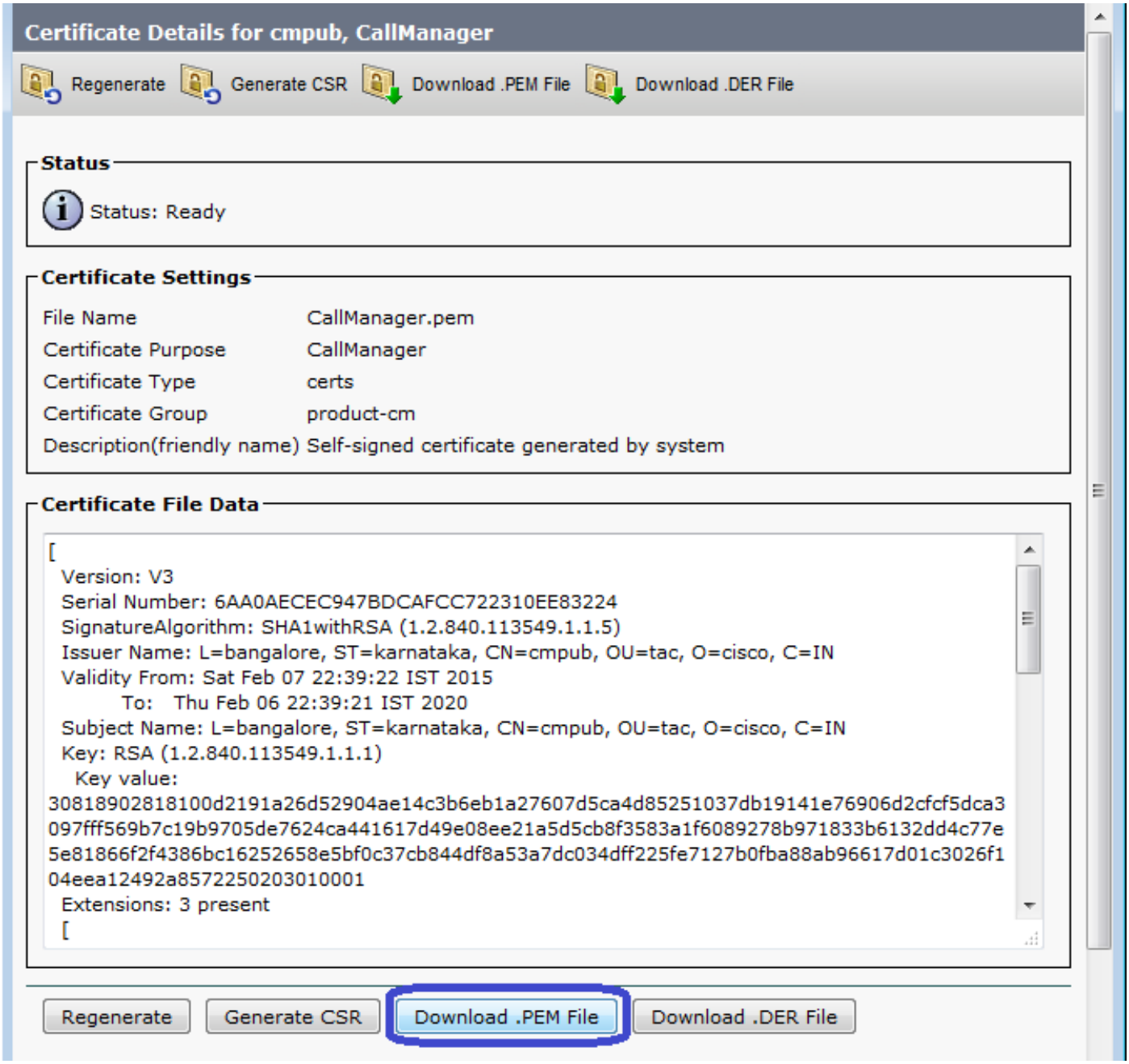
8. Registre o certificado CUCM PARA CUBAR.

Etapa 1. Início de uma sessão ao OS admin CUCM.

Etapa 2. Navegue ao **> gerenciamento de certificado > ao achado da Segurança.**



Etapa 3. Clique o certificado do **CallManager**, a seguir transfira e salvar o arquivo do .PEM segundo as indicações desta imagem.



Etapa 4. Abra o arquivo no bloco de notas e copie o índice do COMEÇAM O CERTIFICADO TERMINAR O CERTIFICADO .

Etapa 5. Cole este certificado no CUBO como mostrado.

```
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)#
```

Etapa 6. Siga o mesmo procedimento para os outros server CUCM.

9. Configurar TCP TLS como o protocolo de transporte.
Isto pode ser feito em um global ou em um dial-peer em nível.

```
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. Atribua o ponto confiável para o sorvo-UA, este ponto confiável é usado para toda a sinalização do SORVO entre o CUBO e o 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)#
```

ou o ponto confiável do padrão pode ser configurado para toda a sinalização do SORVO do CUBO.

```
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. Permita o 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. Para o funcionamento entre redes SRTP e RTP, fixe o transcodificador é exigido.

Se a Versão do IOS é 15.2.2T (CUBO 9.0) ou mais tarde então, transcodificador LTI pode ser configura para minimizar a configuração.

O transcodificador LTI não precisa a configuração do ponto confiável PKI para atendimentos SRTP-RTP

```
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)#
```

Se os IO estão abaixo de 15.2.2T, a seguir configurar o transcodificador do sccp.

O transcodificador do Skinny Call Control Protocol (SCCP) precisaria o ponto confiável para sinalizar contudo se o mesmo roteador está usado para hospedar o transcodificador então que o mesmo ponto confiável (CUBE-TLS) pode ser usado para o CUBO assim como o transcodificador.

```
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)#
```

Configuração CUCM

1. Certificado do CUBO IO da exportação a CUCM.

Etapa 1. Certificado da exportação IO. Copie o certificado de CA auto-assinado e salvar como o arquivo do .PEM por exemplo, Secure-CUBE.pem

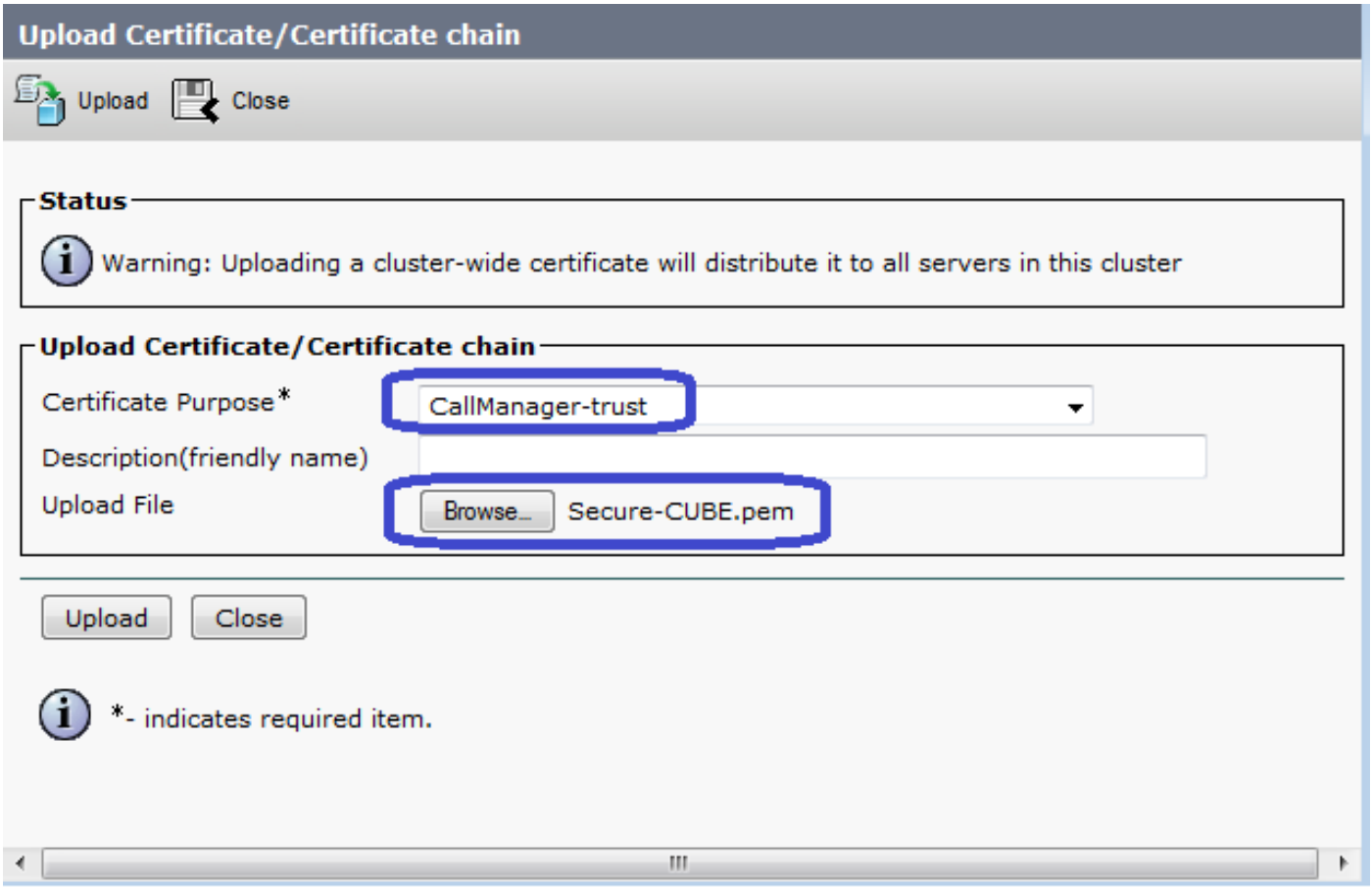
```
 Secure-CUBE(config)#crypto pki export CUBE-TLS pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB/TCCAWagAwIBAgIBATANBgkqhkiG9w0BAQQFADASMRAwDgYDVQQDEwdjdWJl
LWNhMB4XDTE1MDIxMTEyNTYyMVoXDTE4MDIxMDEyNTYyMVowEjEQMA4GA1UEAxMH
```

```
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)#
```

Etapa 2. Certificado de CA da transferência de arquivo pela rede IO em CUCM como a CallManager-confiança.

Etapa 3. Navegue ao **> gerenciamento de certificado do > segurança da administração do OS CM > ao certificado/certificate chain da transferência de arquivo pela rede**

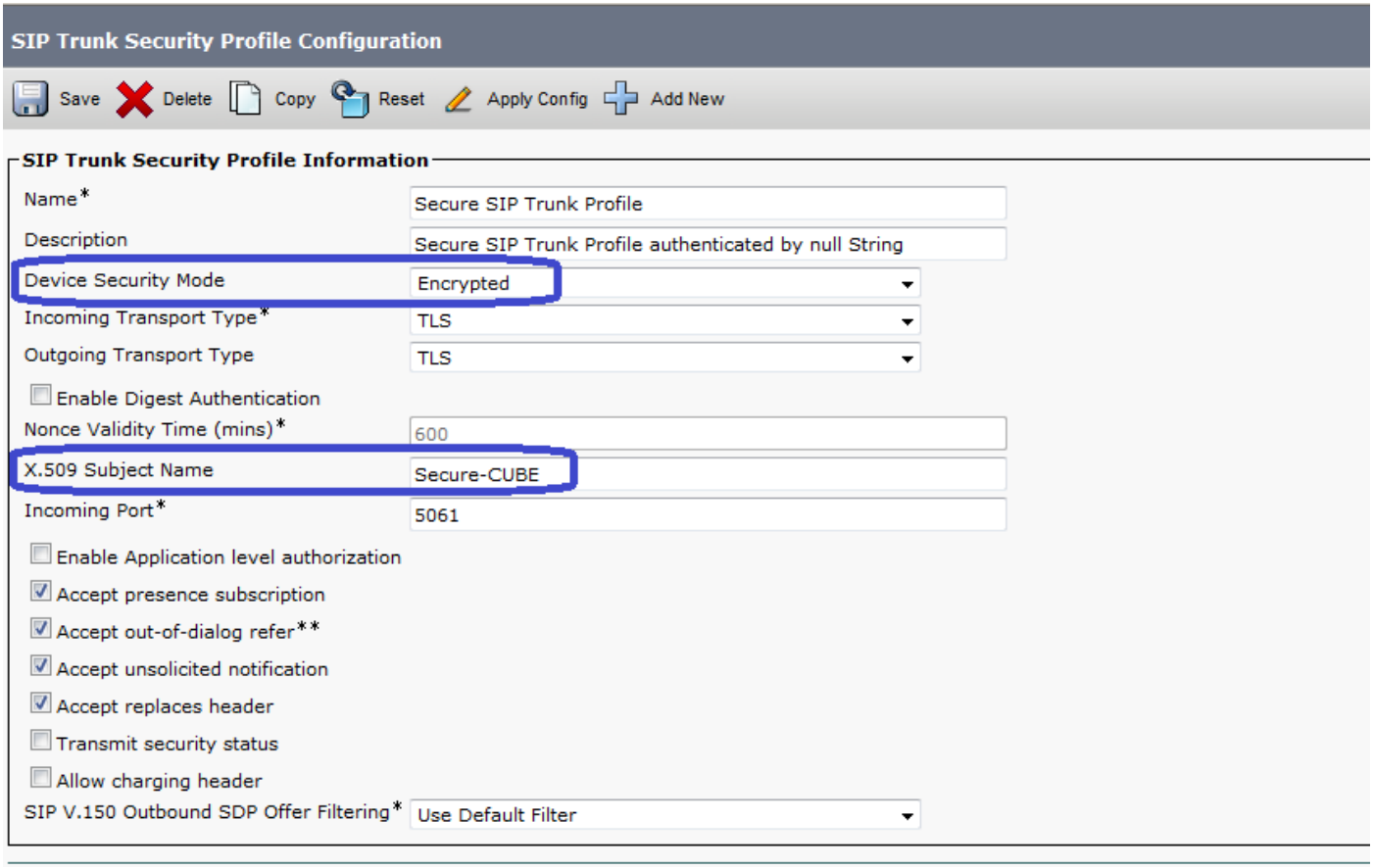
Etapa 4. Arquivo do .PEM da transferência de arquivo pela rede segundo as indicações desta imagem.



2. Crie o perfil de segurança novo do tronco do SORVO

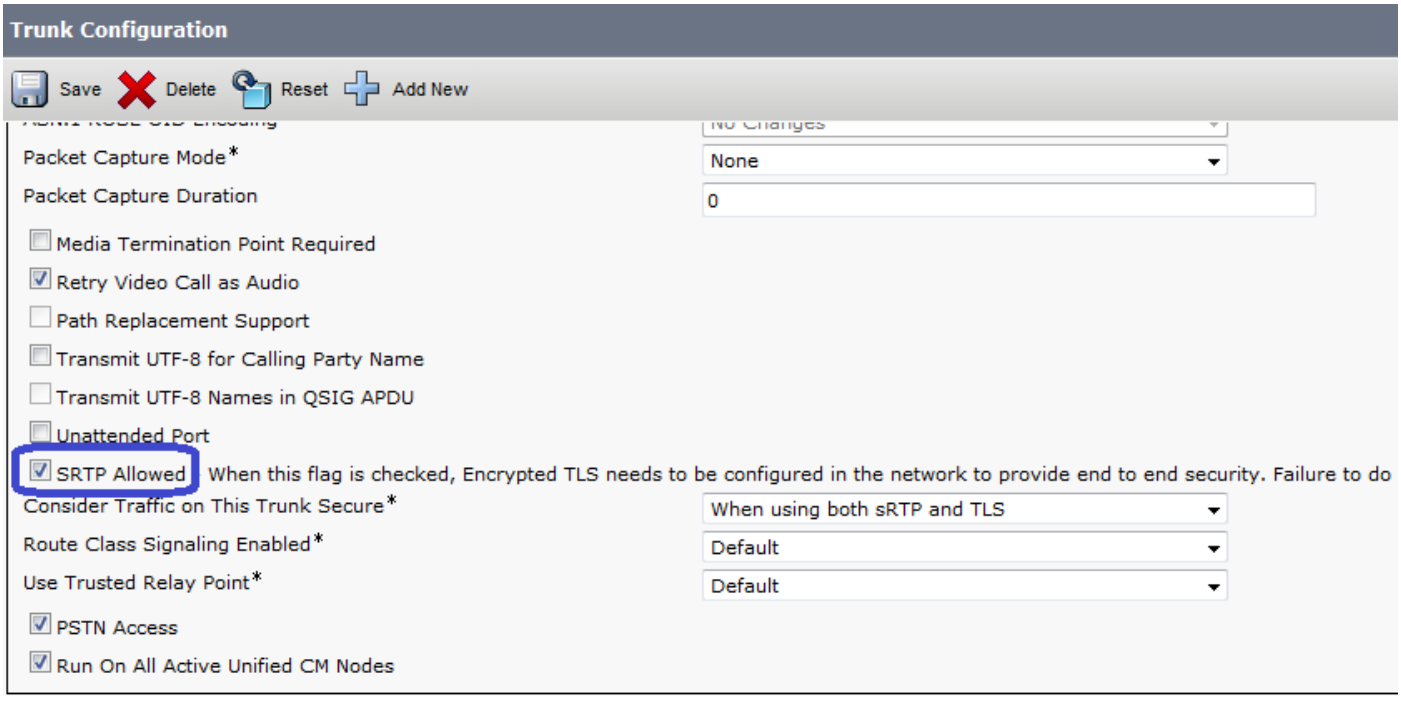
Etapa 1. Na administração CM navegue ao **> segurança do sistema > aos perfis de segurança > ao arquivo do tronco do SORVO.**

Etapa 2. Copie a existência **perfil não seguro do tronco do SORVO** a fim criar o perfil seguro novo segundo as indicações desta imagem.

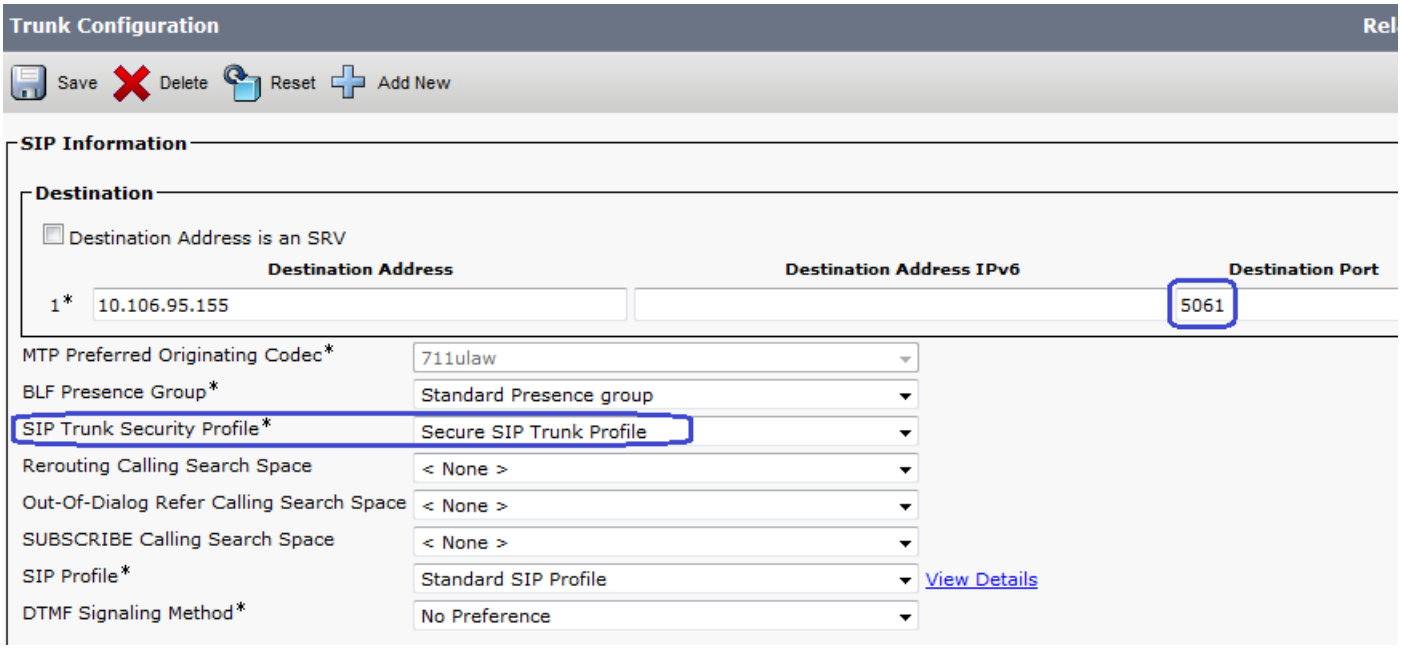


3. Crie o tronco do SORVO ao CUBO

Etapa 1. Permita o SRTP no tronco do SORVO segundo as indicações desta imagem.



Etapa 2. Configurar a porta do destino 5061 (TLS) e aplique novo fixam o perfil de segurança do tronco do SORVO no tronco do SORVO segundo as indicações desta imagem.



Verificar

```
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
```

A saída de é capturada show call ative voice brief quando o transcodificador LTI é usado.

```
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
```

Igualmente quando um atendimento cifrado SRTP é feito entre o Cisco IP Phone e o CUBO ou o gateway, um ícone do fechamento é indicado no telefone IP.

Troubleshooting

Estes debugam são úteis para pesquisar defeitos edições 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
```