# ل SCEP ليجست نيوكت لااثم SCEP ل AnyConnect

### المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> معلومات أساسية <u>نظرة عامة على التغييرات المطلوبة</u> إعدادات XML لتمكين ميزة SCEP في AnyConnect إحترار بروتوكول AnyConnect في AnyConnect إختبار بروتوكول SCEP ل AnyConnect بعد طلب SCEP تخزين الشهادة في Microsoft Windows بعد طلب SCEP معلومات ذات صلة معلومات ذات صلة

#### <u>المقدمة</u>

يتم إدخال وظيفة تسجيل SCEP في العميل المستقل AnyConnect 2.4. في هذه العملية، تقوم بتعديل ملف تعريف AnyConnect XML لتضمين تكوين مرتبط ب SCEP وإنشاء ملف تعريف اتصال ونهج مجموعة معين لتسجيل الشهادة. عندما يتصل مستخدم AnyConnect بهذه المجموعة المحددة، يرسل AnyConnect طلب تسجيل شهادة إلى خادم CA، ويقبل خادم CA الطلب أو يرفضه تلقائيا.

### <u>المتطلبات الأساسية</u>

#### <u>المتطلبات</u>

لا توجد متطلبات خاصة لهذا المستند.

#### <u>المكونات المستخدمة</u>

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- أجهزة الأمان القابلة للتكيف ASA 5500 Series من Cisco التي تشغل الإصدار x.8 من البرنامج
  - Cisco AnyConnect VPN، الإصدار 2.4

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

#### <u>الاصطلاحات</u>

راجع <u>اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.</u>

### <u>معلومات أساسية</u>

يتمثل الهدف من تسجيل SCEP التلقائي ل AnyConnect في إصدار شهادة إلى العميل بطريقة آمنة وقابلة للتطوير. على سبيل المثال، لا يحتاج المستخدمون إلى طلب شهادة من خادم CA. يتم دمج هذه الوظيفة في عميل AnyConnect. تصدر الشهادات إلى العملاء بناء على معلمات الشهادة المذكورة في ملف تعريف XML.

#### نظرة عامة على التغييرات المطلوبة

تتطلب ميزة تسجيل SCEP ل AnyConnect تحديد معلمات شهادة معينة في ملف تعريف XML. يتم إنشاء ملف تعريف "نهج المجموعة" و"الاتصال" في ASA لتسجيل الشهادة، ويقترن ملف تعريف XML بهذا النهج. يتصل عميل AnyConnect بملف تعريف الاتصال الذي يستخدم هذا النهج المحدد ويرسل طلبا للحصول على شهادة مع المعلمات المحددة في ملف XML. تقبل جهة منح الشهادة (CA) الطلب أو ترفضه تلقائيا. يسترجع عميل AnyConnect الشهادات باستخدام بروتوكول SCEP إذا كان عنصر <CertificateSCEP> محددا في ملف تعريف الع

يجب أن تفشل مصادقة شهادة العميل قبل أن يحاول AnyConnect إسترداد الشهادات الجديدة تلقائيا، لذلك إذا كان لديك شهادة صالحة مثبتة بالفعل، فلن يحدث التسجيل.

عند تسجيل دخول المستخدمين إلى مجموعة معينة، يتم تسجيلهم تلقائيا. هناك أيضا طريقة يدوية متاحة لاسترجاع الشهادة حيث يتم تقديم المستخدمين مع زر **الحصول على شهادة**. وهذا لا يعمل إلا عندما يكون لدى العميل وصول مباشر إلى خادم CA، وليس من خلال النفق.

راجع <u>دليل مسؤول عميل AnyConnect VPN، الإصدار 2.4 من Cisco</u> للحصول على مزيد من المعلومات.

## إعدادات XML لتمكين ميزة SCEP في AnyConnect

هذه هي العناصر المهمة التي يلزم تعريفها في ملف AnyConnect XML. راجع <u>دليل مسؤول عميل AnyConnect XML</u> V<u>PN، الإصدار 2.4 من Cisco</u> للحصول على مزيد من المعلومات.

- <AutoSCEPHost>—يحدد اسم مضيف ASA وملف تعريف الاتصال (مجموعة النفق) الذي تم تكوين إسترداد شهادة SCEP له. يجب أن تكون القيمة بتنسيق اسم المجال المؤهل بالكامل لاسم ملف تعريف ASA\Connection أو عنوان IP الخاص باسم ملف تعريف ASA\Connection.
  - <CAURL>–یحدد خادم SCEP CA.
  - <certificateSCEP>—يحدد كيفية طلب محتويات الشهادة.
  - <DisplayGetCertButton>—يحدد ما إذا كانت واجهة المستخدم الرسومية (GUI) ل AnyConnect تعرض الزر الحصول على الشهادة. وهو يمكن المستخدمين من طلب تجديد الشهادة أو توفيرها يدويا. . . . . . .

هنا مثال لملف تخصيص:

<sup>&</sup>lt;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/>
```

## تكوين ASA لدعم بروتوكول SCEP ل AnyConnect

من أجل توفير الوصول إلى سلطة تسجيل خاصة (RA)، يجب على مسؤول ASA إنشاء اسم مستعار يحتوي على قائمة التحكم في الوصول (ACL) التي تقيد اتصال الشبكة الجانبية الخاصة ب RA المرغوب. لاسترداد شهادة تلقائيا، يتصل المستخدمون بهذا الاسم المستعار ويصادقون عليه.

أكمل الخطوات التالية:

- 1. قم بإنشاء اسم مستعار على ASA للإشارة إلى المجموعة التي تم تكوينها بشكل محدد.
- 2. حدد الاسم المستعار في عنصر <AutomaticSCEPHost> في ملف تعريف العميل الخاص بالمستخدم.
- 3. قم بإرفاق ملف تعريف العميل الذي يحتوي على قسم <CertificateEnrollment> بالمجموعة المحددة التي تم تكوينها.
- 4. قم بتعيين قائمة تحكم في الوصول (ACL) للمجموعة التي تم تكوينها بشكل محدد لتقييد حركة المرور إلى RA الخاصة.

أكمل الخطوات التالية:

1. تحميل ملف تعريف XML إلى ASA.أخترت Remote Access VPN > شبكة (زبون) منفذ > متقدم > SSL

V**PN>زبون عملية إعداد**.تحت SSL VPN Client Profile، انقر فوق **إضافة**.انقر **تصفح الملفات المحلية** لتحديد ملف التخصيص، وانقر **تصفح Flash** لتحديد اسم ملف Flash.انقر فوق **تحميل** 

الملف.

Remote Access VPN 🔗 🏾 🖉 🖉	Configuration > Remote Access VPN > Ne	twork (Client) Access > Advanced > SSL VPN > Client Setting
Introduction     Network (Client) Access     AnyConnect Connection Profiles     IPsec Connection Profiles     Group Policies     AnyConnect Customization/Localization     Advanced     Advanced	Identify AnyConnect Client related files. AnyConnect Client Images The regular expression is used to match the u You can also minimize connection setup time to Add C Edit 1 Delete +	user-agent of a browser to an image. by moving the image used by the most commonly encountered operation
B- SAdvanced	Image	Regular expression to match user-agent
Clent Settings	SSL VPN Clent Profiles	Package
DHCP Server	Unload Package	
Advanced	Upload a file from local computer to I few minutes. Please wait for the ope Local File Path: cuments a Flash File System Path: disk0:/ac_s Upload Fi	fiash file system on the device. The upload process might take a sration to finish. nd Settings\asimalik\Desixtop\ac_scep Browse Local Files Ecp Browse Flash le Close Help

2. إعداد نهج مجموعة Certenroll لتسجيل الشهادة.أختر Remote Access VPN (**الوصول عن بعد) > Network (الوصول عن بعد) > Client Access (وصول عميل الشبكة) > Group Policy (نهج المجموعة**)، وانقر فوق Add.

🚰 Edit Internal Group Poli	icy: certenroll			
General Portal ⊕-More Options	Name: certenroll Banner: 🗹 Inherit			
	More Options			<u> </u>
	Tunneling Protocols:	📃 Inherit	Clientless SSL VPN 🕑 SSL V	PN Client 🔲 IPsec
	Web ACL:	🗹 Inherit		Manage
	Access Hours:	🖌 Inherit		Manage
	Simultaneous Logins:	🖌 Inherit		
	Restrict access to VLAN:	🖌 Inherit		~
	Connection Profile (Tunnel Group) Lock:	🗹 Inherit		~
	Maximum Connect Time:	🗹 Inherit	Unlimited minutes	
	Idle Timeout:	🗹 Inherit	Unlimited minutes	
Find:	Next @ Previ	ous		
	OK Can	iel 🗌	Help	

إضافة نفق انقسام لخادم CA.قم بالتوسيع **المتقدم**، ثم حدد **تقسيم الاتصال النفقي**.أختر **قائمة شبكات النفق أدناه** من قائمة النهج، وانقر فوق **إدارة** لإضافة قائمة التحكم في الوصول.

🚰 Edit Internal Group Pol	icy: certenroll		<b>X</b>				
General Servers	Split tunneling network lists tunneling. The security app of addresses on the private	distinguish networks that require traffic to go through t liance makes split tunneling decisions on the basis of a n a network.	he tunnel and those that do not require etwork list, which is an ACL that consists of list				
IE Browser Proxy	DNS Names: 🕑 Inherit						
SSL VPN Client — IPsec Client	Policy: 📃 Inherit	Tunnel Network List Below	×				
	Network List: 🔲 Inherit	scep	Manage				
	Intercept DHLP Conne	juration Message from Microsoft Clients	*				
Find:	Ne	xt 🔘 Previous					
	C	OK Cancel Help					
🔁 ACL Manager	r						
Standard ACL	Extended ACL						
🖶 Add 👻 🗹	Edit <u>î</u> Delete	≁ チ \$ @ @					
No Ad	dress	Action Descrip	otion				
Ģ∴scep							
1 🛃	10.11.11.0/24	🖌 Permit					
🖻 split							
1 🔳	10.1.1.11	🖌 Permit					
		- 1 11 <sup>4</sup> - 2 11 2 5 6 7 11 - 1					
			6				
<		illi	>				
			and Andrea				
	ОК	Cancel Help					

حدد SSL VPN Client، واختر ملف التعريف ل certenroll من قائمة **ملف تعريف العميل** ل**لتنزيل**.

Edit Internal Group Pol	licy: certenroll		
General	Keep Installer on Client System:	🔽 Inherit	🔿 Yes 🔹 No
Servers Advanced	Compression:	🖌 Inherit	C Enable C Disable
Spit Tunneing IE Browser Proxy	Datagram TLS:	🖌 Inherit	C Enable C Disable
SSL VPN Client	Keepalive Messages:	🔽 Inherit	Disable Interval: seconds
a short clout	MTU:	🔽 Inherit	
	Client Profile to Download:	🗌 Inherit	ac_scep V New
	Optional Client Modules to Download:	🖌 Inherit	· · · · · · · · · · · · · · · · · · ·

3. قم بإنشاء مجموعة أخرى تسمى **Certauth** لمصادقة الشمادة

General	Name: certauth	$\rightarrow$			
-Servers -Advanced	Banner: 🗹 Inherit				
	Address Pools: 🔽 Inherit		Sele	et	
	IPv6 Address Pools: 🗹 Inherit		Sele	sct	
	More Options			*	
	Tunneling Protocols:	🔄 Inherit	Clientless SSL VPN V SSL VPN C	L VPN Client	
	IPv4 Filter:	🔽 Inherit	×.		
	IPv6 Filter:	🔽 Inherit	×		
	NAC Policy:	🔽 Inherit	×		
	Access Hours:	🔽 Inherit	×.		
	Simultaneous Logins:	🗹 Inherit			
	Restrict access to VLAN:	🔽 Inherit	×		
	Connection Profile (Tunnel Group) Lock	: 🔽 Inherit	×		
	Maximum Connect Time:	🗹 Inherit	Unlimited minutes		
ind:	Next Prev	lous			

4. إنشاء ملف تعريف اتصال Certenroll.أختر Remote Access VPN **(الوصول عن بعد) >** Network Client، ثم انقر فوق **إضافة**.أدخل مجموعة Access (وصول عميل الشبكة) > توصيفات توصيل AnyConnect، ثم انقر فوق **إضافة**.أدخل مجموعة certenroll في حقل الأسماء المستعارة.ملاحظة: يجب أن يتطابق اسم الاسم المستعار مع القيمة المستخدمة في ملف تعريف AnyConnect ضمن

#### .AutoSCEPHost

둴 Add SSL VPN Connecti	on Profile		$\overline{\times}$
Advanced General Client Addressing Authentication Secondary Authenticat Authorization Authorization Accounting SSL VPN	Name: Aliases: Authentication Method: AAA Server Group:	certenroll Certenrol AAA Certificate Both LOCAL USe LOCAL if Server Group fails	Manage
	Client Address Assignent —		
	DHCP Servers:		
	Client Address Pools:	ssl_pool	Select
	Client IPv6 Address Pools:		Select
	Default Group Policy		
	Group Policy:	Certenroll 💌	Manage
	(	(Following field is an altribute of the group policy selected above.)	

5. إنشاء توصيف توصيل آخر يسمى **التحقق** بمصادقة الشهادة. هذا هو ملف تعريف الاتصال الفعلي الذي يتم إستخدامه بعد

			ىجىل.
Edit SSL VPN Co	nnection Profile: certauth		-
Basic	Name:	certauth	
Advanced	Aliases:	certauth	
	Authentication		
	Method:	○ AAA	
	AAA Server Group:	LOCAL	Manage
		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:	certauth	Manage
		(Following field is an attribute of the group policy selected above.)	
		C Enable SSL VPN Client protocol	

6. للتأكد من تمكين إستخدام الاسم المستعار، راجع **السماح للمستخدم بتحديد ملف تعريف الاتصال، المعرف** بواسطة الاسم المستعار، في صفحة تسجيل الدخول. وإلا، فإن DefaultWebVPNGgroup هو ملف تعريف الاتصال.

🚯 Home 🔥 Configuration 📴 Monitoring	Save (	🗞 Refresh 🚺 Back 🔘 fi	orward 🧳 Help			CISCO
Remote Access VPN	9 9 X	Configuration > Remote A	ccess VPN > Network (Clien	t) Access > AnyConnect	Connection Profiles	0
		The security appliance autor client deployment requires e Layer Security (DTLS) tunne (More client-related parame Access Interfaces Pable Cisco AnyConne	matically deploys the Cisco Anys nd-user administrative nights. T ling options. sters, such as client images and ct VPN Client or legacy SSL VPN	Connect VPN Client or legacy he Cisco Any-Connect VPN Cl client profiles, can be found Client access on the interfac	SSL VPN Client to remote users upon conne lent supports the HTTPS/TCP (SSL) and Dat at <u>Client Settings.</u> ) es selected in the table below	ction. The initial agram Transport
B 🙀 SSL VPN		Interface	Allow Access	Enable DTLS		
- Clent Settings		outside	Image: A start and a start	2		
Bypess Interface Access List		inside				
Easy VFN Remote     AAA(Local Users     AAA(Local Users     Certificate Management     Certificate Management     Certificate Management     Did Development     Did Server     Advanced		Access Port: 443 Click here to <u>Assign Certific</u> Login Page Setting Allow user to select con Connection Profiles Connection profile (tunnel g Add C Edit Dele	DTLS Port: 443 ate to Interface. nection profile, identified by its - roup) specifies how user is auth te	alias, on the login page. Oth enticated and other paramet	erwise, DefaultWebVPINGroup will be the cor ters.	nection profile.
		Name	Enabled	Allases	Authentication Method	
		certenvol		certenvol	AAA(LOCAL)	
		Sales		Sales	AAA(LOCAL)	
		DefaultRAGroup			AAA(LOCAL)	
		certauth		certauth	Certificate	
		DefaultWEBVPWGroup		default	AAA(LOCAL)	

## إختبار بروتوكول SCEP ل AnyConnect

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. بدء تشغيل عميل AnyConnect، والاتصال بملف تعريف

	省 Cisco AnyCon	nect VPN Client	
	🔌 Connection	🕄 Statistics  ಿ About	
		cisco	
	Connect to:	asa2.cisco.com	✓ 3 <sup>2</sup>
	Group:	certenroll	✓
	Username:	cisco	
	Password:	****	
		Connect	
یقوم AnyConnect	Please enter your us	ername and password.	Certenroll
		CA من خلال	بتمرير طلب التسجيل إلى خادم



8				
Č.	Cisco AnyConne	ect VPN Client		
1	🗞 Connection [	Statistics 🏾 🍰 About		
		ılıılı cısco		
	Connect to:	asa2.cisco.com	✓ 30	
	Group:	certenroll		
	Username:	cisco	7.1	
1	Password:			
가지 않으며 가지 않으며 않는 것		Connect Get C	ertificate	
Plea	ase enter your userr	name and password.		<b>.</b> _
	م والشهادة	لى <b>نعم</b> لتثبيت شهادة المستخدر	سهاده. ظهر هذا التحذير. انقر عا	ر 2. يا
			لجذر	1
certificate from a cer	rtification authority (CA) claiming to re	ipresent:	-	
that the certificate is	s actually from "CA2003". You should r	confirm its origin by contacting "CA2003". The follows	ing number will assist you in this process:	
IDAAEF F3DA5383 FDF	8CP3C 20637469 A587FCF2			
certificate, Windows will wedge this risk.	automatically trust any certificate issi	ued by this CA. Installing a certificate with an unconf	inmed thumbprint is a security risk. If you	
I this certificate?				
	Ϋ́es	No		

Security Warning

Δ

You are about

Warning: If you install th click "Yes" you

Do you want b

CA2003 Windows cann Thumbprint (st

3. بمجرد تسجيل الشهادة، اتصل بملف تعريف **الشهادة**.

## <u>تخزين الشهادة في Microsoft Windows بعد طلب SCEP</u>

أكمل الخطوات التالية:

- 1. انقر على **ابدأ > تشغيل > mmc**.
  - 2. انقر فوق **إضافة/إزالة انجذاب**.

#### 3. انقر **إضافة**، واختر **شهادات**.

4. إضافة شهادات **حساب المستخدم** وحساب **الكمبيوتر**.تظهر هذه الصورة شهادة المستخدم المثبتة في مخزن شهادات

:Windows



, مخزن شهادات	المصدق المثبتة في	شهادة المرجع ا	تظهر هذه الصورة ب
			:Windows

📸 Console Root\Certificates - Current User\Trus	ste	ed F	Root Certification Authorities\Ce	ertificates 📃 🗆 🖻	R
😑 🐻 Certificates - Current User	^		Issued To 🔺	Issued By	~
🖻 🦳 Personal	-	10	12.196.15.106	12.196.15.106	
Certificates			12.96.152.222	12.96.152.222	Ξ
Trusted Root Certification Authorities			171.69.89.134	171.69.89.134	
Certificates			B 216.159.244.70	216.159.244.70	
Enterprise Trust			E 66.10.80.99	66.10.80.99	
Active Directory Liser Object			B66.246.64.10	66.246.64.10	
Insted Publishers	-		AAA Certificate Services	AAA Certificate Services	
Intrusted Certificates	=		BABA.ECOM Root CA	ABA.ECOM Root CA	
Third-Party Root Certification Authorities			🔤 AddTrust External CA Root	AddTrust External CA Root	
🗉 🧰 Trusted People			🖼 Autoridad Certificadora de la Asoci	Autoridad Certificadora de la As	
🗉 🧰 Other People			🕾 Autoridad Certificadora del Colegi	Autoridad Certificadora del Cole	
🕀 🚞 Other			🔤 av-prod-ca-1	av-prod-ca-1	
🕀 🚞 Certificate Enrollment Requests			Baltimore EZ by DST	Baltimore EZ by DST	
🗄 🚞 _NMSTR	-	- 6	🔤 Belgacom E-Trust Primary CA	Belgacom E-Trust Primary CA	
			🔤 C&W HKT SecureNet CA Class A	C&W HKT SecureNet CA Class A	
● ● ● 券			🔤 C&W HKT SecureNet CA Class B	C&W HKT SecureNet CA Class E	
			🔤 C&W HKT SecureNet CA Root	C&W HKT SecureNet CA Root	
Certificates (Local Computer)			🔄 C&W HKT SecureNet CA SGC Root	C&W HKT SecureNet CA SGC Rc	
Personal			SECA1	CA 1	
Certificates		$\square$	CA2003	CA2003	
Cartificator		16	NO. 7 N 70 10 2	CA2002	×.
Certificates	~	1).	• ] · · · · · · · · · · · · · · · · · ·	2	
Trusted Root Certification Authorities store contains 128 certil	ficat	ates	6		

## <u>استكشاف الأخطاء وإصلاحها</u>

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- يعمل تسجيل بروتوكول SCEP ل AnyConnect فقط عند فشل مصادقة الشهادة. إذا لم يتم التسجيل، تحقق من مخزن الشهادات. إذا كانت الشهادات مثبتة بالفعل، قم بحذفها ثم أعد إختبارها.
- لا يعمل تسجيل SCEP ما لم يتم إستخدام الأمر ssi certificate-authentication interface خارج المنفذ 443. راجع معرفات أخطاء Cisco هذه للحصول على مزيد من المعلومات:معرف تصحيح الأخطاء من Cisco (العملاء المسجلون فقط) — لا يعمل تسجيل SCEP ل AnyConnect مع مصادقة الوحدة النمطية 2 لكل مجموعةمعرف تصحيح الأخطاء من Cisco <u>CSCtf06844 (العملاء المسجلون</u> فقط) —تسجيل SCEP ل AnyConnect لا يعمل مع ASA لكل مجموعة مصادقة
  - إذا كان خادم CA على الجزء الخارجي من ASA، فتأكد من السماح بدوران الشعر باستخدام الأمر **نفسه**security-traffic allowed intra-interface. أضفت أيضا ال nat خارج و access-list أمر كما هو موضح في هذا المثال:

nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87 حيث يمثل 172.16.1.0 تجمع AnyConnect، ويمثل 171.69.89.87 عنوان IP لخادم CA.

• إذا كان خادم CA موجودا بالداخل، فتأكد من تضمينه في قائمة الوصول إلى النفق المقسم لنهج مجموعة certenroll. في هذا المستند، يفترض أن خادم CA موجود بالداخل.

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

#### <u>معلومات ذات صلة</u>

- دليل مسؤول عميل AnyConnect VPN من Cisco، الإصدار 2.4
  - الدعم التقني والمستندات Cisco Systems

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما