在ASA上使用證書身份驗證配置AnyConnect VPN電話

目錄

<u>簡介</u> <u>必要條件</u> <u>需求用元件</u> <u>慣電設定 設態證 排解</u> 相關資訊

簡介

本文檔提供配置示例,說明如何配置自適應安全裝置(ASA)和CallManager裝置,為在Cisco IP電話 上運行的AnyConnect客戶端提供證書身份驗證。完成此配置後,思科IP電話可以建立到ASA的 VPN連線,利用證書來保護通訊。

必要條件

需求

嘗試此組態之前,請確保符合以下要求:

• AnyConnect Premium SSL許可證

• 適用於Cisco VPN的AnyConnect電話許可證

根據ASA版本,您會看到ASA 8.0.x版的「適用於Linksys電話的AnyConnect」或ASA 8.2.x版或更 高版本的「適用於Cisco VPN電話的AnyConnect」。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• ASA - 8.0(4)版或更高版本

• IP電話型號 — 7942 / 7962 / 7945 / 7965 / 7975

- •電話 8961 / 9951 / 9971,帶9.1(1)版韌體
- Phone 9.0(2)SR1S版 Skinny Call Control Protocol(SCCP)或更高版本
- •思科統一通訊管理器(CUCM)-8.0.1.100000-4版或更高版本

此組態範例中使用的版本包括:

•ASA 9.1(1)版

• CallManager — 版本8.5.1.10000-26 有關CUCM版本中受支援電話的完整清單,請完成以下步驟:

1. 開啟此URL:https://<CUCM Server IP Address>:8443/cucreports/systemReports.do

2. 選擇Unified CM電話功能清單>生成新報告>功能: 虛擬私人網路。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

電話證書型別

思科在電話中使用以下憑證型別:

- 製造商安裝證書(MIC) 所有7941、7961和較新型號Cisco IP電話都包含MIC。MIC是由思科 憑證授權單位(CA)簽署的2048位金鑰憑證。如果存在MIC,則無需安裝本地有效證書(LSC)。 為了讓CUCM信任MIC證書,它在其證書信任儲存中使用預安裝的CA證書CAP-RTP-001、 CAP-RTP-002和Cisco_Manufacturing_CA。
- LSC 在配置裝置安全模式進行身份驗證或加密後,LSC會保護CUCM和電話之間的連線。
 LSC擁有思科IP電話的公鑰,該公鑰由CUCM證書授權代理功能(CAPF)私鑰簽名。這是首選方法(與使用MIC相反),因為只允許管理員手動調配的Cisco IP電話下載和驗證CTL檔案。附註:由於安全風險增加,Cisco建議僅將MIC用於LSC安裝,而不是繼續使用。將Cisco IP電話配置為使用MIC進行傳輸層安全(TLS)驗證或用於任何其他目的的客戶需要自行承擔風險。

設定

本節提供用於設定本文件中所述功能的資訊。

附註:使用<u>命令查詢工具(僅供已註冊</u>客戶使用)可獲取本節中使用的命令的詳細資訊。

組態

本檔案將說明以下組態:

- ASA配置
- CallManager配置

- CallManager上的VPN配置
- IP電話上的證書安裝

ASA配置

ASA的配置與將AnyConnect客戶端電腦連線到ASA時的配置幾乎相同。但是,以下限制適用:

- •隧道組必須具有group-url。此URL將在CM中的VPN網關URL下配置。
- 組策略不得包含拆分隧道。

此配置使用先前在ASA裝置的安全套接字層(SSL)信任點中配置和安裝的ASA(自簽名或第三方)證 書。如需詳細資訊,請參閱以下檔案:

- 配置數位證書
- ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例
- ASA 8.x:使用AnyConnect VPN客戶端使用自簽名證書的VPN訪問配置示例

```
ASA的相關配置為:
```

ip local pool SSL_Pool 10.10.10.10.10.10.254 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

若要從ASA匯出證書並將證書作為Phone-VPN-Trust證書匯入CallManager,請完成以下步驟:

- 1. 向CUCM註冊生成的證書。
- 2. 檢查用於SSL的證書。 ASA(config)#**show run ssl** ssl trust-point SSL outside
- 3. 匯出證書。

ASA(config)#crypto ca export SSL identity-certificate Privacy Enhanced Mail(PEM)編碼的身份證書如下:

-----BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwN1ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1 NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4Clq6ZQwpahde22sdf1 wsidpQWq1DDrJD1We83L/oqmhkWJ07QfNrGZhOLv9xOpR7BFpZd1yFyzwAPkoBl1 -----END CERTIFICATE-----

- 4. 從終端複製文字並將其另存為.pem檔案。
- 5. 登入到CallManager並選擇Unified OS Administration > Security > Certificate Management >

Upload Certificate > Select Phone-VPN-trust以上步驟中儲存的證書檔案進行上傳。 CallManager上的VPN配置

- 1. 導航到Cisco Unified CM Administration。
- 2. 從選單欄中選擇Advanced Features > VPN > VPN Gateway。

CISCO CISCO Unified CM Ad For Cisco Unified Communic	dministration ations Solutions		
System - Call Routing - Media Resources -	Advanced Features - Device - Appli	cation 🔻 User Management 🔻 Bulk A	dministration
	Voice Mail		
	SAF 🕨		
Cisco Unified CM Adm	EMCC +		
System version: 8.5.1.10000-26	Intercompany Media Services		
Licencia e Manufacere	Fallback +	2	
System is operating on Domo license:	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 Pf	4		

3. 在VPN網關配置視窗中,完成以下步驟:在VPN Gateway Name欄位中,輸入名稱。可以是 任何名稱。在VPN Gateway Description欄位中,輸入說明(可選)。在VPN Gateway URL欄 位中,輸入在ASA上定義的group-url。在此位置中的VPN證書欄位中,選擇之前上傳到 CallManager的證書,以將其從信任庫移動到此位置。

System 👻 Call Routing 👻 Media Reso	urces 🔻 Advanced Features 👻 Device 💌 Application 👻 User Management 👻 Buk Administration 👻 Help 👻
VPN Gateway Configuration	
Save 🗙 Delete 🗋 Copy (Add New
Status	
i Status: Ready	
VPN Gateway Information	
VPN Gateway Name* ASA_Pho	IN 8 VPN
VPN Gateway Description	
VPN Gateway URL* https://a	sa5520-c.disco.com/SSL
VPN Gateway Certificates	
VPN Certificates in your Truststore	SUBJECT: CN-10.198.16.136,unstructuredName-10.198.16.136 ISSUER: CN-10.198.16.136,unstructuredName- SUBJECT: CN-10.198.16.140,unstructuredName-10.198.16.140 ISSUER: CN-10.198.16.140,unstructuredName- SUBJECT: CN-10.198.16.140:8443 ISSUER: CN-10.198.16.140:8443 S/N: e7:e2:72:4f SUBJECT: CN-ASA5510-F-IP-PHONE,unstructuredName-ASA5510-F.cisco.com ISSUER: CN-ASA5510-F-IP-PHON
	* *
VPN Certificates in this Location*	SUBJECT: unstructuredNeme=ASA5520-C.cisco.com,CN=ASA5520-C.cisco.com ISSUER: DC=com,DC=crtec,DC=
- Save Delete Copy .	Add New

4. 從選單欄中選擇Advanced Features > VPN > VPN Group。

System 👻 Call Routing 👻 Media Resources 👻	Advanced Features Device Applic	cation 👻 User Management 👻 Bulk Adminis
VPN Gateway Configuration	Voice Mail SAF EMCC Intercompany Media Services	
(i) Update successful	Fallback	VPN Profile
VPN Gateway Information		VPN Group
VPN Gateway Name* ASA_PhoneVPN VPN Gateway Description		VPN Gateway VPN Feature Configuration
VPN Gateway URL* https://asa5520-c	.cisco.com/SSL	

5. 在All Available VPN Gateways欄位中,選擇先前定義的VPN Gateway。點選向下箭頭將所選 網關移動到此VPN組欄位中的Selected VPN Gateways。

System 👻 Call Routing 👻	Media Resources 🔻	Advanced Features 🔻	Device 🔻	Application 🔻	User Mana <u>c</u>
VPN Group Configura	tion				
🔚 Save 🗙 Delete	Copy 🕂 Add	d New			
Status					
i Status: Ready					
_ ¥PN Group Informati	ion —				
VPN Group Name*	ASA_PhoneVPN				
VPN Group Description					
∀PN Gateway Inform	ation				
All Available VPN Gate	ways				
		Move the Gatews	ay down		Ŧ
		**			

Selected VPN Gateways in this VPN Group* ASA_PhoneVPN		
		×
	-	

6. 從選單欄中選擇Advanced Features > VPN > VPN Profile。

System Call Routing	Media Resources 🔻	Ad	vanced Features 🔻	Device 🔻	Applic	ation 🔻	User Management	 Bulk 	Administ
VPN Group Configura Save X Delete	ition D Copy 👍 Add		Voice Mail SAF EMCC Intercompany Media Fallback	a Services					
			VPN		•	VPN	Profile		
VPN Group Informat	ion ASA_PhoneVPN					VPN VPN VPN	Group Gateway Feature Configuratio	n	

7. 要配置VPN配置檔案,請填寫所有標有星號(*)的欄位。

System 🔻 Call Ro	uting 👻 Media Resources 👻 Advanced Features 👻 Device 👻 Application 👻
VPN Profile Cor	nfiguration
Save 🗙 (Delete 🚺 Copy 🕂 Add New
Status ———	
i Status: Rea	dy
∀PN Profile Inf	ormation —
Name* ASA	PhoneVPN
Description	
🗖 Enable Auto I	Network Detect
_ ⊤Tunnel Parame	eters
мти*	1290
Fail to Connect*	30
Enable Host 1	ID Check
Client Authenti	cation
Client Authentica	ation Method* Certificate 🗸
Enable Passw	vord Persistence
- Save Del	ete Copy Add New
啟用自動網路檢測 VPN連線。 啟用主 CN/SAN進行比較。 。 啟用密碼永續性	:如果啟用,VPN電話ping TFTP伺服器,如果未收到響應,則自動發起 機ID檢查:如果啟用,VPN電話會將VPN網關URL的FQDN與證書的 。如果客戶端不匹配或使用帶有星號(*)的萬用字元證書,則客戶端無法連線 :這允許VPN電話快取下次VPN嘗試的使用者名稱和密碼。

Device -	Application -	User Managem	ent .	Bulk Administration He	elp 🔻
CTI Ro Gateke Gatew Phone Trunk Remote	ute Point eper ay e Destination				
Device	Settings			Device Defaults Firmware Load Information Default Device Profile Device Profile Phone Button Template Softkey Template Phone Services SIP Profile Common Device Configuration	
System ▼ Common 🔚 Save	Call Routing ▼ Phone Profile ★ Delete	Media Resource Configurat	ion	 Advanced Features ▼ □ Beset)evice ▼ / ⊐ Add New
- VPN Info VPN Grou VPN Profi	rmation P ASA_Phone le ASA_Phone	VPN		•	

9. 如果您為特定電話/使用者建立了新配置檔案,請轉到「電話配置」視窗。在Common Phone Profile欄位中,選擇**Standard Common Phone Profile**。

CTI Route Point		Relate	d Links: Ba	ck To Find/Lis
	Gatekeeper			
nfig c	Gateway			
Phone Phone				-
Desc	Trunk	SCB64F576113		
Devis	Remote Destination	Default		View Details
Com	Device Settings	None >	÷	View Details
Phone E	Button Template*	Standard 7962G SCCP	•	
Softkey	Template	Walter Phones	•	1
Commo	n Phone Profile*	Standard Common Phone Profile		

10. 再次向CallManager註冊電話,以便下載新配置。

證書身份驗證配置

要配置證書身份驗證,請在CallManager和ASA中完成以下步驟:

- 1. 從選單欄中選擇Advanced Features > VPN > VPN Profile。
- 2. 確認Client Authentication Method欄位已設定為Certificate。

System Call Routing Media Resources Advanced Features Device Applie	ation 🔻
VPN Profile Configuration	
🔚 Save 🗶 Delete 🗋 Copy 🕂 Add New	
_ Status	
i Status: Ready	
┌ ¥PN Profile Information	
Name* ASA_PhoneVPN	
Description	
Enable Auto Network Detect	
_ Tunnel Parameters	
MTU* 1290	
Fail to Connect* 30	
Enable Host ID Check	
Client Authentication	
Client Authentication Method* Certificate	-
Enable Password Persistence	

- 3. 登入到CallManager。從選單欄中選擇**Unified OS Administration > Security > Certificate** Management > Find。
- 4. 匯出所選證書身份驗證方法的正確證書:MIC:Cisco_Manufacturing_CA 使用MIC驗證IP電話

Find Certificate List where	File Name 👻	begins with 🔹	Find Clear Filter
Certificate Name		Certificate Type	.PEM Fle
tomcat	certs		tomcat.sem
ipsec	certs		ipcec.pem
tonneat-trust	trust-ce	rls	CUCM85.pen
ipsec-trust	trust-ce	rts	CUCM85.pem
CallManager	certs		CallNanager.pem
CAPF	certs		CAPF.pem
TVE	oarts		TVS.zem
CallManager-trust	trust-ce	rts	Cisco Nanufactoring CA.pent
CallManager-trust	trust-ce	rts	CAP-RTP-001.pem
CallManager-trust	trust-ce	rts	Cisco Root CA 2048.pem
CallManager-trust	trust-ce	rts	CAPF-18cfD46e.pem
CallManager-trust	trust-ce	rtr	CAP-RTP-002.pem

LSC:思科憑證授權代理功能(CAPF) — 使用LSC驗證IP電話

Certificate Name	Certificate Type	.PEM File	
tomcat	certs	iomcat.pem	tomcat.der
psec	certs	bsec.pam	ipeec.der
:omcat-trust	trust-certs	CUCM85.pem	OLCM85.der
psec-trust	trust-certs	CUCM85.perr	CLCN85.der
CalManager	certs	CallManacer.pem	CaliManager.der
CAPE	certs	CAPF.pem	CAPF.der
TVS	certs	TV5.pem	TVS.der
CallManager-trust	trust-certs	Cisco Manufacturing CA.pem	

5. 查詢證書(Cisco_Manufacturing_CA或CAPF)。下載.pem檔案並另存為.txt檔案

6. 在ASA上建立新的信任點,並使用以前儲存的證書驗證信任點。當系統提示您輸入base-64編碼的CA憑證時,請選擇並貼上下載的.pem檔案中的文字以及BEGIN和END行。範例如下: 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. 確認隧道組上的身份驗證已設定為證書身份驗證。 tunnel-group SSL webvpn-attributes authentication certificate group-url https://asa5520-c.cisco.com/SSL enable

IP電話上的證書安裝

IP電話可以與MIC或LSC一起使用,但每個證書的配置過程不同。

MIC安裝

預設情況下,支援VPN的所有電話都預裝了MIC。7960和7940電話不附帶MIC,並且需要特殊的安 裝步驟才能使LSC安全地註冊。

附註:思科建議您僅將MIC用於LSC安裝。Cisco支援LSC對CUCM的TLS連線進行身份驗證。由於 MIC根證書可能受到危害,因此將電話配置為使用MIC進行TLS驗證或用於任何其他目的的客戶會自 行承擔風險。如果MIC受到危害,思科不承擔任何責任。

LSC安裝

- 1. 在CUCM上啟用CAPF服務。
- 2. 啟用CAPF服務後,分配電話說明以在CUCM中生成LSC。登入到Cisco Unified CM管理並選 擇**Device > Phone**。選擇您配置的電話。
- 3. 在「Certificate Authority Proxy Function(CAPF)Information(證書頒發機構代理功能(CAPF)資 訊)」部分,確保所有設定都正確無誤,並且操作已設定為未來的日期。

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.UU)		

- 4. 如果身份驗證模式設定為空字串或現有證書,則無需執行進一步的操作。
- 5. 如果身份驗證模式設定為字串,請在電話控制檯中手動選擇Settings > Security Configuration > **# > LSC > Update。

驗證

使用本節內容,確認您的組態是否正常運作。

- -

ASA驗證

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

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
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驗證

System 💌 Cal Ro	ting 💌 Media Resources 👻 Advi	anced Features 👻 Devic	ce 👻 Application 👻	User klangement 💌 Bulk	Administration 👻 Help 💌	
Find and List Ph	nnes					Related Links: Actively Log
🕂 Add New	Select Al 🗮 Geer Al 🙀	Dalate Salacted 🏻 🔭 Re	isəl Sələctəci 🧷 Aqı	aly Config to Selected		
Status (1) 4 records to Phone (1 - 4	und of 4)					
Find Phone where	Device Name	▼ begins with ▼	Select item or enter s	Find Clear fil search text 👻	ts: 🕹 👄	IP Phone registered with the CUCM using VPN address
	Device Name(Line) *	Description	Device Pool	Deside Protocol	Status	CP Address
	SHE	Auto 1001	Default	SCCP	Unknown	Unknown
E 762	SEPERFECT	Auto 1000	Default	SCCP (Registered with 192.168.100.1	10.10.10.2

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關錯誤

- •思科漏洞ID CSCtf09529,在CUCM中新增對於8961、9951、9971電話的VPN功能支援
- Cisco錯誤ID <u>CSCuc71462</u>,IP電話VPN故障轉移需要8分鐘
- 適用於非預設連線埠號碼的Cisco錯誤ID CSCtz42052 IP電話SSL VPN支援
- •思科錯誤ID CSCth96551,在電話VPN使用者+密碼登入過程中不支援所有ASCII字元。

- Cisco錯誤ID <u>CSCuj71475</u>,IP電話VPN所需的手動TFTP條目
- 思科錯誤ID <u>CSCum10683</u>,未記錄未接、已撥或已接呼叫的IP電話

相關資訊

• 技術支援與文件 - Cisco Systems