# 在CUCM-CUBE/CUBE-SBC之间配置SIP TLS

## 目录

<u>简介</u> <u>先决条件</u> <u>要用 的组件</u> <u>配 四 配 验 []</u> <u>验 证 排除</u> 目录

# 简介

本文档帮助在思科统一通信管理器(CUCM)和思科统一边界元素(CUBE)之间配置SIP传输层安全 (TLS)

### 先决条件

思科建议了解这些主题

- SIP 协议
- 安全证书

要求

- •终端上的日期和时间必须匹配(建议使用相同的NTP源)。
- CUCM必须处于混合模式。
- •需要TCP连接(在任何传输防火墙上打开端口5061)。
- CUBE必须安装安全许可证和UCK9许可证。

### 使用的组件

- SIP
- 自签名证书

### 配置

网络图



### 配置步骤

### 步骤1: 创建信任点以保存CUBE的自签名证书

crypto pki trustpoint CUBEtest(this can be any name)

enrollment selfsigned

serial-number none

fqdn none

ip-address none

subject-name cn= ISR4451-B.cisco.lab !(this has to match the router's host name)

revocation-check none

rsakeypair ISR4451-B.cisco.lab !(this has to match the router's host name) 步骤2.创建信任点后,运行命令Crypto pki enroll CUBEtest以获取自签名证书

crypto pki enroll CUBEtest

% The fully-qualified domain name will not be included in the certificate

Generate Self Signed Router Certificate? [yes/no]: yes 如果注册正确,则必须预期此输出

Router Self Signed Certificate successfully created 步骤3.获取证书后,需要将其导出

crypto pki export CUBEtest pem terminal 以上命令必须生成以下证书 % Self-signed CA certificate:

----BEGIN CERTIFICATE----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU110 NDUxLUIuY21zY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix 7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR00BBYEFPmM tVKinW/q6yDX07WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4 LDQaxQ==

----END CERTIFICATE-----

% General Purpose Certificate:

----BEGIN CERTIFICATE----

MIIBgDCCASqgAwIBAgIBATANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDExNJU110 NDUxLUIuY21zY28ubGFiMB4XDTE1MTIxNTAxNTAxNVoXDTIwMDEwMTAwMDAwMFow HjEcMBoGA1UEAxMTSVNSNDQ1MS1CLmNpc2NvLmxhYjBcMA0GCSqGSIb3DQEBAQUA A0sAMEgCQQDGtZ974Tfv+pngs1+cCeLZ/e0b2zq6CrIj4T1t+NS1G5sjMJ919/ix 7Fa6DG33LmEYUM1NntkLaz+8UNDAyBZrAgMBAAGjUzBRMA8GA1UdEwEB/wQFMAMB Af8wHwYDVR0jBBgwFoAU+Yy1UqKdb+rrINc7tZcrdIRMKPowHQYDVR00BBYEFPmM tVKinW/q6yDX07WXK3SETCj6MA0GCSqGSIb3DQEBBQUAA0EADQXG2FYZ/MSewjSH T88SHXq0EVqcLrgGpScwcpbR1mKFPpIhDVaJfH/FC6jnkGW7JFWcekA5Kp0tzYx4 LDQaxQ==

-----END CERTIFICATE-----复制上述生成的自签名证书并将其粘贴到文件扩展名为.pem的文**本文件** 以下示例命名为ISR4451-B.ciscolab.pem

File	ICD/461 D sizes lab som	
File name:	ISR4451-B.Cisco.lab.pem	
Save as type:	All types (*.*)	

步骤4.将CUBE证书上传到CUCM

- CUCM OS Admin > Security > Certificate Management > Upload Certificate/Certificate chain
- 证书用途= CallManager-Trust
- 上载.pem文件

https://cucm10-5.cisco.lab,	/cmplatform/certificateUpload.do	
pload Certificate/Certific	ate chain	
Upload 🖳 Close		
Status		
Warning: Uploading a c	luster-wide certificate will distribute it to all server	s in this cluster
Jpload Certificate/Certific	ate chain	
Certificate Purpose*	CallManager-trust	•
Description(friendly name)		
Upload File	Browse ISR4451-B.cisco.lab.pem	
Upload Close		
opioad		
	em.	
indicates required it		
*- indicates required it		

步骤5.下载Call Manager自签名证书

- 查找显示Callmanager的证书
- 单击主机名
- 点击下载PEM文件
- 将其保存到计算机

Cisco Unified Operating System Administration     For Cisco Unified Communications Solution	Nevigetic	Gess Unified OS Adm	integration
• Setrige + Security + Setrieve Upgrades + Services + Halp +	Cisco	search Documentation	About
forte Liet			
Cerverale Seffeigned 🖓 Lipitual Certificate Certificate chain 🔃 Generale CER			
48			
10 records found			
tificate List (1 - 20 of 20)		Area	per Page
Cestificate List where Cestificate 📴 begins with 📑 Californiager Find Clear Piter 👰 🖷			
Centralize Comment Name Trat Net Trat Ostribution Issuel Br Dorro Nemager CUCM1052 Self-signed RSA CUCM1052 CUCM1052 07/26/2	itton Ki23 Setti-s	Description Agrical contribute generation	ed by syste
Certificate Details(Self-signed)			
D 💫 https://10.201.196.162/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security/CallMater Security/CallMater Security	anager/c	erts/Call	
ertificate Details for CUCM1052, CallManager			
S Regenerate CSR Download .PEM File Download .DER File			
Status			
i 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			
t IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII			
Version: V3			
Serial Number: 4A7B503A9A3D202AD7D54B1F874B7DF7 SignatureAlgorithm: SHA1withBSA (1,2,840,113540,1,1,5)			
Issuer Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US			
Validity From: Thu Jul 21 13:11:22 CDT 2016			
To: Tue Jul 20 13:11:21 CDT 2021			
Subject Name: L=rcdn5, ST=Texas, CN=CUCM1052, OU=prime, O=cisco, C=US			
Key value:			
3082010a0282010100b803883f1177dcd68431efc16d7fdb127db637091d1d8e7b5			
8d913a1689d2a289ea74fc1b42b5a571bc0abc1310e63b8924a84a3e7dc03e5001ac			
4fb551b9f1569d44c1f336d5a1c2a80cbf65ebc93e2bb1619ca3d1c77984aeed1a752			
3C433011085t019725C801108580399765e00851c0d73336244870214091f7892be 38d07ae913dee31954028c16a6b0207378006c3663653da0ca6bba6bd59f3c3b77202			
89d50f14b7d8d4ae303069072917f6491ba1083584cae22122bd6ed524da1598353			
70			
Regenerate Generate CSR Download .PEM File Download .DER File		_	
Close			

### 步骤6.将Callmanager.pem证书上传到CUBE

- 使用文本文件编辑器打开Callmanager.pem
- 复制文件的整个内容
- 在CUBE上运行以下命令

enrollment terminal

revocation-check none

crypto pku authenticate CUCMHOSTNAME

(PASTE THE CUCM CERT HERE AND THEN PRESS ENTER TWICE)

You will then see the following:

Certificate has the following attributes:

Fingerprint MD5: B9CABE35 24B11EE3 C58C9A9F 02DB16BC

Fingerprint SHA1: EC164F6C 96CDC1C9 E7CA0933 8C7518D4 443E0E84

% Do you accept this certificate? [yes/no]: yes

If everything was correct, you should see the following:

Trustpoint CA certificate accepted.

% Certificate successfully imported 步骤7.将SIP配置为使用CUBE的自签名证书信任点

sip-ua

crypto signaling default trustpoint CUBEtest 步骤8.使用TLS配置拨号对等体

dial-peer voice 9999 voip

answer-address 35..

destination-pattern 9999

session protocol sipv2

session target dns:cucm10-5

voice-class sip options-keepalive

#### srtp

步骤9.配置CUCM SIP中继安全配置文件

- CUCM Admin页面> System > Security > SIP Trunk Security Profile
- 配置配置文件,如下所示

SIP Trunk Security Profile Configurati	on Reset 🧷 Apply Config 🛟 A	Add New	
Status Status: Ready			
-SIP Trunk Security Profile Information	1		
Name*	CUBE Secure SIP Trunk Profile		
Description	Secure SIP Trunk Profile authent	ticated by null String	
Device Security Mode	Encrypted	-	
Incoming Transport Type*	TLS	•	
Outgoing Transport Type	TLS	•	
Enable Digest Authentication			
Nonce Validity Time (mins)*	600		
X.509 Subject Name	ISR4451-B.cisco.lab		
Incoming Port*	5061		
Enable Application level authorization			
Accept presence subscription			
Accept out-of-dialog refer**			
Accept unsolicited notification			
Accept replaces header			
Transmit security status			
Allow charging header			
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter	•	

注意: 生成自签名证书时,X.509字段与您之前配置的CN名称匹配至关重要

步骤10.在CUCM上配置SIP中继

- 确保选中SRTP allowed复选框
- •配置正确的目标地址并确保将端口5060替换为端口5061
- •确保选择正确的SIP中继安全配置文件(在步骤9中创建)

SIP Information				
Destination				
Destination Address is an SRV Destination Address I Destination Address I Destinati Destinati Destination Address I Destination Addr	ddress	Destination A	ddress IPv6	Destination Port
1* 10.201.160.12				5061
MTP Preferred Originating Codec*	711ulaw	•		
BLF Presence Group*	Standard Presence group	•		
SIP Trunk Security Profile*	ISR4451-B 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-options	- X	ew Details	
DTMF Signaling Method *	No Preference	•		

### •保存并重置中继。

# 验证

由于您在CUCM上启用了OPTIONS PING,因此SIP中继必须处于FULL SERVICE状态

Name *	Descriptio	n Calli	ng Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Dur	ation
ISR4451-	8			G711-Secure					SIP Trunk	Full Service	Time In Full Service: 0 d minute	ay 0 hour 0
SIP中结	继状态	显示	完全肌	<b>贤务</b> 。								
拨号对	等体物	大态显	显示如	下:								
show d	ial-pe	er vo	ice su	ummary								
TAG	TYPE	MIN	OPER	PREFIX	DEST	-PATTEI	RN	FEF	R THRU	SESS-TARGET	STAT PORT	
KEEPAL	IVE											
9999	voip	up	up		9999			0	syst	dns:cucm10-5		active

# 故障排除

### 启用并收集这些调试的输出

debug crypto pki api debug crypto pki callbacks debug crypto pki messages debug crypto pki transactions debug ssl openssl errors debug ssl openssl msg debug ssl openssl states debug ip tcp transactions debug ccsip verbose

### Webex录制链接:

https://goo.gl/QOS1iT