Configurar recursos de segurança da Voz com CUBO e CUCM

Índice

Introdução

Este documento descreve como configurar a Segurança entre o Cisco Unified Border Element (CUBO) e o gerente das comunicações unificadas de Cisco (CUCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Gerente das comunicações unificadas de Cisco (CUCM)
- Cisco Unified Border Element (CUBO)
- Transport Layer Security (TLS)
- Fixe o protocolo de transporte em tempo real (o SRTP)
- Real-Time Transport Protocol (RTP)
- Session Initiation Protocol (SIP)
- Protocolo de datagrama de usuário (UDP)
- Provedor de serviços da telefonia pelo Internet (ITSP)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Informações de Apoio

Como configurar o TLS e o SRTP ao RTP no CUBO com CUCM

Antes desta configuração, o CUCM deve ser ajustado no modo da mistura com Segurança permite.

O CUBO atua como o Certificate Authority (CA) do sistema operacional inter-redes (IO), os Certificados CUCM é auto assinado.
Fluxo de chamadas do laboratório
Telefone CP-8945 > CUCM- (SIP/TLS) - CUBO > (SIP/UDP) - o resto do mundo simula ITSP (RTP) > telefone
O SRTP está entre o telefone CP-8945 e o CUBO
CP-8945 o número de telefone 2088, o comando show é baseado no atendimento do ITSP para 2088.

Configurar

Etapa 1. A fim configurar o pulso de disparo, **execute o comando clock set ou configurar o NTP**.

```
Set clock 8:00:00 01 JAN 2012
Or
Ntp server x.x.x.x
ntp source FastEthernet0/0

clock timezone AEST +10

Configure gateway to act as http server: "ip http server"
```

Etapa 2. Configurar o servidor PKI IO & os pontos confiáveis (o roteador local como CA)

```
crypto pki server iosca
 database level complete
 database url nvram:
 grant auto
 lifetime certificate 1800

crypto pki trustpoint iosca
  enrollment url http://10.66.75.246:80 (local Giga Ethernet ip address)
  revocation-check none
  rsakeypair iosca

Wait 30 seconds before issuing "no shutdown" on iosca server

crypto pki server iosca
 no shutdown

############################
MS-3945(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:Ciscotac123

Re-enter password:Ciscotac123
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

Jan  7 06:30:15.825: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate Server
signing certificate and keys...
```

```
% Certificate Server enabled.
Jan  7 06:30:25.384: %PKI-6-CS_ENABLED: Certificate server now enabled.
MS-3945(cs-server)#
############################
```

Etapa 3. Configurar pontos confiáveis (para o SORVO e fixe o transcodificador)

> Nota: Fixe o transcodificador registrado no CUBO é exigido para a rede interna SRTP e RTP.

> Nota: Fixe o transcodificador não é exigido para a plataforma do roteador dos serviços de Agregation (ASR), somente para o Roteadores dos Serviços integrados (ISR) G1,G2.

```
crypto pki trustpoint cube3945
 enrollment url http://10.66.75.246:80 (local Giga Ethernet 0/1)
serial-number none
 fqdn none
subject-name CN=MS-3945.eim.com (needs to match the X.509 subject name in CUCM's secure SIP
trunk profile)
 ip-address none
 revocation-check none

crypto pki authenticate cube3945

####################
MS-3945(config)#crypto pki authenticate cube3945
Certificate has the following attributes:
       Fingerprint MD5: 2F2D61A4 EACCC730 141B2966 7370A9AA
      Fingerprint SHA1: E6B86D4F C84B5453 8F63F019 773E1E0C 0DE5B883

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
MS-3945(config)#
####################

crypto pki enroll cube3945

###################
MS-3945(config)#crypto pki enr cube3945
%
% 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:Ciscotac123
Jan  7 06:31:06.884: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:Ciscotac123

% 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 cube3945' commandwill show the fingerprint.
Jan  7 06:31:24.088: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 9A128490 01A60E1D
9F3C3253 48706E5F
Jan  7 06:31:24.088: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: 733EE8B1 DBB0F25C
595D48E3 0830047C 50DEFB16
MS-3945(config)#
Jan  7 06:31:29.156: %PKI-6-CERTRET: Certificate received from Certificate Authority
#################
```

```
crypto pki trustpoint secdsp
 enrollment url http://10.66.75.246:80
 serial-number
 revocation-check none
 rsakeypair iosca

crypto pki authenticate secdsp (same procedure as other trustpoints)
 crypto pki enroll secdsp (same procedure as other trustpoints)



sccp local GigabitEthernet0/1
sccp ccm 10.66.75.246 identifier 10 version 7.0
sccp
!

!
sccp ccm group 20
 associate ccm 10 priority 1
 associate profile 20 register XCODER_IOS


!
dspfarm profile 20 transcode universal security
 trustpoint secdsp
 codec g711ulaw
 codec g711alaw
 codec g729ar8
 codec g729abr8
 maximum sessions 10
 associate application SCCP
!
telephony-service
 secure-signaling trustpoint secdsp
 tftp-server-credentials trustpoint scme
 sdspfarm units 10
 sdspfarm transcode sessions 128
 sdspfarm tag 1 XCODER_IOS
 max-ephones 50
 max-dn 300
 ip source-address 10.66.75.246 port 2000
```

The Secure transcoder must be showing up and action by following command,

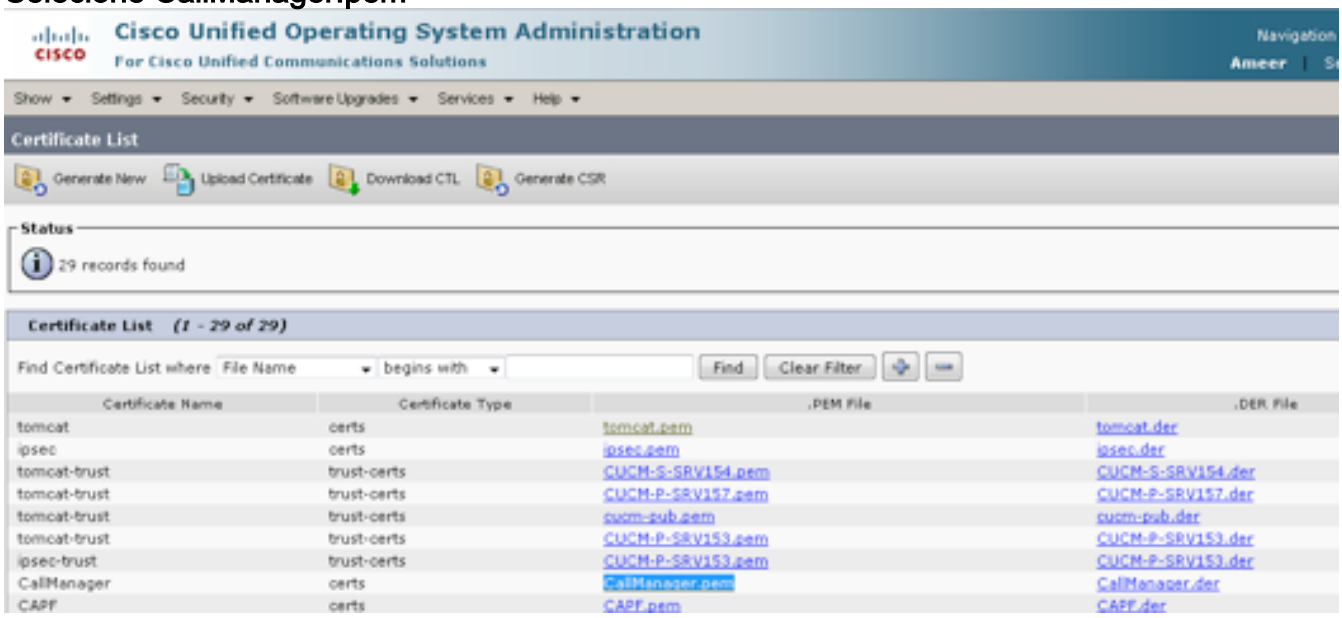
```
MS-3945#sh sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
        IPv4 Address: 10.66.75.246
        Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.66.75.246, Port Number: 2000
  Priority: N/A, Version: 7.0, Identifier: 10
  Trustpoint: N/A

Transcoding Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.66.75.246, Port Number: 2443
TCP Link Status: CONNECTED, Profile Identifier: 20
Security
 Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 20, Reported Max OOS Streams: 0
```

```
Supported Codec: g711ulaw, Maximum Packetization Period: 30
Supported Codec: g711alaw, Maximum Packetization Period: 30
Supported Codec: g729ar8, Maximum Packetization Period: 60
Supported Codec: g729abr8, Maximum Packetization Period: 60
Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
TLS : ENABLED
```

Etapa 4. Configurar o ponto da confiança para CUCM e registre o certificado CUCM no CUBO.

```
MS-3945(config)#crypto pki trustpoint cucm50
MS-3945(ca-trustpoint)# enrollment terminal
MS-3945(ca-trustpoint)# revocation-check none
```

- Entre agora na página de administração do OS CUCM (sistema operacional):
- **> gerenciamento de certificado > achado da Segurança**
- **Selecione CallManager.pem**



- Selecione a **transferência o certificado** e **salvar como o** arquivo do **.pem**
- Abra o arquivo do .pem no bloco de notas
- Copie de "**-----COMECE O CERTIFICADO-----**"até "**-----CERTIFICADO DA EXTREMIDADE-----**"
- Copie o certificado em cube3945 como o exemplo

```
crypto pki authenticate cucm50

After entering the command paste the certificate and press two times enter after END
CERTIFICATE.

############################
MS-3945(config)#crypto pki authenticate cucm-pub

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

-----BEGIN CERTIFICATE-----
MIICszCCAhygAwIBAgIIFOPHFlcCUbcwDQYJKoZIhvcNAQEFBQAwXzEWMBQGA1UE
AwwNQ1VDTS1QLVNSVjE1MzEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDSVNDTzEM
MAoGA1UEBwwDQkFOMQwwCgYDVQQIDANLQVIxCzAJBgNVBAYTAklOMB4XDTExMTEx
NjEyMDUwMloXDTE2MTExNjEyMDUwMlowXzEWMBQGA1UEAwwNQ1VDTS1QLVNSVjE1
MzEMMAoGA1UECwwDVEFDMQ4wDAYDVQQKDAVDSVNDTzEMMAoGA1UEBwwDQkFOMQww
CgYDVQQIDANLQVIxCzAJBgNVBAYTAklOMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
```

```
iQKBgQCRt2YXfOMgQueva16tyMCwQw0fKCDw3bqq/63atNUhSqFpswk+04GhPqxh
Pesx6bMW3E22AGWoTjsrqYTRY7TA/p2u03yPcgd0OPMoxNk6VN88/FLW6YNd3rOK
TmABim1UEMVMYDFQoGhtzUxya7ZFe3vpqBnDlUrgy0q01zQzJwIDAQABo3gwdjAL
BgNVHQ8EBAMCArwwJwYDVR0lBCAwHgYIKwYBBQUHAwEGCCsGAQUFBwMCBggrBgEF
BQcDBTAfBgNVHREEGDAWhhRodHRwOi8vQ1VDTS1QLVNSVjE1MzAdBgNVHQ4EFgQU
ZIiGXzZQV0phnLrsY8Bby3jM9S0wDQYJKoZIhvcNAQEFBQADgYEAQzIvbQm8EOSU
v+bm9oykvHLmrQXjvSgSylO8mC5koUurYa/a0yf0AjMwDMc8F/NArTktsDyjddmw
Oq0GlYMuMh1oyPeb41/bbc+AJxI/d/xprOJSt1qwFI3CJjCvsWm3azC4wflItZNo
4gaCwzzY2UoedUA/rHrWcYod6Vl6Adw=
-----END CERTIFICATE-----

Certificate has the following attributes:
       Fingerprint MD5: 05813269 C50FD13F 20D65A7C 0C4CD73E
      Fingerprint SHA1: 8BE549A5 FB3A856F A6B3CC8B 7C30F0DF C9280288

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

MS-3945(config)#
############################
```

- Se você tem mais de um CallManager no grupo CCM, configurar o ponto confiável para todos os Nós e importe os Certificados do CallManager porque as etapas precedentes, se não, Failover não ocorrem.

Etapa 5. Exporte o certificado IO a fim instalar no CallManager do gerenciador de chamada

```
##############################
MS-3945(config)#crypto pki export cube3945 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB+TCCAWKgAwIBAgIBATANBgkqhkiG9w0BAQQFADAQMQ4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBgNVBAMTBWlv
c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgx7LSPwS0iAgv6Zq
1AMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhDgbjvj43/TzqcJLSricIkBnSHSVme
SXxo+gz2sGhgzBABBvjtJ86/kaVOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx
a1TQid2ylUOnAwpJKx8LTQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjAfBgNVHSMEGDAWgBQf+4wpeDVM3rkjL5LoZkjr4n4j+DAdBgNV
HQ4EFgQUH/uMKXg1TN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEEBQADgYEAcHvx
2hhF/eD2/mCgmcDWrh86OU5VV+0I3Eiphto6I8s+y2UhPMshF3sJ+OhDsT6T+C7U
xi0g96lTxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCMaoBlxCLtHsZvcnsVGrar3Jt
dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIBrTCCARagAwIBAgIBAjANBgkqhkiG9w0BAQQFADAQMQ4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMxMjRaFw0xNTAxMDYwNjMwMTVaMBwxGjAYBgNVBAMTETAw
OjI0OjE0OkJCOjVCOkRGMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALIxjJSbcgK3
6c4EnOs/FDrqKtwHXQhwncAh2N3k4LghdwAdsQFXGtHjeFJWA6TBm/fLibLD4fW8
eoacG7fpJJkCAwEAAaNPME0wCwYDVR0PBAQDAgWgMB8GA1UdIwQYMBaAFB/7jCl4
NUzeuSMvkuhmSOvifiP4MB0GA1UdDgQWBBSW11Md2rFbqZf0IuicijOJ15PnPDAN
BgkqhkiG9w0BAQQFAAOBgQCZeTK4TeNrtoQ3/3eaCD7sL/RNic8aRbNOn2KcCxyO
WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S8O0YXTDYOeQ/kO9i9RrTFq
ARbDZRUULb02tgRbJyHngQ5dV7C7hqwr4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G
GQ==
-----END CERTIFICATE-----

MS-3945(config)#
####################################
```

- Copie o certificado e salvar no bloco de notas como arquivo cube3945g.pem.

  Nota: Somente o certificado de uso geral necessário

- Transfira arquivos pela rede o certificado de CA IO como a CallManager-**confiança**.
- Navegue à página de administração do OS CUCM
- >gerenciamento de certificado da **Segurança > certificado da transferência de arquivo pela rede**

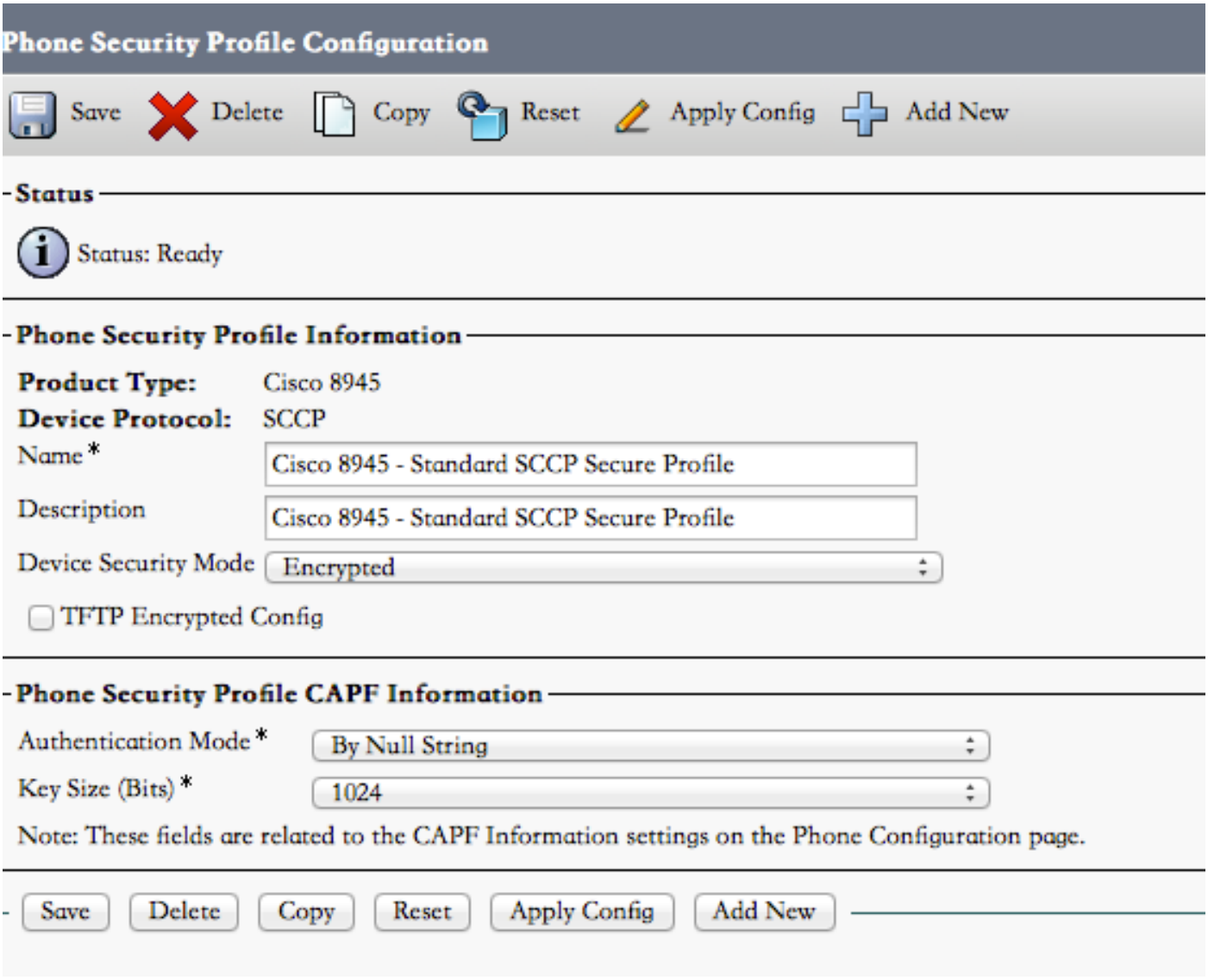
Etapa 6. Configurar Cube3945 e CUCM para fixam o telefone CP-8945

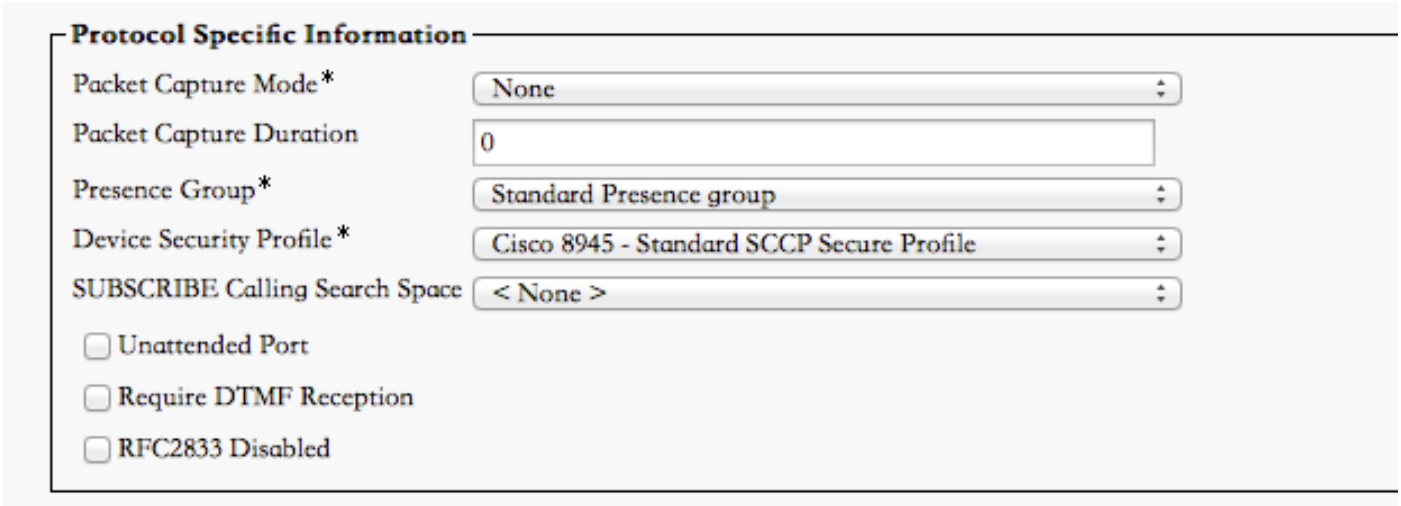
No CUBO

```
################################
MS-3945(config)#crypto pki export cube3945 pem terminal
% CA certificate:
-----BEGIN CERTIFICATE-----
MIIB+TCCAWKgAwIBAgIBATANBgkqhkiG9w0BAQQFADAQMQ4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBgNVBAMTBWlv
c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgx7LSPwS0iAgv6Zq
1AMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhDgbjvj43/TzqcJLSricIkBnSHSVme
SXxo+gz2sGhgzBABBvjtJ86/kaVOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx
a1TQid2ylUOnAwpJKx8LTQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjAfBgNVHSMEGDAWgBQf+4wpeDVM3rkjL5LoZkjr4n4j+DAdBgNV
HQ4EFgQUH/uMKXg1TN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEEBQADgYEAcHvx
2hhF/eD2/mCgmcDWrh86OU5VV+0I3Eiphto6I8s+y2UhPMshF3sJ+OhDsT6T+C7U
xi0g96lTxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCMaoBlxCLtHsZvcnsVGrar3Jt
dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIIBrTCCARagAwIBAgIBAjANBgkqhkiG9w0BAQQFADAQMQ4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMxMjRaFw0xNTAxMDYwNjMwMTVaMBwxGjAYBgNVBAMTETAw
OjI0OjE0OkJCOjVCOkRGMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALIxjJSbcgK3
6c4EnOs/FDrqKtwHXQhwncAh2N3k4LghdwAdsQFXGtHjeFJWA6TBm/fLibLD4fW8
eoacG7fpJJkCAwEAAaNPME0wCwYDVR0PBAQDAgWgMB8GA1UdIwQYMBaAFB/7jCl4
NUzeuSMvkuhmSOvifiP4MB0GA1UdDgQWBBSW11Md2rFbqZf0IuicijOJ15PnPDAN
BgkqhkiG9w0BAQQFAAOBgQCZeTK4TeNrtoQ3/3eaCD7sL/RNic8aRbNOn2KcCxyO
WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S8O0YXTDYOeQ/kO9i9RrTFq
ARbDZRUULb02tgRbJyHngQ5dV7C7hqwr4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G
GQ==
-----END CERTIFICATE-----

MS-3945(config)#
####################################
```

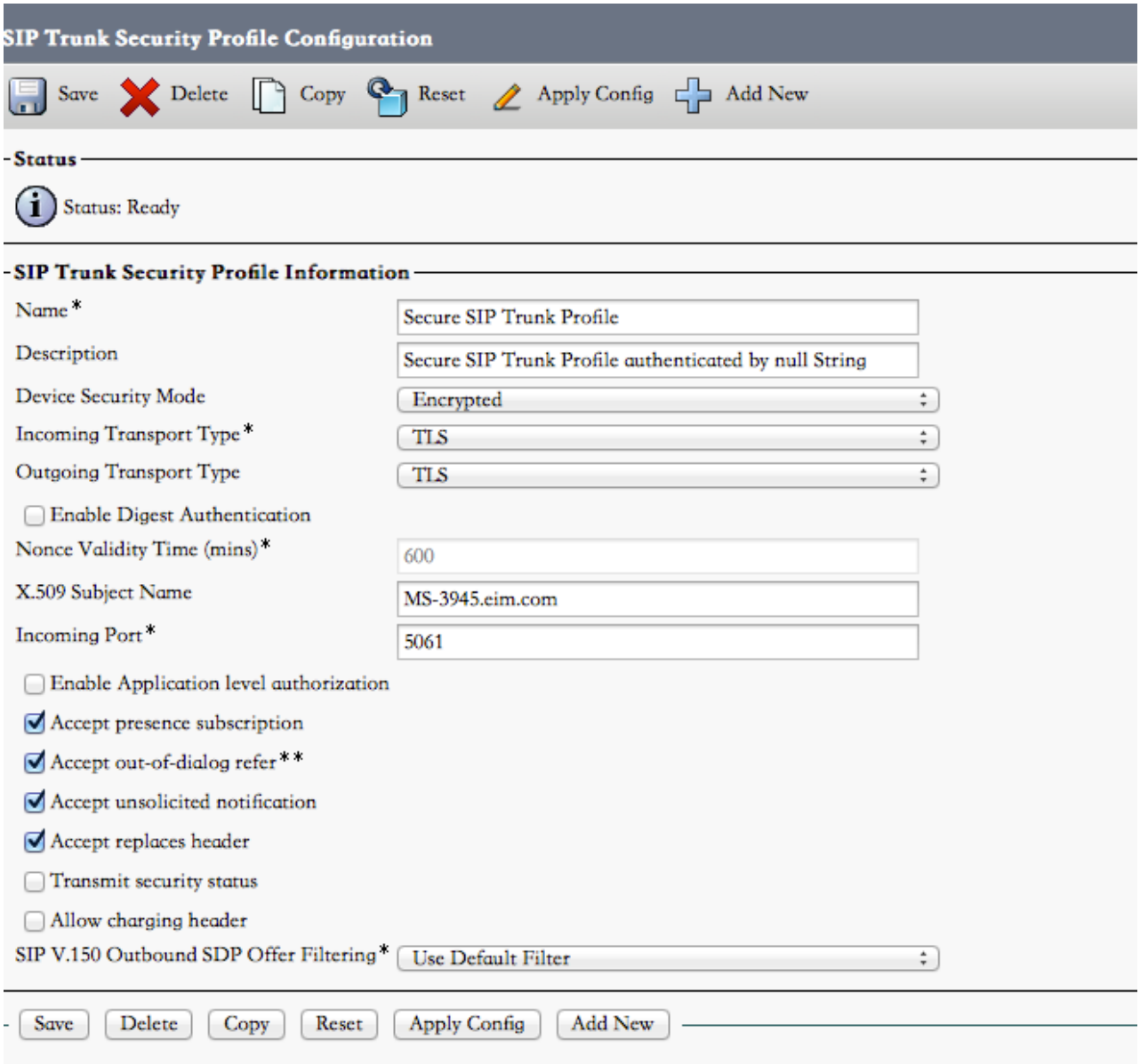
Em CUCM

- Registro CP-8945 em CUCM no modo seguro.
- Crie um perfil seguro SCCP para CP-8945
- Selecione o perfil seguro sob a configuração em CP-8945.

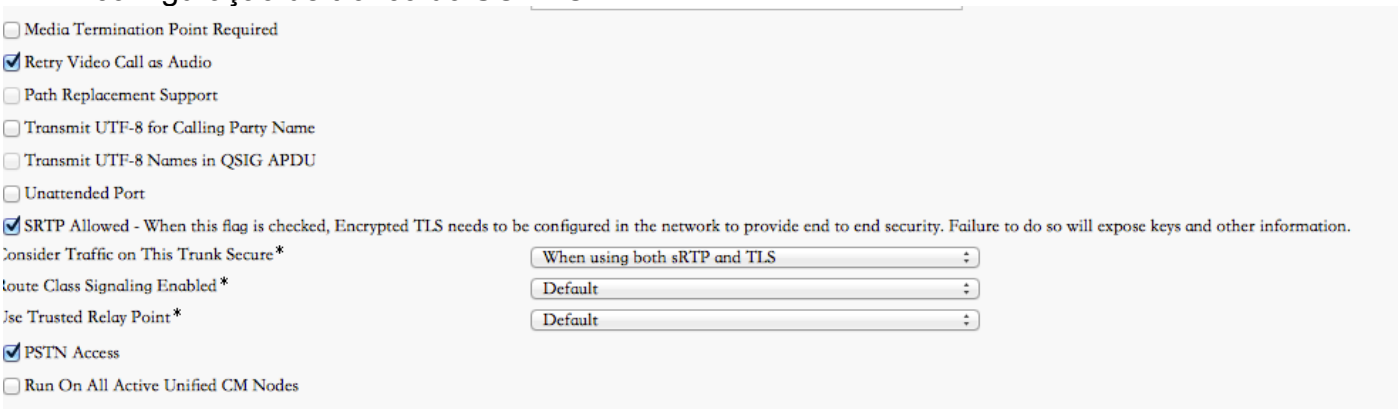


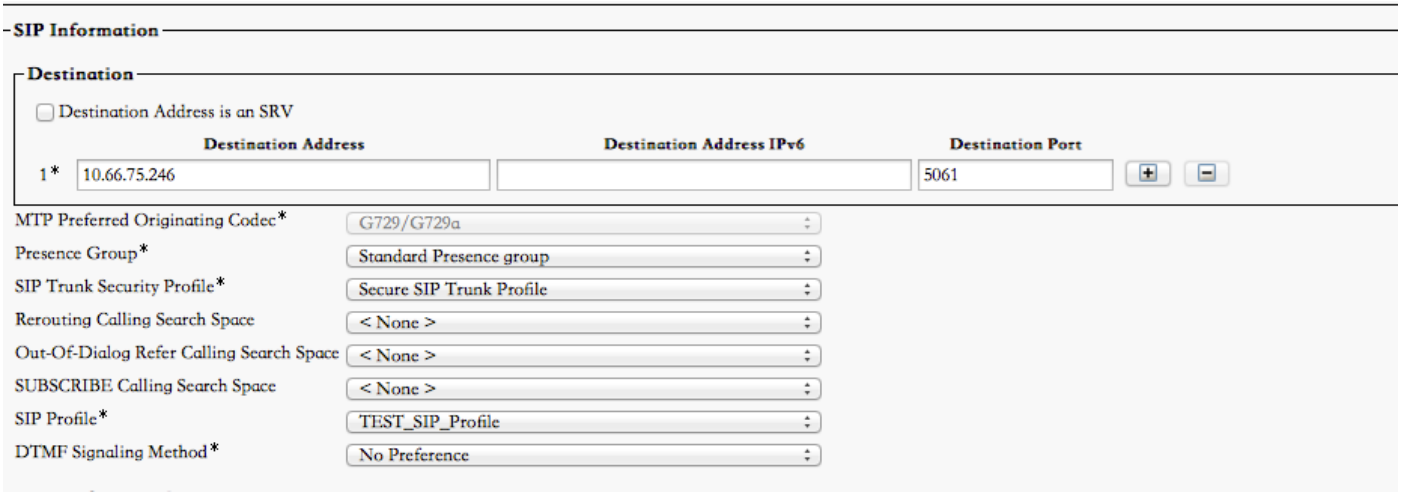


- **Salvar** e **restaure a** configuração CP-8945, assegure-se de que se registre está bem
- **Aplique o** perfil seguro do SORVO no tronco do SORVO para o CUBO



- A configuração de tronco do SORVO





- Com uma chamada de teste, você pode usar o comando show a fim verificar que o atendimento está no SRTP ao RTP no CUBO, e a imagem do cacifo na tela CP-8945 confirma, há SRTP entre o telefone e o CUBO

```
MS-3945#sh sccp conn
sess_id     conn_id      stype mode     codec   sport rport ripaddr conn_id_tx

458757      20         s-xcode sendrecv g711u   16770 2000  10.66.75.246
458757      24           xcode sendrecv g711u   16768 2000  10.66.75.246

Total number of active session(s) 1, and connection(s) 2

MS-3945#sh call active voice brief
<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded

 media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

 long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  <codec> (payload size)
 Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
dBm
  MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
         speeds(bps): local <rx>/<tx> remote <rx>/<tx>
 Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
 bw: <req>/<act> codec: <audio>/<video>
  tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
 rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>



Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
```

```
0    : 32138 423566780ms.1 (02:08:15.881 UTC Tue Feb 5 2013) +2270 pid:2088 Answer 1005 active
 dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.66.75.178:24714 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

0    : 32139 423566790ms.1 (02:08:15.891 UTC Tue Feb 5 2013) +2250 pid:1006 Originate 2088
active
 dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 10.66.75.76:22512 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

0    : 32142 423569050ms.1 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate  connecting
 dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0x0 video tos:0x0
 IP 10.66.75.246:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: No
 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

0    : 32144 423569050ms.2 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate  connecting
 dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0x0 video tos:0x0
 IP 10.66.75.246:2000 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
 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


Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4
```

Informações Relacionadas

- Guia da Segurança CUCM
- Manual de configuração do CUBO