使用比利時eID卡的ASA 8.x Anyconnect身份驗證

目錄

簡介 必要條件 需求 採用元件 慣例 背景資訊 <u>本地PC設定</u> 作業系統 讀卡器 elD運行時軟體 驗證憑證 <u>AnyConnect安裝</u> ASA要求 ASA配置 步驟1. 啟用外部介面 步驟2.配置域名、密碼和系統時間 步驟3.在外部介面上啟用DHCP伺服器。 步驟4.配置elD VPN地址池 步驟5.匯入比利時根CA證書 步驟6.配置安全套接字層 步驟7.定義預設組策略 步驟8.定義憑證對應 步驟9.新增本地使用者 步驟10.重新啟動ASA 微調 一分鐘配置 相關資訊

<u>簡介</u>

本文檔介紹如何設定ASA 8.x Anyconnect身份驗證以使用比利時的eID卡。

<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:

- ASA 5505及相應的ASA 8.0軟體
- AnyConnect客戶端
- ASDM 6.0

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。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱思科技術提示慣例。

<u>背景資訊</u>

eID是比利時政府頒發的PKI(公開金鑰基礎架構)卡,使用者必須使用該卡才能在遠端Windows PC上進行驗證。AnyConnect軟體客戶端安裝在本地PC上,並從遠端PC獲取身份驗證憑證。完成 身份驗證後,遠端使用者將通過完整的SSL隧道訪問中央資源。遠端使用者使用從ASA管理的池獲 取的IP地址進行調配。

<u>本地PC設定</u>

<u>作業系統</u>

本地PC上的作業系統(Windows、MacOS、Unix或Linux)必須最新並安裝了所有必需的修補程式。

<u>讀卡器</u>

您的本地電腦上必須安裝電子讀卡器才能使用elD卡。電子讀卡器是建立電腦程式與身份證晶片之間 通訊通道的硬體裝置。

有關批准的讀卡器清單,請參閱以下URL:<u>http://www.cardreaders.be/en/default.htm</u>

註:要使用讀卡器,必須安裝硬體供應商推薦的驅動程式。

<u>elD運行時軟體</u>

您必須安裝比利時政府提供的elD運行時軟體。此軟體允許遠端使用者讀取、驗證和列印elD卡的內容。該軟體提供法語和荷蘭語版本,適用於Windows、MAC OS X和Linux。

如需詳細資訊,請參閱以下URL:

http://www.belgium.be/zip/eid_datacapture_nl.html



必須將身份驗證證書匯入本地PC上的Microsoft Windows應用商店。如果無法將證書匯入到儲存區 ,AnyConnect客戶端將無法建立到ASA的SSL連線。

程式

若要將驗證憑證匯入Windows儲存區,請完成以下步驟:

1. 將elD插入讀卡器,然後啟動中介軟體以訪問elD卡的內容。此時將顯示elD卡的內容。

📫 Carte d'identité					
😑 🗖 🖨 🖬 🖨 🗶	Contraction and the second	Sector States States		Sector Contraction of	
Identité Certificats Carte & PIN Optio	ns Info			an a	12122
BELGIQUE	BELGIË	BELGIEN	BEL	GIUM	
CARTE D'IDENTITE	IDENTITEITSKAART	PERSONALAUSWEIS	IDEN	ITITY CARD	
	Identité				1
	Nom				
	Prénome				
	1 Persona				E
	Lieu de naissance	Date de naissance	Sexe	Nationalité	
	The	14/04/1963	M	be	
	The		63.04.14-033.25		
Carte	Adresse				
Numéro de la puce	Rue		122222337227223	000000000000000000000000000000000000000	
534C494E336600296CFF271507	182C36				
Numero de la carte 590.5942800.24	Code postal Commune	•		Pays	
Valide du Au	Statut spécial		000000000		
07/06/2007 07/06/2012	Canne blanche				
Commune d'émission	Canne jaune	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
	Minorité étendue				
			in a		
				Jan 1	
			24	and the	
				1	
				W & S NO	
Fini		and the second			

2. 按一下Certificates(FR)頁籤。將顯示證書層次結構。

📾 Carte d'identité		
6 🖸 🖙 🖬 🍪 🗙 Identité Certificats Carte & PIN Options Info		
Certificats		
BELPIC Belgium Root CA	Propriétaire	entication)
- Californic A	Citizen CA	
(Signature)	Longueur de clé 1024 bits	
	Valide du 15/06/2007	Au 08/06/2012
	Statut du certificat Non validé	
	Les certificats de la carte utiliser la carte d'identité OpenOffice.org. Adobe P sélectionnez-le et cliquez	eID doivent être enregistrés dans Windows pour pouvoir électronique dans Internet Explorer, Microsoft Office, leader, Outlook, Pour enregistrer un certificat, sur le bouton « Enregistrer ». <u>Enregistrer</u> <u>Détails >></u>
Fini		

- 3. 展開Belgium Root CA, 然後展開Citizen CA。
- 4. 選擇Authentication版本的指定證書。
- 5. 按一下Enregistrer(FR)按鈕。證書將複製到Windows應用商店。

註:單擊Details按鈕時**出現**一個視窗,顯示有關證書的詳細資訊。在詳細資訊頁籤中,選擇 Subject欄位以檢視Serial Number欄位。Serial Number欄位包含一個用於使用者授權的唯一值。例 如,序列號'56100307215"表示其出生日期為1956年10月3日的用戶,其序號為072,校驗位為15。 您必須提交聯邦當局的批准請求才能儲存這些號碼。您有責任就維護貴國比利時公民資料庫作出適 當的官方宣告。

驗證

:

若要確認憑證是否成功匯入,請完成以下步驟:

- 1. 在Windows XP電腦上,開啟DOS視窗,然後鍵入mmc命令。系統將顯示Console應用程式。
- 2. 選擇File > Add/Remove Snap-in (或按Ctrl+M)。將出現「新增/刪除管理單元」對話方塊。
- 3. 按一下Add按鈕。將出現「新增獨立管理單元」對話方塊。
- 4. 在可用獨立管理單元清單中,選擇證書,然後按一下新增。
- 5. 按一下**My user account**單選按鈕,然後按一下**Finish**。「證書」管理單元出現在「新增/刪除 管理單元」對話方塊中。
- 6. 按一下關閉以關閉「新增獨立管理單元」對話方塊,然後在「新增/刪除管理單元」對話方塊 中按一下確定,以儲存更改並返回到Console應用程式。
- 7. 在Console Root資料夾下,展開Certificates Current User。
- 8. 展開**Personal**,然後展開**Certificates**。匯入的證書必須出現在Windows應用商店中,如下圖所 示

🚡 Console1 - [Console Root\Certific	ates - Current User/Personal\Ce	rtificates]			X		
🚡 File Action View Favorites Wind	dow Help			_16	×		
Console Root	Issued To 🖉	Issued By	Expiration Date	Intended Purposes	Frier		
Certificates - Current User Personal Certificates Trusted Root Certification Author Enterprise Trust Intermediate Certification Author Active Directory User Object Trusted Publishers Untrusted Certificates Trusted People Other People Other Certificate Enrollment Requests	(Authentication)	Citizen CA	8/06/2012	Client Authentication	Clé c		
	<				>		
Personal store contains 1 certificate.							

<u>AnyConnect安裝</u>

必須在遠端PC上安裝AnyConnect客戶端。AnyConnect軟體使用可編輯的XML配置檔案,以預置可 用網關的清單。XML檔案儲存在遠端PC上的以下路徑中:

C:\Documents和設定\%USERNAME%\Application Data\Cisco\Cisco AnyConnect VPN客戶端

其中%USERNAME%是遠端PC上使用者的名稱。

XML檔案的名稱為preferences.xml。以下是檔案內容的範例:

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectPreferences> <DefaultHost>*192.168.0.1*</DefaultHost> </AnyConnectPreferences> 其中*192.168.0.1*是ASA網關的IP地址。

<u>ASA要求</u>

確保ASA滿足以下要求:

 AnyConnect和ASDM必須在快閃記憶體中運行。要完成本文檔中的步驟,請使用安裝了適當 ASA 8.0軟體的ASA 5505。必須在快閃記憶體中預載入AnyConnect和ASDM應用程式。使用 show flash命令以檢視flash:的內容

ciscoasa#**show flash:**

67 6889764 Jun 26 2007 10:25:28 asdm-602.bin

68 2635734 Jul 09 2007 07:37:06 anyconnect-win-2.0.0343-k9.pkg

 ASA必須使用出廠預設設定運行。如果您使用新的ASA機箱來完成本文檔中的步驟,則可以跳 過此要求。否則,請完成以下步驟,將ASA重置為出廠預設值:在ASDM應用中,連線到
 ASA機算,就要求

ASA機箱,然後選擇File > Reset Device to the Factory Default Configuration。

1 (isco ASDM 6.0 for ASA - 192.16	8,100,2	54										- 2
File	View Tools Wizards Window	Help						Look P	lor:		Find -	aha	h.,
	Refresh ASDM with the Running Config	puration on	the De	vice ES	Back	Forwar	nd 🤣 Helt					CISC	0
i.	Reset Device to the Factory Default Co	onfiguration	n.	noonnioettine.									0
	Show Running Configuration in New Wi	indow			Frewal	Dashboard	CONTRACTOR						
	Save Running Configuration to Flash			<u>C</u> trl+S					Inte	eface O abus			-
	Save Running Configuration to TFTP Se	erver			1.10				Inte	where status	ID Address/Mask	Line	
	Save Running Configuration to Standby	y Unit							I insid	de la	192.168.100.254/24	Q up	1
	Save Internal Log Buffer to Flash				isco.be				outs	side	192.168.0.1/24	🙂 down	
	Print			OrleP	1.1	Device Upti	ne: Od Oh 1-	im 21s					
	Clear ASDM Carbo			-	1.1	Context Mo	i: ASA 554	15					
	Clear Internal Los Buffer					Total Memo	v: 256 MB						
	E-A	-		Abulia					Sele	ct an interface	to view input and outp	ut Kbps	
	EXE		Turner	Picter a	Transfer of				Test	for Chalans			
		WE .	runne	Dear: 0	and	Harr CO UDAL	0 00	UDM Chards 0	Ira	Inc status	farmed the sea		
		are		1730C: 0	Client	0010 3.34 TPTE	0 35	C THIS CIEFC: 0	Lo	nnections re	Second Usage		
		Sys	tem Re	esources Statu	s				-				
		CPI		CPU Usage (p	ercent)				- 1				
				20				N	0				_
				10					-	22	47 22:48	22:40	
										00P: 0	1CP: 0 1008c 1	,	
		22.6	3.02		22:47	22:48	22:40	22:50 2	2.5 '04	Aside' Interfa	ice Traffic Usage ()	(bps)	
		Me	mory	Memory Usag	e (MD)								
				200					0				
		10 10	495	100						00	:56 00:57	00:58	
				0								is down.	8
		Latest	ASDM	Syslog Messa	oes							000	×
		Sevenity	/ Date	Time	Sy	slog ID Sou	rce IP	Destination IP	Description				
		4.6	34.5	6 2007 22:5	1:07 10	6015 192	.168.100.100	192.168.100.254	Deny TCP (no	connection) fro	m 192.168.100.100/1	114 to 19; •	
		4.6	342	6 2007 22:5	1:07 30	2014 192	.168.100.100	192.168.100.254	Teardown TCI	P connection 34	for inside:192.168.10	0.100/111	
		4.6	20.2	6 2007 22:5	1:07 10	192	168.100.100	192.168.100.254	Deny TCP (no	connection) fro	m 192.168.100.100/1	113 to 190	0
		4.0	10.0	0 2007 22:5	107 30	2017 192	108.100.100	192-100-100-254	reardown TO	e connection 33	LOL 10306:137-108-10	N.100/111 V	-
-									-				-

在模板中保留預設值。將您的PC連線到Ethernet 0/1內部介面,並續訂由ASA的DHCP伺服器調 配的IP地址。注意:要從命令列將ASA重置為出廠預設值,請使用以下命令: ciscoasa#conf t

ciscoasa#config factory-default 192.168.0.1 255.255.255.0

<u>ASA配置</u>

重置ASA出廠預設設定後,可以將ASDM啟動到192.168.0.1,以便連線到Ethernet 0/1內部介面上的ASA。

注意:您以前的密碼將被保留(或者預設情況下可以為空)。

預設情況下,ASA接受源IP地址在子網192.168.0.0/24中的傳入管理會話。在ASA內部介面上啟用 的預設DHCP伺服器提供192.168.0.2-129/24範圍內的IP地址,這些地址對於通過ASDM連線到內部 介面有效。

完成以下步驟以配置ASA:

- 1. <u>啟用外部介面</u>
- 2. 配置域名、密碼和系統時間
- 3. 在外部介面上啟用DHCP伺服器
- 4. 配置eID VPN地址池

- 5. <u>匯入比利時根CA證書</u>
- 6. 配置安全套接字層
- 7. 定義預設組策略
- 8. <u>定義證書對映</u>
- 9. 新增本地使用者
- 10. <u>重新啟動ASA</u>

步驟1.啟用外部介面

此步驟說明如何啟用外部介面。

- 1. 在ASDM應用程式中,按一下Configuration,然後按一下Device Setup。
- 2. 在Device Setup區域中,選擇Interfaces,然後按一下Interfaces頁籤。

📬 Cisco ASDM 6.0 for ASA - 192.168.0.1							
File View Tools Wizards Window Help			Look F	lor:		Find	ababa
Home Configuration Monitoring Sa	ve 🔇 Refresh 🔇 Bi	sck 🔘 Forward 🐴	? Неір				CISCO
Device List c ² P × Configural	ion > Device Setup > Inte	erfaces					0
Add Delete S Connect Interface	5 Switch Ports						
Name Name	Switch Ports	Enabled Se	curity IP Address	Subnet Mask	Restrict	VLAN	
inside	Ethernet0/1, Ethernet0/	2, Et Yes	100 192.168.0.1	255.255.255.0	THE IS NOT	viant	
outside	Ethernet0/0	Yes	0 197.0.100.1	255.255.255.0		vlan2	EdR
							Delete
Benire Setup							
g ⁹ Sartup Weard							
W +3+ Reuting							
Pervice Name/Pessword							
🗷 🧿 System Time							
0							
By Device setup							
Strewal							
Remote Access VPN							
Cal State State	traffic between two or mo	re interfaces which are	configured with same sec	urity levels			
Enable	traffic between two or mo	re hosts connected to t	the same interface				
Device Management							
5			Apply Re	set			
Device configuration loaded successfully.			<admin></admin>	15	I II I	1 20	/07/07 8:35:14 UTC

- 3. 選擇外部介面,然後按一下Edit。
- 4. 在General頁籤的IP address部分,選擇Use Static IP選項。
- 5. 輸入197.0.100.1作為IP地址, 255.255.255.0作為子網掩碼。
- 6. 按一下「Apply」。

步驟2.配置域名、密碼和系統時間

此步驟說明如何配置域名、密碼和系統時間。

1. 在Device Setup區域中,選擇Device Name/Password。

🔂 Cisco ASDM 6.0 for ASA - 192.168	10.1 ·····	
File View Tools Wizards Window H	look For: Find -	ababa
Home Configuration D Monitor	ing 🔚 Save 🚱 Refresh 🔇 Back 🚫 Forward 🥜 Help	CISCO
Device List d P ×	Configuration > Device Setup > Device Name/Password	0
Add Delete S Connect	Hostname and Domain Name	
BP 192210 MAT	Mostname: ciscoasa	
	Domain Name: cisco.be	
	Enable Password	
	Change the privleged mode password.	
Device Setup	Old Password:	
9 ⁹ Startup Wizard	New Password: *******	
Interfaces	Confirm New Password: *******	
Privice Name/Password		
🛞 🧿 System Time	Telnet Password	
	Change the password to access the console or the security appearce.	
	Old Password:	
	New Password:	
	Confirm New Password:	
Q Design Setting		
OP Center Seats		
🕄 Frewal		
Remote Access VPN		
Ste-to-Site VPN		
Device Management		
:	Apply Reset	
Device configuration loaded successfully.	<admin> 15 🔯 🛃 🔂 27</admin>	/07/07 8:36:04 UTC

- 2. 輸入cisco.be作為域名,輸入cisco123作為啟用密碼值。注意:預設情況下,密碼為空。
- 3. 按一下「Apply」。
- 4. 在Device Setup區域中,選擇**System Time**,然後更改時鐘值(如有必要)。
- 5. 按一下「Apply」。

步驟3.在外部介面上啟用DHCP伺服器。

此步驟描述如何在外部介面上啟用DHCP伺服器以便進行測試。

- 1. 按一下Configuration,然後按一下Device Management。
- 2. 在Device Management區域中,展開DHCP,然後選擇DHCP Server。

G Cisco ASDM 6.0 for ASA - 192.168	.0.1			· · · · · ·			
File View Tools Wizards Window He	dp		Look	For:		Find -	alada
Home 🔏 Configuration 📴 Monitori	ng 🔚 Save 💽 Refresh	🔆 Back 🚫 Forward 💡 He	p				cisco
Device List d P ×	Configuration > Device Man	agement > DHCP > DHCP Server					
◆ Add ① Delete ∅ Connect	Interface DHCP Enabled Inside Yes outside Yes	Address Pool 192.168.0.2 - 192.168.0.129 197.0.100.20 - 197.0.100.30	DNS Servers	WINS Servers	Domain Name	Ping Timeout Lu	Edk
Device Management Provide Management Access Provide System Image/Configuration Provide System Imag	Clobal DHCP Options Clobal DHCP Options Chable auto-configuration take precedence over the a DNS Server 1: DNS Server 2: Domain Name:	on from interface: Outs	Allow VPN override ally configure DNS Server: 25 Server:	, WINS and the d	efault domain na	me. The values in th	ve fields below
9	Lease Length:	secs					
Device Setup Proval Proval	Ping Timeout:	DMCD Conver				C	Advanced
Remote Access VPN Ret-to-Site VPN Device Management	Update DNS Settings for	s Override Client Settings	Aoply R	eset			
Running configuration successfully saved to flas	sh memory.		<admin></admin>	15		🗎 🗋 Z	7/07/07 8:48:04 UTC

- 3. 從Interface清單中選擇外部介面,然後按一下Edit。系統將顯示Edit DHCP Server對話方塊。
- 4. 選中Enable DHCP Server覈取方塊。
- 5. 在DHCP地址池中,輸入從197.0.100.20到197.0.100.30的IP地址。
- 6. 在Global DHCP Options區域中,取消選中Enable auto-configuration from interface覈取方塊
- , 7. 按一下「Apply」。

步驟4.配置elD VPN地址池

此步驟描述如何定義用於調配遠端AnyConnect客戶端的IP地址池。

- 1. 按一下Configuration,然後按一下Remote Access VPN。
- 2. 在Remove Access VPN區域中,展開**Network(Client)Access**,然後展開**Address** Assignment。
- 3. 選擇Address Pools,然後按一下Configure named IP Address pools區域中的Add按鈕。系統 將顯示Add IP Pool對話方塊。

GC Cisco ASDM 6.0 for ASA - 192.168	.0.1					
File Wew Tools Wizards Window He	þ			Look For:	Find +	advada.
Home 🔓 Configuration 📴 Monitori	ng 🔚 Save 🔇 Refrest	h 🚫 Back 🔘 Forwa	a 🦿 Help			cisco
Device List d ^a P ×	Configuration > Remote a	Access VPN > Hetwork (Client) Access > Add	tress Assignment >	Address Pools	
Add 👔 Delete 🔊 Connect	Configure named IP Addr	ess pools.				
192.160.0.1	This assumption is and one	ad in address a 19761 Wasse and			and a star coefficienties	
	ins parameter is enroro	ed in eicher a vers proc.com	recomprone, 22, 19	A CONTRECTOR DEGENO	Construction Construction	
	◆ Add @ Edt @ 0	elste				
	Pool Name	Starting Address		Ending Address	Subnet Mask	
Remote Access VPN 🗗 🔍 🗙	S 50	Add IP Pool		×		
🖃 🗃 Network (Client) Access 🔺						
SSL VPN Connection Profiles						
Prec Connection Profiles			-muntered			
Do Dynamic Access Policies		Name:	elb-whwoor			
Address Assignment			100 140 10 100			
Assignment Policy		Starting IP Address:	192.168.10.100	1999		
Address Pools			100 140 10 110			
Martinee SD VSN Access	to an an an and the	Ending IP Address:	192.160.10.110			
Callerous Jok Thin Access						
🗄 🖌 AAA Setup		SUDNER Mask:	10.00.00.0			
🗄 👸 Secure Desktop Manager 🛛 🚽						
Certificate Management						
f DHCP Server				_		
S Denire Setur			Cancel Help			
De France State						
Frowal						
Remote Access VPN						
Ste-to-Site VPN						
Device Management						
5			Apply.	Reset		
			< a	tmin> 15	😡 🔐 🛛 🙆 2	7/07/07 8:53:04 UTC

- 4. 在「名稱」欄位中,輸入eID-VPNPOOL。
- 5. 在Starting IP Address(起始IP地址)和Ending IP Address(結束IP地址)欄位中,輸入從 192.168.10.100到192.168.10.110的IP地址範圍。
- 6. 從Subnet Mask下拉選單中選擇255.255.255.0,按一下OK,然後按一下Apply。

步驟5.匯入比利時根CA證書

此步驟說明如何將比利時根CA證書匯入ASA。

- 1. 從政府網站下載並安裝比利時根CA證書(belgiumrca.crt和belgiumrca2.crt),並將其儲存在本地PC上。比利時政府網站位於以下網址:<u>http://certs.eid.belgium.be/</u>
- 2. 在Remote Access VPN區域中,展開Certificate Management,然後選擇CA Certificates。
- 3. 按一下Add,然後按一下Install from file。
- 4. 瀏覽到儲存比利時根CA證書(belgiumrca.crt)檔案的位置,然後按一下Install Certificate。
- 5. 按一下「Apply」以儲存變更內容。
- 此圖顯示ASA上安裝的證書:



步驟6.配置安全套接字層

此步驟描述如何區分安全加密選項的優先順序、定義SSL VPN客戶端映像和定義連線配置檔案。

 優先使用最安全的加密選項。在Remote Access VPN區域中,展開Advanced,然後選擇SSL Settings。在Encryption部分中,按如下方式自上而下堆疊活動演算法:AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1

Gisco ASDM 6.0 for ASA - 192.168	8.0.1	an an an that the set of a state of the set of		
File View Tools Wizards Window H	telp		Look Por: Frid	alada
Home 🖧 Configuration 🗾 Monitor	ring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Form	nd 🦿 Help	and a second	cisco
Device List d ¹ # ×	Configuration > Remote Access VPH > Advanced	t > SSL Settings		0
◆ Add 1 Delete Ø Connect	Configure SSL parameters. These parameters affect I	ooth ASDM and SSL VPN acco	55.	
	Server SSL Version: 14/1/	e version: veria		
	Encryption			
	Available Algorithms	Add >>	Active Algorithms	Move Up
	RC4-MD5		AES256-5HA1	
	DES-SHA1	<< Remove	AES128-SHA1	Move Down
Remote Access VPN D Q ×		a start of the start of the	30E5-SHA1	1.
Clentless SSL VPN Access			RC4/SHA1	
Sa Easy VPN Remote			L	
B M AAA Setup	Certificates			
Secure Desizop Manager Certificate Manager	Specify which certificates, if any, should be used for	s SS, authentication on each	interface. The failback certificate will be used on inter	faces not
PDHCP Server	associated with a certificate of their own.			
A DNS	Technology	ID Continue		
Advanced	Uncertace locide	10 Ceronicao	0	EdR
Connection Gateway	outside			
SSL Settings				
Certificate to SSL VPN Conne				
HTTP Redrect				
Maximum SSL VPN Sessions				
🗈 🦉 E-mail Proxy 💉				1.100000.0000
<				
A Device Setup				
🖏 Firowal				
Remote Access VPN				
Ste-to-Site VPN				
Device Management	Esliharis Castilizatas (hinn			
ŝ		Apply	Reset	
Running configuration successfully saved to fla	ish memory.	<sdmin< td=""><td>> 15 😡 🔐 健</td><td>27/07/07 8:57:34 UTC</td></sdmin<>	> 15 😡 🔐 健	27/07/07 8:57:34 UTC

2. 為AnyConnect客戶端定義SSL VPN客戶端映像。在Remote Access VPN區域中,展開 Advanced,展開SSL VPN,然後選擇Client Settings。在SSL VPN Client Images區域中,按 一下Add。選擇儲存在快閃記憶體中的AnyConnect軟體包。AnyConnect軟體包出現在SSL VPN客戶端映像清單中,如下圖所示

:

📫 Cisco ASDM 6.0 for ASA - 192.	168.100.254						
File View Tools Wizards Window	Help Look For: Find	ahaha					
Home Configuration 🕖 Mo	🔥 Home 🥰 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦿 Help						
Device List ♂ ♀ ×	Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings	0					
🗣 Add 📋 Delete 🖋 Connect	Identify SSL VPN Client (SVC) related files.						
A 192.168.0.1	EEL VID Flient Images						
B1192100100254	Mininge connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.						
	A Add T Declara 1 Calde + Mount O. J. Mount Press						
	dskuljanycomectivani z JUUSISHSLprg						
Remote Access VPH GP 9 ×							
Network (Client) Access							
SSL VPN Connection Profiles							
Group Policies							
Dynamic Access Policies	SSL VPN Client Profiles						
B S. Address Assignment	4 44 BT 570 B 1000						
Address Pools							
😑 🐯 Advanced	Name Package						
A Endpoint Security							
Clent Settings							
Bypass Interface Ac							
a ug Psec M							
Device Setup							
🕄 Firewal	SSL VPN Client Localization File						
Remote Access VPN	To set the Localization file go to Language Localization,						
Ste-to-Site VPN	Cache File System (to hold CSD and SVC images)	-					
Device Management	Meximum Szer: 20 MB						
5	Apply Reset						
	<admin> 15 🔯 🔂 🔂 25(0</admin>	17/07 23:20:54 UTC					
🌆 start 🔰 🔟 🕹 🐵 😣	🚳 🦈 🔁 9 wind + 🛐 2002ino 🔯 Cilwillio 😭 Caso AS 🏪 2 Infan + 💽 TestPad 🤇	S 12 - 10-09					

3. 定義DefaultWEBVPNGroup連線配置檔案。在Remote Access VPN區域中,展開 Network(Client)Access,然後選擇SSL VPN Connection Profiles。在Access Interfaces區域中 ,選中Enable Cisco AnyConnect VPN Client覈取方塊。對於外部介面,請選中Allow Access、Require Client Certificate和Enable DTLS覈取方塊,如下圖所示

Cisco ASDM 6.0 for ASA - 192.168	.100.254					
File View Tools Wizards Window H	elp		And the second second	Look For:	Find +	de de
Home 🔏 Configuration [Honitori	ng 🔚 Save 💽 F	tefresh 🔇 Back 🔇	Porward ? Help			cisco
Device List of A ×	Configuration > Res	note Access VPH > Ne	twork (Client) Access > SSL	VPN Connection Profile	5	0
🗣 Add 📋 Delete 🚿 Connect	The security applie	nce automatically deploy	s the Cisco AnyConnect VPN Cle	ent or legacy SSL VPN Client	to remote users upon connection.	The initial client
192.168.0.1 192.168.100.254	deployment requin Security (DTLS) tu	es end-user administrativ meling options.	e rights. The Cisco Any Connect	VPN Client supports the HT	IPS/TCP (SSL) and Datagram Trans	port Layer
	(More client-relate	d parameters, such as d	ient images and client profiles, c	an be found at Serie Serie	2.)	
	Access Interfaces					
Remote Access VPN @ Q ×	Enable Osco A	wConnect VPN Client or	legacy SSL VPN Client access on	the interfaces selected in t	he table below	
B Network (Client) Access	Contraction Contraction	18	Designed Classic Contribution	Paula Pric	7	
SS. VPN Connection Profiles	Interface	Allow Access	Require Client Certificate	Enable DTLS		
IPsec Connection Profiles	inside	ñ	ň			
Group Policies						
Address Assignment						
Advanced						
Clentless SSL VPN Access	Access Port: 443	DTLS Port	443			
Connection Profiles						
Portal	Click here to Assis	n Certificate to Interface	 March 1997 			
De Dupanic Access Dolicies						
Advanced	Connection Profile	5				
Encoding 🖌	Connection profile	(tunnel group) table belo	w contains records that determine	ne connection policies. A re	cord identifies a default group polic	y for the
C interesting and the second second	connection and co	itains protocol-specific co	nnection parameters.			
0	💠 Add 🛃 Edit	Delete				
Device Setup	Name	Alases	SSL VPN C	Client Protocol	Group Policy	
Preval	DefaultWEBVPNG	oup	Enabled		OfItGypPolicy	
63.1	DefaultRAGroup		Enabled		DritGrpPolicy	
Remote Access VFN						
Ste-to-Site VPN						
Device Management	Allow user to s	elect connection. idenitifi	ed by alias in the table above. a	it loain page		
:			Apply	Reset		
			<ac< th=""><th>śmin> 15</th><th>😡 🚱 🔰 🙆 🗃</th><th>(07)07 0:20:25 UTC</th></ac<>	śmin> 15	😡 🚱 🔰 🙆 🗃	(07)07 0:20:25 UTC

在「連線配置檔案」區域中,選擇**DefaultWEBVPNGroup**,然後按一下**Edit**。系統將顯示Edit SSL VPN Connection Profile對話方塊。

٦	🕯 Edit SSL VPN Connecti	on Profile: DefaultWEE	WPNGroup	
	Basic	Name: Aliases:	DefaultWEBVPNGroup	
		Authentication		
		Method:	🔿 AAA 💿 Certificate 🔵 Both	
		AAA Server Group:	LOCAL	Manage
			Use LOCAL if Server Group fails	
		Client Address Assigne	ent	
		DHCP Servers:		
		Client Address Pools:		Select
		Default Group Policy -		
		Group Policy:	DfltGrpPolicy	Manage
		SSL VPN Client Protocol:	C Enabled	
		OK	Cancel Help	

在導航區域中,選擇**Basic**。在Authentication區域中,按一下**Certificate**單選按鈕。在Default

Group Policy區域中,選中SSL VPN Client Protocol復選框。展開Advanced,然後選擇 Authentication。按一下Add,然後使用本機伺服器群組新增外部介面,如下圖所示

Edit SSL VPN Connecti	ion Profile: Default)	WEBVPNGroup	2 Versenaan van de seeren een een de seeren de see	X
Basic	Interface-Specific /	Authentication Server Group	35	
General	🗣 Add 🗹 Edit	📋 Delete		
Client Addressing	Interface	Server Group	Fallback to LOCAL	
Authentication	outside	LOCAL		
Authorization				
SSL VPN				
	ОК	Cancel Hel	q	

在導航區域中,選擇Authorization。在Default Authorization Server Group區域中,從Server Group下拉選單中選擇LOCAL,並選中Users must exist in the authorization database to connect復選框。在User Name Mapping區域中,從Primary DN Field下拉選單中選擇SER(Serial Number),從Secondary DN Field中選擇None,然後按一下OK。

📫 Edit SSL VPN Connecti	on Profile: DefaultWEBVPNGroup	×
Basic Advanced General Client Addressing Authentication Authorization Accounting SSL VPN	Default Authorization Server Group Server Group: LOCAL Image: Image: Interface-specific Authorization Server Groups Add Edt Image:	
	Interface Server Group	
	User Name Mapping Use the entire DN as the username Specify individual DN fields as the username Primary DN Field: SER (Serial Number) Secondary DN Field: None	
	OK Cancel Help	

步驟7.定義預設組策略

此步驟說明如何定義預設組策略。

1. 在Remote Access VPN區域中,展開**Network(Client)Access**,然後選擇**Group Policies**。

🖆 Cisco ASDM 6.0 for ASA - 192.168	.0.1				
File View Tools Wizards Window He	elp		Look For:	Find -	ahaha
Home 🖧 Configuration 🔀 Monitori	ng 🔚 Save 🔇 Refresh 🔇 Ba	ick 🔘 Forward 🧳 He	þ		cisco
Device List on P ×	Configuration > Remote Access Vi	PN > Network (Client) Acc	ess > Group Policies		
Add T Delete S Connect	Manage VPN group policies. A VPN g	roup policy is a collection of u	ser-oriented attribute/value pairs that m	ay be stored internally on the de	vice or
Sector and the sector of the s	A Add - T Edt T Takes	 The group policy informatic 	n is referenced by 1991 tunnel groups an	d user accounts.	
	Name	Ture	Turnaling Destand	AAA Server Group	
	DfRGrpPolicy (System Default)	Internal	L2TP-IPSec, svc, IPSec, webvpn	N/A	
Remote Access VPN & Q ×					
Retwork (Client) Access					
IPsec Connection Profiles					
Group Policies					
Address Assignment					
Gentless SS. VPN Access					
Easy VPN Remote					
AAA Setup Secure Desktop Manager					
Certificate Management Child Service					
A DNS					
Advanced					
Revice Setup					
🚱 Frewal					
Remote Access VPN					
Ste-to-Ste VPN					
Device Management					
t			Apply Reset		
		and the second second	cadmin> 15	27	07/07 15:23:14 UTC

2. 從組策略清單中選擇**DfltGrpPolicy**,然後按一下**Edit**。 3. 系統將顯示Edit Internal Group Policy對話方塊。

🚳 Edit Internal Group Po	licy: DfltGrpPolicy		8
General	Name: Dfito		
Advanced Split Tunneling IE Browser Proxy SSLVPN Cleant	Banner: Address Pools: eI	D-VPNPOOL	Select
Login Setting Key Regeneration	More Options	: Clientless SSI VPN Z SSI VPN Client D IPser	
Customization	Filter:	None	Manage
	NAC Policy: Access Hours:	None	Manage
	Simultaneous Logins	81 3	
	Restrict access to V Maximum Connect T	LAN: Unrestricted ime: Unlimited minutes	
	Idle Timeout:	Unlimited 30 minutes	
	ОК	Cancel Help	

- 4. 在導航區中選擇General。
- 5. 對於地址池,按一下Select以選擇地址池,然後選擇elD-VPNPOOL。
- 6. 在「更多選項」區域中,取消選中IPsec和L2TP/IPsec覈取方塊,然後按一下OK。

步驟8.定義憑證對應

此步驟描述如何定義證書對映條件。

- 1. 在Remote Access VPN區域中,按一下Advanced,然後選擇Certificate to SSL VPN Connection Profile Maps。
- 在Certificate to Connection Profile Maps區域中,按一下Add,然後從對映清單中選擇 DefaultCertificateMap。此對映必須與Mapped to Connection Profile欄位中的 DefaultWEBVPNProfile匹配。
- 3. 在「對映條件」區域中,按一下新增,然後新增以下值:欄位:簽發人,國家(地區),等於 ,「be」欄位:頒發者,公用名(CN),等於,「公民ca」對映條件應如下圖所示
 - 🔀 Cisco ASDM 6.0 for ASA 192,168,100,254 File View Tools Wizards Window Help Look For: Home 🔏 Configuration 📴 Monitoring 🥁 Save 🔇 Refresh 🔇 Back 🚫 Forward 🤗 Help cisco d + × Configuration > Remote Access VPN > Advanced > Certificate to SSL VPN Connection Profile Mag Add 📋 Delete 🚿 Connect Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together with their 192.168.0.1 matching criteria for the selected rule. 192.168.100.254 **Certificate to Connection Profile Maps** I Add 🛃 Edit 📋 Delete Rule Priority Mapped to Connection Profile Map Name temote Access VPN d + × Certificate Management CA Certificates Code Signer P DHCP Server DNS Mapping Criteria Advanced 🗣 Add 💽 Edit 📋 Delete SSL Settings Field Component Operator Value Country (C) Equals HTTP Redirect Maximum SSL VPN Sessions E-mail Proxy A Device Setup Frewal Remote Access VPN Ste-to-Site VPN Device Management Reset 🐻 🚱 🔂 configuration changes saved successfully 25/07/07 23:20:54 UTC <admin > 15
- 4. 按一下「Apply」。

步驟9.新增本地使用者

此步驟說明如何新增本地使用者。

- 1. 在Remote Access VPN區域中,展開AAA Setup,然後選擇Local Users。
- 2. 在「本地使用者」區域中,按一下新增。
- 3. 在Username欄位中,輸入使用者證書的序列號。例如,56100307215(如本檔案的<u>驗證憑證</u>一

節所述)。

📫 Cisco ASDM 6.0 for ASA - 192.168.	100.254					
File View Tools Wizards Window He	b			Look For:	Find +	ahaha
Home Configuration D Monitorin	ng 🔚 Save 🔇	Refresh 🔇 Back 🔘 Fi	rward 🦻 Help			cisco
Device List a P ×	Configuration > R	emote Access VPH > AAA S	ietup > Local Users			0
Add Delete S Connect	Create entries in	the ASA local user database.				
192.168.100.254	Command autho	rization must be enabled in ord	er for the user account privile	ges to be enforced. To enable	command authorization, go to	Duthorization.
	AAA authentical	ion console commands must be	enabled in order for certain a	ccess restrictions to be enfor	ed. To enable AAA authentica	ation command
	go to Authentica	<u>100</u> ,				
	Username	Privilege Level (Role)	Access Restrictions	VPN Group Policy	VPN Group Lock	Add
Remote Access VPN d P ×	enable_15 63041403325	15	Full Full	N/A	N/A	E.te
Application Helper		-				
+2+ Web ACLs						Delete
G Easy VPN Remote						
AAA Setup						
LDAP Attribute Map						
Cocal Users						
Certificate Management						
P DHCP Server						
Advanced						
+5+ Connection Gateway						
<						
Bevice Setup						
Firewal						
Remote Access VPN						
Ste-to-Ste VPN						
Device Management						
:			Apply	Reset		
Running configuration successfully saved to flash	h memory.		<adm< td=""><td>in> 15</td><td>2 🚰 🚺 🙆 2</td><td>6/07/07 0:22:25 UT</td></adm<>	in> 15	2 🚰 🚺 🙆 2	6/07/07 0:22:25 UT

4. 按一下「Apply」。

步驟10.重新啟動ASA

重新啟動ASA以確保所有更改都應用到系統服務。

<u>微調</u>

測試時,某些SSL隧道可能無法正確關閉。由於ASA假定AnyConnect客戶端可能會斷開連線並重新 連線,因此不會丟棄隧道,從而有機會返回。但是,在使用基本許可證(預設情況下為2個SSL隧道)進行實驗室測試期間,如果未正確關閉SSL隧道,則可能會用完您的許可證。如果發生此問題 ,請使用**vpn-sessiondb logoff <***option>***命令註銷所有活動的SSL會話**。

<u>一分鐘配置</u>

為了快速建立工作配置,請將ASA重置為出廠預設設定,然後在配置模式下貼上此配置:

ciscoasa
ciscoasa# conf t
ciscoasa# clear configure all
ciscoasa# domain-name cisco.be
ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted
!
interface Vlan1

nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 interface Vlan2 nameif outside security-level 0 ip address 197.0.100.1 255.255.255.0 interface Ethernet0/0 switchport access vlan 2 no shutdown interface Ethernet0/1 no shutdown ! passwd 2KFQnbNIdI.2KYOU encrypted dns server-group DefaultDNS domain-name cisco.be ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110 mask 255.255.255.0 asdm image disk0:/asdm-602.bin no asdm history enable global (outside) 1 interface nat (inside) 1 0.0.0.0 0.0.0.0 dynamic-access-policy-record DfltAccessPolicy http server enable http 192.168.0.0 255.255.255.0 inside crypto ca trustpoint ASDM_TrustPoint0 enrollment terminal crl configure crypto ca certificate map DefaultCertificateMap 10 issuer-name attr c eq be issuer-name attr cn eq citizen ca crypto ca certificate chain ASDM_TrustPoint0 certificate ca 580b056c5324dbb25057185ff9e5a650 30820394 3082027c a0030201 02021058 0b056c53 24dbb250 57185ff9 e5a65030 0d06092a 864886f7 0d010105 05003027 310b3009 06035504 06130242 45311830 16060355 0403130f 42656c67 69756d20 526f6f74 20434130 le170d30 33303132 36323330 3030305a 170d3134 30313236 32333030 30305a30 27310b30 09060355 04061302 42453118 30160603 55040313 0f42656c 6769756d 20526f6f 74204341 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101 00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d c720eb30 915a75f5 e2d2cfc8 4c149842 58adc711 c540406a 5af97412 2787e99c e5714e22 2cd11218 aa305ea2 21b9d9bb fff674eb 3101e73b 7e580f91 164d7689 a8014fad 226670fa 4b1d95c1 3058eabc d965d89a b488eb49 4652dfd2 531576cb 145d1949 b16f6ad3 d3fdbcc2 2dec453f 093f58be fcd4ef00 8c813572 bff718ea 96627d2b 287f156c 63d2caca 7d05acc8 6d076d32 be68b805 40ae5498 563e66f1 30e8efc4 ab935e07 de328f12 74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf 6ce3841d de872e33 0b3c74e2 21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b a7210687 1d27d3c4 a1c94cb0 6f020301 0001a381 bb3081b8 300e0603 551d0f01 01ff0404 03020106 300f0603 551d1301 01ff0405 30030101 ff304206 03551d20

043b3039 30370605 60380101 01302e30 2c06082b 06010505 07020116 20687474 703a2f2f 7265706f 7369746f 72792e65 69642e62 656c6769 756d2e62 65301d06 03551d0e 04160414 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609 60864801 86f84201 01040403 02000730 1f060355 1d230418 30168014 10f00c56 9b61ea57 3ab63597 6d9fddb9 148edbe6 300d0609 2a864886 f70d0101 05050003 82010100 c86d2251 8a61f80f 966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59 48a74c49 37d773a1 6a01655e 32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9 5d0f37ba 76d240bd cc2d3fd3 4441499c fd5b29f4 0223225b 711bbf58 d9284e2d 45f4dae7 b5634544 110d2a7f 337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1 60f2d787 f6572e7a 7e6a1380 1ddce3d0 631e3d71 31b160d4 9e08caab f094c748 755481f3 1bad779c e8b28fdb 83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636 ba218c97 1a21d4ea 2d3bacba eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297 fff26e87 7d46c974 d6efeb3d 7de6596e 069404e4 a2558738 286a225e e2be7412 b004432a quit no crypto isakmp nat-traversal ! dhcpd address 192.168.0.2-192.168.0.129 inside dhcpd enable inside dhcpd address 197.0.100.20-197.0.100.30 outside dhcpd enable outside 1 service-policy global_policy global ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4sha1 ssl certificate-authentication interface outside port 443 webvpn enable outside svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1 svc enable certificate-group-map DefaultCertificateMap 10 DefaultWEBVPNGroup group-policy DfltGrpPolicy attributes vpn-tunnel-protocol svc webvpn address-pools value eID-VPNPOOL username 63041403325 nopassword tunnel-group DefaultWEBVPNGroup general-attributes authentication-server-group (outside) LOCAL authorization-server-group LOCAL authorization-required authorization-dn-attributes SER tunnel-group DefaultWEBVPNGroup webvpn-attributes authentication certificate exit copy run start



- <u>Cisco PIX防火牆軟體</u> <u>Cisco Secure PIX防火牆命令參考</u>
- 安全產品現場通知(包括PIX)
- <u>要求建議 (RFC)</u>
- <u>技術支援與文件 Cisco Systems</u>