在ASA上配置AnyConnect VPN电话的证书身份验 证

目录

简介

本文档提供的配置示例显示如何配置自适应安全设备(ASA)和CallManager设备,以为在思科IP电话 上运行的AnyConnect客户端提供证书身份验证。完成此配置后,思科IP电话可以建立与ASA的 VPN连接,这些连接使用证书来保护通信。

先决条件

要求

尝试进行此配置之前,请确保满足以下要求:

• AnyConnect Premium SSL许可证

• Cisco VPN电话许可证的AnyConnect

根据ASA版本,您将看到ASA版本8.0.x的"AnyConnect for Linksys电话"或8.2.x或更高版本的 "AnyConnect for Cisco VPN Phone"。

使用的组件

本文档中的信息基于以下软件和硬件版本:

• ASA - 8.0(4)版或更高版本

• IP电话型号 — 7942 / 7962 / 7945 / 7965 / 7975

- •电话 --- 8961/9951/9971,带9.1(1)版固件
- 电话 版本9.0(2)SR1S 瘦呼叫控制协议(SCCP)或更高版本

•思科统一通信管理器(CUCM)-8.0.1.100000-4版或更高版本

此配置示例中使用的版本包括:

• ASA — 版本9.1(1)

• CallManager — 版本8.5.1.10000-26

有关CUCM版本中支持的电话的完整列表,请完成以下步骤:

1. 打开此URL:https://<CUCM服务器IP地址>:8443/cucreports/systemReports.do

2. 选择Unified CM Phone Feature List > Generate a new report > Feature:虚拟私有网络。 本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

电话证书类型

思科在电话中使用以下证书类型:

- 制造商安装证书(MIC) 所有7941、7961和更新型号的思科IP电话都包含MIC。MIC是由思科 证书颁发机构(CA)签名的2048位密钥证书。当存在MIC时,无需安装本地有效证书(LSC)。为 使CUCM信任MIC证书,它在其证书信任库中使用预安装的CA证书CAP-RTP-001、CAP-RTP-002和Cisco_Manufacturing_CA。
- LSC 在您配置设备安全模式进行身份验证或加密后,LSC可保护CUCM和电话之间的连接。
 LSC拥有Cisco IP电话的公钥,该公钥由CUCM证书颁发机构代理功能(CAPF)私钥签名。这是首选方法(与使用MIC相反),因为只有管理员手动调配的思科IP电话才允许下载和验证CTL文件。注意:由于安全风险增加,思科建议仅将MIC用于LSC安装,而不是继续使用。将思科IP电话配置为使用MIC进行传输层安全(TLS)身份验证或用于任何其他目的的客户会自行承担风险。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意:使用<u>命令查找工具(仅限注册用户)可获取有关本部分所使用命令的详细信息。</u>

配置

本文档介绍以下配置:

• ASA 配置

- CallManager 配置
- CallManager上的VPN配置
- IP电话上的证书安装

ASA 配置

ASA的配置与将AnyConnect客户端计算机连接到ASA时的配置几乎相同。但是,这些限制适用:

- •隧道组必须具有group-url。此URL将在CM的VPN网关URL下配置。
- 组策略不得包含拆分隧道。

此配置使用ASA设备安全套接字层(SSL)信任点中以前配置和安装的ASA(自签名或第三方)证书。 有关详细信息,请参阅以下文档:

- 配置数字证书
- 在 ASA 8.x 上手动安装第三方供应商证书以便与 WebVPN 一起使用的配置示例
- ASA 8.x : VPN访问与使用自签名证书的AnyConnect VPN客户端配置示例

ASA的相关配置是:

ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access tunnel-group SSL general-attributes address-pool SSL_Pool default-group-policy GroupPolicy_SSL tunnel-group SSL webvpn-attributes authentication certificate group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside

CallManager 配置

要从ASA导出证书并将证书作为Phone-VPN-Trust证书导入CallManager,请完成以下步骤:

- 1. 向CUCM注册生成的证书。
- 2. 检查用于SSL的证书。 ASA(config)#**show run ssl** ssl trust-point SSL outside
- 号出证书。
 ASA(config)#crypto ca export SSL identity-certificate
 隐私增强邮件(PEM)编码的身份证书如下:

-----BEGIN CERTIFICATE----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMMMTM1MzEwWhcNMjMw MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwN1ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1 NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1 wsidpQWq1DDrJD1We83L/oqmhkWJ07QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1 -----END CERTIFICATE-----

4. 从终端复制文本并将其另存为.pem文件。

5. 登录CallManager并选择**Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust**以上传在上一步中保存的证书文件。 **CallManager上的VPN配置**

- 1. 导航至Cisco Unified CM管理。
- 2. 从菜单栏中,选择Advanced Features > VPN > VPN Gateway。

CISCO Cisco Unified CM A	dministration ations Solutions			
System - Call Routing - Media Resources -	Advanced Features 🔻 Device	a 🔻 Applicati	on 🔻 User Management 🔻 B	ulk Administratio
	Voice Mail	•		_
	SAF	•		
Cisco Unified CM Adn	EMCC	•		
System version: 8.5.1.10000-26	Intercompany Media Servic	es 🕨		
	Fallback	- •		
	VPN		VPN Profile	
Please visit the License Report Page	for more details.		VPN Group	
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU E5540 @ :	2.53GHz	VPN Gateway	RAM
			VPN Feature Configuration	
Last Successful Logon: Feb 5, 2013 5:55:45 P	м	_	The output of the output of the	

3. 在VPN网关配置窗口中,完成以下步骤:在VPN Gateway Name字段中,输入名称。这可以 是任何名称。在VPN Gateway Description字段中,输入说明(可选)。在VPN Gateway URL字段中,输入在ASA上定义的group-url。在"此位置"字段的"VPN证书"中,选择之前上传 到CallManager的证书,以将其从信任库移动到此位置。

System 👻 Call Routing 👻 Media Reso	urces 🔻 Advanced Features 👻 Device 👻	Application 👻 User Management 👻	Bulk Administration 👻 Help 👻
VPN Gateway Configuration			
Gave 🗙 Delete 🗋 Copy	Add New		
Status			
i Status: Ready			
VPN Gateway Information			
VPN Gateway Name* ASA_Pho	DIREVEN		
VPN Gateway Description			
VPN Gateway URL* https://d	sa5520-c.cisco.com/SSL		
VPN Gateway Certificates			
VPN Certificates in your Truststore	SUBJECT: CN-10.198.16.136,unstructure SUBJECT: CN-10.198.16.140,unstructure SUBJECT: CN-10.198.16.140;8443 ISSU SUBJECT: CN-ASA5510-F-IP-PHONE,uns	edName=10.198.16.136 ISSUER: Ci edName=10.198.16.140 ISSUER: Ci ER: CN=10.198.16.140:8443 S/N: c tructuredName=ASASS10-F.cisco.cr	N=10.198.16.136,unstructuredName= + N=10.198.16.140,unstructuredName= e7:e2:72:4f om ISSUER: CN=ASA5510-F-IP-PHON
	~ .	^	
VPN Certificates in this Location*	SUBJECT: unstructuredName=ASA5520-0	C.cisco.com,CN⇔ASA5520-C.cisco.c	xam ISSUER: DC=com,DC=crtec,DC= ▲
			· -
- Save Delete Copy	Add New		

4. 从菜单栏中,选择Advanced Features > VPN > VPN Group。

System - Call Routing - 1	Media Resources 🔻	Ad	vanced Features 🔻	Device 🔻	Applic	ation 🔻	User Management	•	Bulk Adminis
VPN Gateway Configura	ition		Voice Mail		•				
			SAF		•				
Save 🗙 Delete	Copy 🛟 Add		EMCC		•				
- Status			Intercompany Media	Services	•				
(i) Undate successful			Fallback		•				
			VPN		•	VPN	l Profile		-
VPN Gateway Informati	ion	_				VPN	l Group		
VPN Gateway Name*	ASA_PhoneVPN					VPN	l Gateway		
VPN Gateway Description						VPN	l Feature Configurat	ion	
VPN Gateway URL*	https://asa5520-c	.cis	co.com/SSL						

5. 在All Available VPN Gateways字段中,选择之前定义的VPN Gateway。单击向下箭头,将所 选网关移动到此VPN组中的Selected VPN Gateways字段。

System Call Routing Media Resources Advanced F	eatures 👻 Device 👻 Application 👻 User Manag
VPN Group Configuration	
🔚 Save 🗶 Delete 🗋 Copy 🕂 Add New	
Status	
i Status: Ready	
VPN Group Information	
VPN Group Name* ASA_PhoneVPN	
VPN Group Description	
VPN Gateway Information	
All Available VPN Gateways	*
Move the	Gateway down
**	
Selected VPN Gateways in this VPN Group* ASA_Phone	VPN
	×

6. 从菜单栏中,选择Advanced Features > VPN > VPN Profile。

System Call Routing Media Resources	Advanced Features V Device V Appli	cation 🔻 User Management 👻 Bulk Administ
VPN Group Configuration Save Copy Add Status Status: Ready	Voice Mail SAF EMCC Intercompany Media Services Fallback	
VPN Group Information VPN Group Name* ASA_PhoneVPN VPN Group Description	VEN	VPN Group VPN Gateway VPN Feature Configuration

7. 要配置VPN配置文件,请填写标有星号(*)的所有字段。

System 👻 Call Routing 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻
VPN Profile Configuration
🔚 Save 🗶 Delete 🕞 Copy 🕂 Add New
Status
i Status: Ready
VPN Profile Information
Name* ASA_PhoneVPN
Description
Enable Auto Network Detect
MTU*
Fail to Connect* 30
Enable Host ID Check
Client Authentication
Client Authentication Method* Certificate
Enable Password Persistence
- Save Delete Copy Add New
启用自动网络检测: 如果启用,VPN电话会ping TFTP服务器,如果未收到响应.它会自动启
动VPN连接。 启用主机ID检查: 如果启用,VPN电话将VPN网关URL的FQDN与证书的
CN/SAN进行比较。如果客户端不匹配或使用带星号(*)的通配符证书,则客户端无法连接。 启 用密码持久性:这允许//PN电话缓存用户名和密码 以便下次尝试//PN。

8. 在Common Phone Profile Configuration窗口中,单击Apply Config以应用新的VPN配置。您

Device -	Application -	User Managemen	t Bulk Administration Help
CTI Ro Gateko Gatew Phone Trunk Remot	ute Point eeper vay e Destination		
Device	e Settings		Device Defaults Firmware Load Information Default Device Profile Device Profile Phone Button Template Softkey Template Phone Services SIP Profile Common Device Configuration Common Phone Profile
System 🔻	Call Routing 🔻	Media Resource:	s ▼ Advanced Features ▼ Device ▼ A
Common	Phone Profile	Configuratio	
Save	X Delete	🗋 Copy 🎦	Reset 🧷 Apply Config 🕂 Add New
	rmation ——		
VPN Grou	P ASA_PhoneV	PN	
VPN Profi	le ASA_PhoneV	PN	

9. 如果为特定电话/用户创建了新配置文件,请转至"电话配置"窗口。在Common Phone Profile字段中,选择Standard Common Phone Profile。

	CTI Route Point	Polatod	Linker Ra	ck To Find/Lie
	Gatekeeper	Kelateu	Links: Da	ck to Find/Lis
nfig C	Gateway			
MAC	Phone	008645576112		
Desc	Trunk	Auto 1000		
Devi	Remote Destination	Default	•	View Details
Com	Device Settings	< None >	-	View Details
Phone E	Button Template*	Standard 7962G SCCP	•	
Softkey	Template	Walter Phones	•	
Commo	on Phone Profile*	Standard Common Phone Profile	-	

10. 再次将电话注册到CallManager以下载新配置。

证书身份验证配置

要配置证书身份验证,请在CallManager和ASA中完成以下步骤:

- 1. 从菜单栏中,选择Advanced Features > VPN > VPN Profile。
- 2. 确认Client Authentication Method字段设置为Certificate。

System 👻 Call Ro	uting 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻
VPN Profile Con	figuration
🔚 Save 🗶 🕻	Delete [Copy 🕂 Add New
_ Status	
i Status: Rea	dy
_ ¥PN Profile Inf	ormation
Name* ASA	_PhoneVPN
Description	
🗖 Enable Auto I	Network Detect
_C Tunnel Parame	ters
мти*	1290
Fail to Connect*	30
🔲 Enable Host I	D Check
Client Authenti	cation
Client Authentica	tion Method* Certificate
Enable Passw	ord Persistence

- 3. 登录CallManager。从菜单栏中,选择**Unified OS Administration > Security > Certificate** Management > Find。
- 4. 导出所选证书身份验证方法的正确证书:MIC:Cisco_Manufacturing_CA 使用MIC对IP电话 进行身份验证

Find Certificate List where File N	ame v begins with v	Find Clear Filter
Certificate Name	Certificate Type	.ºEM Fle
tomcat	certs	tomcat.sem
ipsec	certs	iprec.pem
tormoat-brast	trust-certs	CUCM85.pen
ipsec-trust	trust-certs	CUCM85.pem
CaliManager	certs	CallNanager.pem
CAPF	certs	CAPF.pem
TVB	oart:	TVS.com
CallManager-trust	trust-cents	Cisco Nanufacturing CA.pern
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CaliManager-trust	trust-certs	CAPF-18cfD46e.pem
CallManager-trust	trust-certs	CAP-PTP-002.pem

LSC:思科证书颁发机构代理功能(CAPF) — 使用LSC对IP电话进行身份验证

Certificate Name	Certificate Type	.PEM File	
tomcat	certs	iomcat.pem	tomczt.der
psec	certs	bsec.pem	ipeec.der
comcat-trust	trust-certs	CUCM85.pem	OLCM85.der
psec-trust	trust-certs	CUCM85.perr	CLCN85.der
CallManager	certs	CallManacer.pem	CallManager.der
CAPF	certs	CAPF.pem	CAPF.der
TVS	certs	TV5.pem	TVS.der
CallManager-trust	trust-certs	Cisco Manufacturing CA.pem	

- 5. 查找证书,即Cisco_Manufacturing_CA或CAPF。下载.pem文件并另存为.txt文件
- 6. 在ASA上创建新信任点,并使用之前保存的证书对信任点进行身份验证。当系统提示您输入 base-64编码的CA证书时,选择文本并粘贴到下载的.pem文件中以及BEGIN和END行。示例 显示:

```
ASA (config) #crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint) #enrollment terminal
ASA(config-ca-trustpoint) #exit
ASA(config) #crypto ca authenticate CM-Manufacturing
ASA(config) #
```

<base-64 encoded CA certificate>

quit

7. 确认隧道组上的身份验证已设置为证书身份验证。 tunnel-group SSL webvpn-attributes **authentication certificate** group-url https://asa5520-c.cisco.com/SSL enable

IP电话上的证书安装

IP电话可以与MIC或LSC配合使用,但每个证书的配置过程不同。

MIC安装

默认情况下,支持VPN的所有电话都预装了MIC。7960和7940电话不附带MIC,需要特殊安装程序 才能使LSC安全注册。

注意:思科建议仅将MIC用于LSC安装。思科支持LSC对与CUCM的TLS连接进行身份验证。由于 MIC根证书可能受到危害,将电话配置为使用MIC进行TLS身份验证或用于任何其他目的的客户会自 行承担风险。如果MIC受到危害,思科不承担任何责任。

LSC安装

o

- 1. 在CUCM上启用CAPF服务。
- 2. 激活CAPF服务后,分配电话指令以在CUCM中生成LSC。登录到Cisco Unified CM管理,然 后选择**设备>电话**。选择您配置的电话。
- 3. 在"证书颁发机构代理功能(CAPF)信息"部分,确保所有设置都正确,并将操作设置为将来日期

Certificate Operation*	Install/Upgrade						
Authentication Mode*	By Authentication String						
Authentication String	123456						
Generate String							
Key Size (Bits)*	2048						
Operation Completes By	2013	3	10	12	(VVVV·MM·DD·HH)		

- 4. 如果"身份验证模式"(Authentication Mode)设置为空字符串或现有证书(Null String or Existing Certificate),则无需进一步操作。
- 5. 如果Authentication Mode设置为字符串,请在电话控制台中手**动选择Settings > Security** Configuration > **# > LSC > Update。

验证

使用本部分可确认配置能否正常运行。

ASA验证

```
Session Type: AnyConnect Detailed
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1) AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1) SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : OGroup Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
```

ASA5520-C(config)#show vpn-sessiondb detail anyconnect

Encapsulation: TLSv1.0 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 1759 Bytes Rx : 799 Pkts Tx : 2 Pkts Rx : 1 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 57.2 Public IP : 172.16.250.15 Encryption : AES128 Hashing : SHA1 Encapsulation: TLSv1.0 TCP Src Port : 50529 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : SSL VPN Client Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 835 Bytes Rx : 0 Pkts Tx : 1 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 57.3 Assigned IP : 10.10.10.2 Public IP : 172.16.250.15 Encryption : AES128 Hashing : SHA1 Encapsulation: DTLSv1.0 UDP Src Port : 51096 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes Client Type : DTLS VPN Client Client Ver : Cisco SVC IPPhone Client v1.0 (1.0) Bytes Tx : 303255 Bytes Rx : 269270 Pkts Tx : 5642 Pkts Rx : 5649 Pkts Tx Drop : 0 Pkts Rx Drop : 0

CUCM验证

System 💌	Cal Routi	ng 💌 Medio Resources 👻 Adva	naed Features 👻 Devia	e 🐐 Application 👻	User klanagement 💌 Bulk	Administration 👻 Help 💌					
Find and L	ist Pho	nes					Related Links: Actively Log				
Add Ne	ew 📕	Select All 🌐 Geer Al 🗮 0	alate Salacted 🛛 🐴 Res	sel Selactad 🧷 App	aly Config to Selected						
Status i 4 records found											
Find Phone	where	Device Name	★ begins with ★ S	elect item or enter s	Find Clear fil search text 👻	ter 🕹 😑	IP Phone registered with the CUCM using VPN address				
		Device Name(Line) *	Description	Device Pool	Desice Protocol	Status	CP Address				
E 8		84 	Auto 1001	Default	SCOP	Unknown	Unknown				
1 2		SEPERATOR	Auto 1000	Default	SCCP (Registered with 192,168,100.1	10.10.10.2				

故障排除

目前没有针对此配置的故障排除信息。

相关 Bug

- Cisco Bug ID <u>CSCtf09529</u>,在CUCM中为8961、9951和9971电话添加对VPN功能的支持
- Cisco Bug ID CSCuc71462, IP电 话VPN故障切换需要8分钟
- Cisco Bug ID CSCtz42052, IP电话SSL VPN支持非默认端口号

- Cisco Bug ID <u>CSCth96551</u>,电话VPN用户+密码登录时不支持所有ASCII字符。
- Cisco Bug ID <u>CSCuj71475</u>,IP电话VPN需要手动输入TFTP
- Cisco Bug ID <u>CSCum10683</u>, IP电话不记录未接、已拨或已接呼叫

相关信息

• <u>技术支持和文档 - Cisco Systems</u>