ASA 8.X:AnyConnect SCEP註冊配置示例

目錄

簡介 必要條件 需求 採用元件 慣例 背景資訊 所需變更概述 啟用Anyconnect SCEP功能的XML設定 配置ASA以支援AnyConnect的SCEP協定 測試AnyConnect SCEP SCEP請求後Microsoft Windows上的證書儲存 疑難排解 相關資訊

<u>簡介</u>

SCEP註冊功能在AnyConnect獨立客戶端2.4中引入。在此過程中,可以修改AnyConnect XML配置 檔案以包含與SCEP相關的配置,並為證書註冊建立特定的組策略和連線配置檔案。當 AnyConnect使用者連線到此特定組時,AnyConnect向CA伺服器傳送證書註冊請求,並且CA伺服 器自動接受或拒絕該請求。

<u>必要條件</u>

<u>需求</u>

本文件沒有特定需求。

<u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- 運行軟體版本8.x的Cisco ASA 5500系列自適應安全裝置
- Cisco AnyConnect VPN版本2.4

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

<u>背景資訊</u>

AnyConnect的自動SCEP註冊的目標是以安全且可擴展的方式向客戶端頒發證書。例如,使用者不 需要從CA伺服器要求憑證。此功能整合在AnyConnect客戶端中。根據XML配置檔案中提到的證書 引數,向客戶端頒發證書。

所需變更概述

AnyConnect SCEP註冊功能要求在XML配置檔案中定義某些證書引數。在ASA上為證書註冊建立組 策略和連線配置檔案,XML配置檔案與該策略相關聯。AnyConnect客戶端連線到使用此特定策略的 連線配置檔案,並傳送證書請求,該請求包含在XML檔案中定義的引數。證書頒發機構(CA)自動接 受或拒絕該請求。如果在客戶端配置檔案中定義<CertificateSCEP>元素,AnyConnect客戶端將檢 索使用SCEP協定的證書。

在AnyConnect嘗試自動檢索新證書之前,客戶端證書身份驗證必須失敗,因此,如果您已經安裝了 有效的證書,則不會進行註冊。

當使用者登入到特定組時,將自動註冊。還有一種可用於證書檢索的手動方法,在該方法中,向使 用者顯示Get Certificate按鈕。這只有在使用者端可以直接存取CA伺服器(而不是透過通道)時才 能使用。

有關詳細資訊,請參閱<u>Cisco AnyConnect VPN客戶端管理員指南2.4版</u>。

這些是需要在AnyConnect XML檔案中定義的重要元素。有關詳細資訊,請參閱<u>Cisco AnyConnect</u> <u>VPN客戶端管理員指南2.4版</u>。

- <AutomaticSEPPERost> 指定為其配置SCEP證書檢索的ASA主機名和連線配置檔案(隧道 組)。該值需要採用ASA\connection配置檔名稱的完全限定域名或ASA\connection配置檔名稱 的IP地址的格式。
- <CAURL> 標識SCEP CA伺服器。
- <CertificateSCEP> 定義如何請求證書的內容。
- <DisplayGetCertButton> 確定AnyConnect GUI是否顯示「獲取證書」按鈕。它使使用者能 夠手動請求證書的續訂或調配。

以下是配置檔案範例:

<?xml version="1.0" encoding="UTF-8"?>

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
```

```
<ClientInitialization>
```

```
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
```

```
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
```

```
<ShowPreConnectMessage>false</ShowPreConnectMessage>
```

```
<CertificateStore>All</CertificateStore>
```

```
<CertificateStoreOverride>false</CertificateStoreOverride>
```

```
<ProxySettings>Native</ProxySettings>
```

```
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
    ReconnectAfterResume
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
   Automatic
 </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
    http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

配置ASA以支援AnyConnect的SCEP協定

為了提供對專用註冊機構(RA)的訪問,ASA管理員必須建立一個別名,該別名的ACL限制專用端與 所需RA的網路連線。為了自動檢索證書,使用者連線到此別名並進行身份驗證。

請完成以下步驟:

- 1. 在ASA上建立指向特定配置組的別名。
- 2. 在使用者客戶端配置檔案的<AutomaticSEPPERost>元素中指定別名。
- 3. 將包含<CertificateEnrollment>部分的客戶端配置檔案附加到特定配置組。
- 4. 為特定配置組設定ACL以限制流向私有RA的流量。

請完成以下步驟:

 將XML配置檔案上傳到ASA。選擇Remote Access VPN > Network(client)access > Advanced > SSL VPN > Client settings。在SSL VPN Client profiles下,按一下Add。按一下「Browse Local Files」以選擇設定檔檔案,然後按一下「Browse Flash」以指定快閃記憶體檔案名稱。 按一下「Upload File」。

emote Access VPN 🗗 🖗	K Configuration > Remote Access VPN > Netw	ork (Client) Access > Advanced > SSL VPN > Client Settin
Introduction Network (Client) Access AnyConnect Connection Profiles IPsec Connection Profiles Group Policies Dynamic Access Policies AnyConnect Customization/Localization Address Assignment	Identify AnyConnect Client related files. AnyConnect Client Images The regular expression is used to match the use You can also minimize connection setup time by r Add C Edit Delete + 4	r-agent of a browser to an image. moving the image used by the most commonly encountered operat
B- B Advanced	Image	Regular expression to match user-agent
Clentiess SSL VPN ACLEManager Clentiess SSL VPN Access Clentiess SSL VPN Access Clentiess SSL VPN Access Control of the	SSL VPN Clent Profiles Add C Lar Collecte Name	Package
BHCP Server	Upload Package	
🐻 Advanced	Upload a file from local computer to flas few minutes. Please wait for the operat Local File Path: scuments and Flash File System Path: disk0:/ac_scep	th file system on the device. The upload process might take a don to finish. Settings\asimalik\Desktop\ac_scep Browse Local Files Browse Flash

2. 為證書註冊**設**置certenroll組策略。選擇**Remote access VPN > Network client access > Group** Policy,然後按一下Add。

🚰 Edit Internal Group Poli	icy: certenroll		×
General Portal H-More Options	Name: certenroll		
	More Options Tunneling Protocols: Web ACL: Access Hours: Simultaneous Logins: Restrict access to VLAN: Connection Profile (Tunnel Group) Lock: Maximum Connect Time: Udd. Timesto	Inherit Clientless SSL VPN ✓ SS ✓ Inherit ✓ ✓ Inherit ✓	L VPN Client IPsec Manage Manage
Find:	OK Can	ous	2

為CA伺服器新增拆分隧道。展開Advanced,然後選擇Split Tunneling。從Policy選單中選擇 Tunnel Network List Below,然後按一下Manage以新增訪問控制清單。

🚰 Edit Internal Group Po	licy: certenro	a							×
General Servers Advanced	Split tunneling tunneling. The of addresses	network lists e security appl on the private	distinquish netv iance makes sp network.	works that require lit tunneling decis	e traffic to ions on the	go thro e basis (ugh the tunnel a of a network list,	nd those that do r which is an ACL ti	nat require nat consists of list
Split Tunneling IE Browser Proxy	DNS Names:	🔽 Inherit							
SSL VPN Client During Client	Policy:	Inherit	Tunnel Netwo	rk List Below				~	
() I set clott	Network List:	Inherit	scep					~	Manage
		_							
	Intercept	DHCP Config	uration Mess	age from Micro	osoft Clie	nts			*
Find:			t Provid	115					
			ок (Cancel	Help				
🖆 ACL Manage	r								
Standard ACL	Extended	ACL							
🗣 Add 🝷 🗹	Edit 📋	Delete	∱ ↓	* 🖻	-	· •			
No Ad	dress		1	Action		Des	cription		
Ģ∴scep									
1	10.11.11.	0/24		V Permit	n ()				
🖨 split		221 1 1 1		10 [°]					
1 🔳	10.1.1.11			🖋 Permit	đ.				
<				IIII /					
		ОК		Cancel		He	lp		

選擇SSL VPN Client,然後從Client Profile to Download選單中選擇certenroll的配置檔案。

General Keep Installer on Client System: Inherit Yes No Servers Compression: Inherit Enable Disable Soft Tunneing Datagram TLS: Inherit Enable Disable SSL WPN Client Keepalive Messages: Inherit Disable Interval: seconds IPsec Client MTU: Inherit Disable Interval: seconds	Edit Internal Group Po	licy: certenroll		
Servers Compression: Inherit Enable Disable Advanced Compression: Inherit Enable Disable Soft Tunneing Datagram TLS: Inherit Enable Disable SSL WPN Clent Keepalive Messages: Inherit Disable Interval: seconds IPSoc Clent MTU: Inherit Disable New	General	Keep Installer on Client System:	🔽 Inherit	⊖ Yes O No
Spit Tunneing Datagram TLS: ✓ Inherit Enable Disable Disable SSL WN Client Keepalve Messages: ✓ Inherit Disable Interval: seconds MTU: Client Profile to Download: Inherit ac_scep New	Servers B-Advanced	Compression:	🔽 Inherit	◯ Enable ◯ Disable
SSL WPN Client Keepalve Messages: Inherit Disable Interval: seconds MTU: Client Profile to Download: Inherit at_scep New	Split Tunneling IE Browser Proxy	Datagram TLS:	🔽 Inherit	◯ Enable ◯ Disable
MTU: Client Profile to Download: Inherit at_scep	SSL VPN Client JProc Client	Keepalive Messages:	🔽 Inherit	Disable Interval: seconds
Client Profile to Download: Inherit ac_scep	Marset Clone	MTU:	🔽 Inherit	
		Client Profile to Download:	🗌 Inheçit	ac_scep 💌 New
Optional Client Modules to Download: V Inherit		Optional Client Modules to Download:	🖌 Inherit	

3. 為證書身份驗證建立另一個名為certauth的組。

🛢 Edit Internal Group Po	licy: certauth					×
General Servers	Name:	certauth	>			
i≟Advanced	Banner:	 Inherit 				
	Address Pools:	🗸 Inherit			Selec	t
	IPv6 Address Pools:	🗸 Inherit			Selec	t
	More Options					*
	Tunneling Protocol	5:	🔄 Inherit	Clientless SSL VPN	SSL VPN Cli	ent
	IPv4 Filter:		🗹 Inherit		*	Mā
	IPv6 Filter:		🗹 Inherit		*	Ma
	NAC Policy:		🖌 Inherit		*	Ma
	Access Hours:		🗸 Inherit		*	Ma
	Simultaneous Login	ns:	🗹 Inherit			
	Restrict access to	VLAN:	🖌 Inherit		*	
	Connection Profile	(Tunnel Group) Lock:	🖌 Inherit		×.	
	Maximum Connect	Time:	🖌 Inherit	Unlimited	minutes	
Find:		🔵 Next 🛛 🔘 Previ	ous			
	ОК	Cancel	Help			

4. 建立certenroll連線配置檔案。選擇**Remote access VPN > Network client access >** AnyConnect connection profiles,然後按一下Add。在「別名」欄位中輸入certenroll組。**注意**

:別名必須與AutomaticSEPPERost下的AnyConnect配置檔案中使用的值匹配。

Add SSL VPN Connecti	on Profile		
Basic	Name:	certenroll	
-Advanced	Aliases:	certenrol	
	Authentication		
-Secondary Authenticat	Method:	AAA Certificate Both	
Authorization Accounting	AAA Server Group:	LOCAL	Manage
SSL VPN		Use LOCAL if Server Group fails	
	Client Address Assigment —		
	DHCP Servers:		
	Client Address Pools:	ssl_pool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	certenroll	Manage
		(Following field is an attribute of the group policy selected above.)	
		Enable SSL VPN Client protocol	

5. 使用證書身份驗證製作另一個名為**certauth**的連線配置檔案。這是註冊後使用的實際連線配置 檔案。

Edit SSL VPN Connec	tion Profile: certauth		
Basic	Name:	certauth	
	Aliases:	certauth	
	Authentication	\sim	
	Method:	AAA O Certificatei O Both	
	AAA Server Group:		Manage
		Use LOCAL if Server Group fails	
	Client Address Assignent —		
	DHCP Servers:		
	Client Address Pools:	ssl_pool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	certauth	Manage
		(Following field is an attribute of the group policy selected above.)	
		Enable SSL VPN Client protocol	

6. 為了確保啟用別名使用,請在登入頁面上選中Allow user to select connection profile, identified by its alias。否則,DefaultWebVPNGroup是連線配置檔案。

Home Of Configuration	intoring 🔄 Save 🌘	Refresh Sack Of	orward y Hep			cisco
Remote Access VPN	9 ¢ ×	Configuration > Remote A	ccess VPN > Network (Clien	t) Access > AnyConnect Co	nnection Profiles	(
Introduction Introduction Network (Clent) Access AnyConnect Connection Profiles IPsec Connection Profiles Group Policies Dynamic Access Policies Dynamic Access Policies Dynamic Access Policies	ies xalization	The security appliance auto client deployment requires e Layer Security (DTLS) tunne (More client-related parame	natically deploys the Cisco Any nd-user administrative rights. T ling options. sters, such as client images and	Connect VPN Client or legacy SS he Cisco Any-Connect VPN Clien client profiles, can be found at	L VPN Clent to remote users upon connect supports the HITPS/TCP (SSL) and Data Clent Settings.)	tion. The initial gram Transport
Advanced Fodorist Security		Enable Cisco AnyConne	ct VPN Client or legacy SSL VPN	Client access on the interfaces	selected in the table below	
SSL VPN		Interface	Allow Access	Enable DTLS		
Clent Settings		outside	Image: A start and a start	2		
Bypass Interface Acc	ess List	inside				
Cleritless SSL VPN Access Easy VPN Remote AAA(Local Users AAA(Local Users Certificate Management Certificate Management DHCP Server DHCP Server Advanced		Access Port: 443 Click here to <u>Assian Certific</u> Login Page Setting Allow user to select con Connection Profiles Connection profile (burnel g Add C Edit Dele	DTLS Port: 443 ate to Interface. nection profile, identified by its i roup) specifies how user is auth te	alias, on the login page. Otherw enticated and other parameter:	ise, DefaultWebVPINGroup will be the conn	action profile,
		Name	Enabled	Allases	Authentication Method	
		certervol		certervol	AAA(LOCAL)	
		Sales		Sales	AAA(LOCAL)	
		DefaultRAGroup			AAA(LOCAL)	
		certauth	. · · · · · · · · · · · · · · · · · · ·	certauth	Certificate	

<u>測試AnyConnect SCEP</u>

使用本節內容,確認您的組態是否正常運作。

1. 啟動AnyConnect客戶端,並連線到certenroll配置檔案。

Cisco AnyCon	nect VPN Client	_ 🗆 🔀	
🗞 Connection	🕄 Statistics 🏾 🍰 About		
	cisco		
Connect to:	asa2.cisco.com	v 🧬	
Group:	certenroll	~	
Username:	cisco		
Password:	****		
	Connect		
se enter your use	ername and password.		

🔋 Cisco AnyCon	nect VPN Client	
🗞 Connection 🛛	🟮 Statistics 🛛 🍰 About	
	cisco	
Connect to:	asa2.cisco.com	✓ 6 ²
Certificate Enrol Please wait whi contacted	<mark>lment</mark> le the Certificate Authority	is
	Enroll	

用Get Certificate按鈕,AnyConnect會直接傳遞註冊請求,而不通過隧道。

請求傳遞到CA伺服器。

🗞 Connection	🚯 Statistics
	alada
	CISCO
Connect to:	asa2.cisco.com 💉 🧬
Group:	certenroll
Username:	cisco
Password:	
	Connect Get Certificate
ase enter your us	ername and password.

<u> </u>	CA2003
	Windows cannot validate that the certificate is actually from "CA2003". You should confirm its origin by contacting "CA2003". The following number will assist you in this process:
	Thumbprint (sha1): 758DAAEF P3DA5383 FDF8CP3C 20837489 A587FCF2
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you advnowledge this risk.
	Do you want to install this certificate?

30



3. 註冊證書後,連線到certauth配置檔案。

SCEP請求後Microsoft Windows上的證書儲存

請完成以下步驟:

- 1. 按一下**開始>運行> mmc**。
- 2. 按一下Add/remove snap in。
- 3. 按一下「Add」,然後選擇「certificates」。

4. 新增**My user account**和**computer account**證書。此圖顯示安裝在Windows證書儲存中的使用 者證書



此圖顯示安裝在Windows證書儲存中的CA證書



<u>疑難排解</u>

本節提供的資訊可用於對組態進行疑難排解。

- AnyConnect SCEP註冊僅在證書身份驗證失敗時起作用。如果未註冊,請檢查證書儲存。如果
 已安裝證書,請刪除這些證書,然後重新測試。
- 除非使用ssl certificate-authentication interface outside port 443命令,否則SCEP註冊不起作用。如需詳細資訊,請參閱以下思科錯誤ID:思科錯誤ID <u>CSCtf06778</u>(僅供<u>註冊</u>客戶使用)-AnyConnect SCEP註冊不適用於Per Group Cert Auth 2思科漏洞ID <u>CSCtf06844</u>(僅限<u>註冊</u>客戶)-AnyConnect SCEP註冊不用於ASA每組證書身份驗證
- 如果CA伺服器位於ASA外部,請確保使用same-security-traffic permit intra-interface命令允許 髮夾操作。另外新增nat outside和access-list命令,如以下示例所示:
 nat (outside) 1
 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87
 其中172.16.1.0是AnyConnect池, 171.69.89.87是CA伺服器IP地址。
- •如果CA伺服器位於內部,請確保將其包括在certenroll組策略的拆分隧道訪問清單中。在本文檔中,假設CA伺服器位於內部。

group-policy certenroll attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value scep

access-list scep standard permit 171.69.89.0 255.255.255.0

相關資訊

- Cisco AnyConnect VPN客戶端管理員指南2.4版
- 技術支援與文件 Cisco Systems