VPN و ASA/PIX 7.x ليمعل IPSec ةقداصم لائم مادختساب ةيمقر تاداهش مادختساب Microsoft CA نيوكت

المحتويات

<u>المقدمة</u> <u>المتطلبات الأساسية</u> <u>المكونات المستخدمة</u> <u>المكونات المستخدمة</u> <u>الاصطلاحات</u> <u>التكوين</u> <u>التكوينات</u> <u>ملخص تكوين ASA</u> <u>ملخص تكوين ASA</u> <u>ملخص تكوين ASA</u> <u>ملخص تكوين ASA</u> <u>ملخص مميل شبكة VPN</u> <u>استكشاف الأخطاء وإصلاحها</u> <u>معلومات ذات صلة</u>

<u>المقدمة</u>

يوضح هذا المستند كيفية تثبيت شهادة رقمية لمورد الطرف الثالث يدويا على خادم جهاز الأمان (7.x (ASA/PIX من Cisco، بالإضافة إلى عملاء شبكة VPN، لمصادقة أقران IPSec باستخدام خادم مرجع الشهادات (CA) من Microsoft.

<u>المتطلبات الأساسية</u>

<u>المتطلبات</u>

يتطلب هذا المستند أن يكون لديك حق الوصول إلى مرجع مصدق (CA) لتسجيل الشهادة. تشمل بائعي CA المدعومين من الطرف الثالث بالتيمور و Cisco و Entrust و iPlanet/Netscape و Microsoft و RSA.

ملاحظة: يستخدم هذا المستند Windows 2003 Server كخادم CA للسيناريو.

ملاحظة: يفترض هذا المستند عدم وجود تكوين شبكة VPN موجود مسبقا في ASA/PIX.

<u>المكونات المستخدمة</u>

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

• ASA 5510 الذي يشغل الإصدار 2,7.2) من البرنامج و ASDM الإصدار 2,5.2).

• عميل شبكة VPN الذي يشغل الإصدار x.4 من البرنامج والإصدارات الأحدث.

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>المنتجات ذات الصلة</u>

كما يمكن إستخدام تكوين ASA مع Cisco 500 Series PIX الذي يشغل الإصدار x.7 من البرنامج.

<u>الاصطلاحات</u>

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

<u>التكوين</u>

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم <u>أداة بحث الأوامر</u> (للعملاء <u>المسجلين</u> فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

<u>الرسم التخطيطي للشبكة</u>

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

<u>التكوينات</u>

يستخدم هذا المستند التكوينات التالية:

- <u>تکوین ASA</u>
- <u>ملخص تکوین ASA</u>
- <u>تكوين عميل شبكة VPN</u>

<u>تکوین ASA</u>

أتمت هذا steps in order to ركبت طرف ثالث بائع شهادة رقمية على ال ASA:

<u>الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية</u>

<u>الخطوة 2. إنشاء زوج مفاتيح RSA</u>

الخطوة 3. قم بإنشاء TrustPoint.

الخطوة 4. إنشاء تسجيل الشهادة.

الخطوة 5. مصادقة TrustPoint

الخطوة 6. تثبيت الشهادة

<u>الخطوة 7. تكوين شبكة VPN للوصول عن بعد (IPSec) لاستخدام الشهادة المثبتة حديثا</u>

الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية

إجراء ASDM

- 1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
- 2. قم بتوسيع **إدارة الأجهزة،** واختر **الساعة**.
- 3. تحقق من صحة المعلومات المدرجة.يجب أن تكون قيم التاريخ والوقت والمنطقة الزمنية دقيقة حتى يتم التحقق من صحة الشهادة بشكل صحيح.

Startup Wizard AAA Setup AAA Setup Anti-Spoofing ARP Auto Update Client Update Client Update Certificate Device Access Device Access Device Access Mathematication Solution Time	
AAA Setup Anti-Spoofing ARP Auto Update Client Update Certificate Device Access Device Administration M T W T F S	
Image: Solution of the second state of the second stat	
Client Update ⊕	
Perice Access December Z007 Time SM T W T F S	
S M T W T F S	
Boot Image/Confic hh : m	m ∶ss
	5 : 41
Console 2 3 4 5 6 7 8	
9 10 11 12 13 14 15	Update D
FTP Mode 16 17 18 19 20 21 22	
Password 30 31	
SMTP	
Apply Reset	

مثال على سطر الأوامر

					Cisc	co AS	A
			C	iscoAs	SA# sho	w cloc	:k
IST	Fri	Dec	28	2007	16:25	:49.58	30

<u>الخطوة 2. إنشاء زوج مفاتيح RSA</u>

يتم دمج مفتاح RSA العام الذي تم إنشاؤه مع معلومات الهوية من ASA لتكوين طلب شهادة PKCS#10. يجب عليك تحديد اسم المفتاح بشكل واضح باستخدام TrustPoint التي تقوم بإنشاء زوج المفاتيح لها.

إجراء ASDM

- 1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
- 2. قم بتوسيع **الشهادة**، واختر **زوج المفاتيح**.
 - 3. انقر فوق **إضافة** (Add).

Configuration > Properties > Certific	ate > Key Pair						
	/ Pair						
🗄 🖬 AAA Setup	Conference the law active to be seened to and	Marta a					
	Configure the key pairs to be used in certificates.						
E-B ARP							
	Note: Operations on this screen are applied immediately upon completion and are irreversible.						
E 🔂 Certificate							
Authentication							
2 Enrolment	Kau Dair Nama	Usaga	Modulus Size	[
- El Import Certificate	Ney Pair Name	Usage	MODUIUS SIZE	Add			
- Stev Pair				1			
Anage Certificat	1			Show Details			
😟 🙀 Trustpoi 🚺 Add Key Pair		×					
E 🜈 Device Acce				Delete			
E 36 Device Admi	C						
- 讨 Banner 🛛 Name:	 Use default key name 			Defeat			
Boot Ima	C much had			retresh			
CLI Prom	(• my.CA.key)						
Clock							
- 🍓 Console 🛛 Size:	1024 💌						
🌆 CSD Set							
Oevice Usage:	General Purpose C Special						
FTP Moc							
CMP Ru							
Manager							
O NTP Generate No	ow Cancel He	4p					
Passwo							

4. قم بإدخال اسم المفتاح، واختر حجم المعامل، وحدد نوع الاستخدام.**ملاحظة:** حجم زوج المفاتيح الموصى به هو 1024.

> 5. انقر فوق **إنشاء الآن**.يجب إدراج زوج المفاتيح الذي قمت بإنشائه في عمود "اسم زوج المفاتيح". **مثال على سطر الأوامر**

Cisco ASA
CiscoASA#configure terminal
CiscoASA(config)#crypto key generate rsa label my.CA.key modulus 1024
Generates 1024 bit RSA key pair. "label" defines!
the name of the key pair. INFO: The name for the keys
will be: my.CA.key Keypair generation process begin.
#(Please wait ciscoasa(config

<u>الخطوة 3. إنشاء TrustPoint</u>

يلزم توفر نقاط الثقة لإعلان المرجع المصدق (CA) الذي سيستخدمه ASA.

إجراء ASDM

- 1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
- 2. قم بتوسيع **الشهادة**، ثم قم بتوسيع TrustPoint.
 - 3. أخترت **تشكيل**، وبعد ذلك طقطقت

يضيف.

Configuration > Properties > Certificate > Trustpoint > Configuration							
00	Startup Wizard		Configur	ation			
÷ f	AAA Setup	11	Confi	imma a Cartificata Aut	horiby (CA) as a trustmaint		
- 🔞	Anti-Spoofing	Ш	Conii	igure a Certificate Aut	nonty (CA) as a trustpoint.		
• 🐯	ARP	Ш					
- 3	Auto Update	Ш					
- 3	Client Update	Ш					
÷	Certificate	Ш		Trustpoint Name	Device Certificate Subject	CA Certificate Subject	Add
	Authentication	Ш					
-	Enrolment	Ш					Edit
	E Import Certificate	Ш					
	🍇 Key Pair	Ш					
	Anage Certificat	Ш					Delete
	Real Trustpoint	Ш					
	Configuration						Request (
	Export						

- 4. قم بتكوين هذه القيم:**اسم TrustPoint**: يجب أن يكون اسم TrustPoint ذا صلة بالاستخدام المقصود. (يستخدم هذا المثال *CA1*.)**زوج المفاتيح**: حدد زوج المفاتيح الذي تم إنشاؤه في <u>الخطوة 2</u> (my.CA.key)
 - 5. تأكد من تحديد التسجيل اليدوي.
 - 6. انقر على **معلمات الشهادة**.يظهر مربع الحوار معلمات الشهادة.
 - 7. طقطقة **يحرر**، وشكلت الشعار يعدد في هذا طاولة:لتكوين هذه القيم، أختر قيمة من القائمة المنسدلة "سمات"، وأدخل القيمة، وانقر فوق

			إضافة.
🔂 Edit DN			
		Attribute	Value
		Common Name (CN)	CiscoASA.cisco.com
DN Attribute to be Added]	Department (OU)	TSWEB
	0.000	Company Name (O)	Cisco Systems
Attribute: Select Attribute	Add >>	Country (C)	US
		State (St)	North Carolina
Value:	Delete	Location (L)	Raleigh
	_		
		J	
ок	Cancel	Help	

- 8. بمجرد إضافة القيم المناسبة، انقر فوق **موافق**.
- 9. في شاشة معلمات الشهادة، أدخل FQDN في حقل تحديد FQDN.يجب أن تكون هذه القيمة نفس FQDN التي أستخدمتها للاسم الشائع

💼 Certificate Paramet	ers				
Enter the values fo	r the parar	meters that are to be in	cluded in the certit		
Subject DN:	Systems,C	C=US,St=North Carolina	i,L=Raleigh		
Subject Alternativ	e Name (F	QDN)			
C Use FQDN	of the devi	ice			
Specify FQDN CiscoASA.cisco.com					
C Use none					
E-mail:					
IP Address:					
🗌 Include device	serial num	nber			
0	(Cancel	Help		

- 10. وانقر فوق **OK**.
- 11. تحقق من تحديد زوج المفاتيح الصحيح، ثم انقر فوق زر **إستخدام التسجيل اليدوي**.
 - 12. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.

🧯 Add Trustpoint Configu	ration				
Trustpoint Name:	41]			
🔲 Generate a self-sign	ed certificate on enr	oliment			
If this option is enable	ed, only Key Pair and	d Certificate Parameters	can be specified.		
Enrollment Settings Re	vocation Check CF	RL Retrieval Policy CRI	L Retrieval Method OCSP		
Key Pair: my.C	A.key	Show Details	New Key Pair		
Challenge		Confirm Challenge			
Password:		Password:			
Enrollment Mode can o	only be specified if t	here are no certificates	associated with this trust		
Enrollment Mode					
💽 Use manual	enroliment				
🔿 Use automat	ic enrollment				
Enrollment URL	.: http://				
Retry Period:	1	minutes			
Retry Count:	0	(Use 0 to indicate un	nlimited retries)		
Certificate Parameter					
	ок	Cancel	Help		

مثال على سطر الأوامر

Cisco ASA
CiscoASA(config)#crypto ca trustpoint CA1
Creates the trustpoint. CiscoASA(config-ca! trustpoint)#enrollment terminal
Specifies cut and paste enrollment with this!
<pre>trustpoint. CiscoASA(config-ca-trustpoint)#subject-name</pre>
,CN=wepvpn.cisco.com,OU=TSWEB
O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh
Defines x.500 distinguished name. CiscoASA(config!

ca-trustpoint)# keypair my.CA.ke y
Specifies key pair generated in <u>Step 2</u> CiscoASA(config-ca-trustpoint)# fqdn CiscoASA.cisco.co
Specifies subject alternative name (DNS:) CiscoASA(config-ca-trustpoint)#exit

<u>الخطوة 4. إنشاء تسجيل الشهادة</u>

إجراء ASDM

- 1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
 - 2. قم بتوسيع **الشهادة**، واختر **التسجيل**.
- 3. تحقق من تحديد TrustPoint الذي تم إنشاؤه في <u>الخطوة 3</u>، وانقر فوق **تسجيل**.يظهر مربع حوار يسرد طلب تسجيل الشهادة (يشار إليه أيضا باسم طلب توقيع ·

شهادة).

🚰 Enrollment Request

To complete the enrollment process, please paste the following PKCS10 enrollment request into the management interface of the CA.

You will need to install the certificate after receiving it.

Go to Configuration > Properties > Certificate > Import Certificate to do so.

Certificate	Request:
-------------	----------

hvcNAQkCFhtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wgZ8wDQYJKoZIhvcN	
$\tt AQEBBQADgYOAMIGJAoGBAL5YNIx1zkfo80ziV7xJdfA7jRtkHXx2Npmr9A0Q1Fzm$	
psMFP7DeKPIQ+RdthaRBzngSgmlkmNYoMx6taicY9pbTVgFcfvJH2dsBoL5GhlKY	
mAH40WUXbil8BHZSSgxPX6BGeiC9BjJZvdqCgq+xR404/lYP0oeKKfq7apCHvVHF	
$\verb+AgMBAAGgRjBEBgkqhkiG9w0BCQ4xNzA1MAsGA1UdDwQEAwIFoDAmBgNVHREEHzAd$	
ghtDaXNjb0FTQS5teWRvbWFpbi5jaXNjby5jb20wDQYJKoZIhvcNAQEEBQADgYEA	
gmoBmSRVnL0qyDtpS1bveKew0AdG5/fxnJRYU2Uunl1W6sG0KaJYCiFH//eaewF3	
gEjVABVhB7Ni6N29710mDAbnPs0R3IyMwbr3eChIFwkZjBTwoe9LuR0gefWfyAH0	
gonnkGTJ11vZCSDXz4BXm4sXAqrwZCDdj0/S5BiQJGc=	
End - This line not part of the certificate request	-

OK

4. انسخ طلب تسجيل PKCS#10 إلى ملف نصي، ثم أرسل CSR المحفوظ إلى مورد الطرف الثالث (مثل Microsoft CA) كما هو موضح في هذا الإجراء:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام بيانات المستخدم المتوفرة لخادم VPN.

🕗 about:blank - Microsoft Iı	iternet Exploi	er provided by	y Cisco Sys	tems, Inc.	
File Edit View Favorites	Tools Help				
🗧 Back 🔻 🤿 👻 🙆 👔	පී 🛛 🔕 Search	😹 Favorites	Media	1 🕲 🖓 🖏	4 e e
Address (http://172.16.5.1)	certsry				
Enter Net	work Passwor	ď			? ×
	Please type yo	our user name and	d password.		
ل کا	Site:	172.16.5.1			
	User Name	vpnuser			
	Password	*****)	
	Domain				
	🔲 Save this p	bassword in your	password list	t	
			ОК		Cancel

ملاحظة: تأكد من وجود حساب مستخدم لخادم ASA (VPN) مزود بخادم CA.انقر فوق <mark>طلب شهادة > طلب</mark> شهادة متقدم، ثم حدد إرسال طلب شهادة باستخدام ملف CMC أو PKCS#10 مرمز بالأساس 64 أو إرسال طلب تجديد باستخدام ملف PKCS#7 مرمز بالأساس-

	-	<u>64</u>
Address 🙆 http://172.16.5.1/certsrv/certrgad.asp	<i>@</i> 60	Lini
Microsoft Certificate Services - CA1	Ho	<u>ne</u>
Advanced Certificate Request		
The policy of the CA determines the types of certificates you can request. Click one of the following options to:		
Create and submit a request to this CA.		
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request a base-64-encoded PKCS #7 file.	by us	ing
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment s Note: You must have an enrollment agent certificate to submit a request on behalf of another user.	tation.	•
لعلومات التي تم ترميزها ولصقها في حقل نص الطلب المحفوظ ، وانقر	ىخ الە	انس

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded (source (such as a Web server) in the Saved Request box.

Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	VQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQFAAO 4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8 D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+ 8Ux9emhFHpGHnQ/MpSfU0dQ== not part of the certificate request	
Certificate Temp	late:	
	IPSEC -	
Additional Attribu	utes:	
Attributes:		
	Submit >	
	ال Base 64 يرمز لاسلكي زر، وطقطقة تنزيل	یں بت
Micros	soft Certificate Services CA1	
Certifi	icate Issued	
The ce	ertificate you requested was issued to you.	
	 DER encoded or Base 64 encoded Download certificate Download certificate chain 	
عندما بظهر		ة.

مربع الحوار تنزيل الملف، قم بحفظه بالاسم **cert_client_id.cer**، وهو شهادة الهوية التي سيتم تثبيتها على

File Dowi	nload 🔀				
?	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.				
	File name: certnew.cer				
	File type: Security Certificate				
	From: 172.16.5.1				
	This type of file could harm your computer if it contains malicious code.				
	Would you like to open the file or save it to your computer?				
	Open Save Cancel More Info				
	Always ask before opening this type of file				

مثال على سطر الأوامر

Cisco ASA CiscoASA(config)#crypto ca enroll CA1 Initiates CSR. This is the request to be submitted ---! !--- via web or email to the 3rd party vendor. % Start certificate enrollment .. % The subject name in the certificate will be: CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco Systems, C=US, St=North Carolina, L=Raleigh % The fully-qualified domain name in the certificate will be: CiscoASA.cisco.com % Include the device serial number in the subject name? [yes/no]: no Do not include the device's serial number in the ---! subject. Display Certificate Request to terminal? [yes/no]: yes Displays the PKCS#10 enrollment request to the ---! terminal. !--- You will need to copy this from the terminal to a text !--- file or web text field to submit to the 3rd party CA. Certificate Request follows: MIICHjCCAYcCAQAwgaAxEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgT Dk5vcnRo IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z dGVtczEO MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv bTEhMB8G CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3 DQEBAQUA A4GNADCBiQKBqQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqqBaB 9M4yTx5b Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt 30MXSNPO mldZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar gwIDAQAB oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw

```
FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
bkc2ykkm
bYvRt/wiKc8FjpvPpfOkjMK0T3t+HeQ/5QlKx2Y/vrqs+Hg5SLHpbhj/
Uo13yWCe 0Bzg59cYXq/vkoqZV/tBuACr ---End - This line not
part of the certificate request--- Redisplay enrollment
request? [yes/no]: no
#(ciscoasa(config
```

<u>الخطوة 5. مصادقة TrustPoint</u>

بمجرد إستلام شهادة الهوية من مورد الطرف الثالث، يمكنك المتابعة بهذه الخطوة.

إجراء ASDM

- 1. قم بحفظ شهادة الهوية على الكمبيوتر المحلي.
- 2. إذا تم توفير شهادة مرمزة وفقا لمعيار base64 لم يتم إرسالها كملف، فيجب نسخ الرسالة base64 ولصقها في ملف نصي.
- 3. أعد تسمية الملف بامتدا<u>د .cer.**ملاحظة:**</u> بمجرد إعادة تسمية الملف بامتداد .cer، يجب أن تظهر أيقونة الملف



کشهادة کما هو موضح.

4. قم بالنقر <u>المزدوج على ملف</u>



ملاحظة: إذا ظهرت

رسالة "Windows لا يحتوي على معلومات كافية للتحقق من هذه الشهادة" في علامة التبويب "عام"، فيجب الحصول على شهادة المرجع المصدق الجذر (CA) أو شهادة المرجع المصدق الوسيط (CA) للجهة الخارجية قبل متابعة هذا الإجراء. اتصل بمورد الطرف الثالث أو بمسؤول CA للحصول على شهادة CA أو شهادة CA الوسيطة للإصدار.

- 5. انقر على صفحة **مسار الشهادة**
- 6. انقر على شهادة المرجع المصدق الموجودة فوق شهادة الهوية الصادرة، وانقر فوق **عرض**

Certificate		? >
General Details Certification Path		
Certification path		
CiscoASA.cisco.com OU=TSWEB		
	<u>V</u> iew Cer	tificate
Certificate <u>s</u> tatus:		
This certificate is OK.		
		OK

معلومات تفصيلية حول شهادة المرجع المصدق.

7. انقر فوق **تفاصيل** لمعرفة المزيد من المعلومات حول شهادة

rtificate	?	×
General Details Certification	Path	
Show:	Ţ	
Field	Value 🔺	
💳 Version	V3	
💳 Serial number	611E E59B 0000 0000 0007	
🚍 Signature algorithm	sha1RSA —	
EIssuer	CA1, TSWeb, cisco, com	
🚍 Valid from	Saturday, December 15, 2007	
🚍 Valid to	Monday, December 14, 2009	
E Subject	CiscoASA.cisco.com OU=TSW	
🖻 Public key	RSA (1024 Bits)	
	Edit Properties Copy to File	

8. قبل تثبيت شهادة الهوية، يجب تنزيل شهادة المرجع المصدق من خادم CA وتثبيتها في ASA. أتمت هذا steps جابت ال CA شهادة من ال CA نادل يعين *CA*1:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام تكوينات المستخدم المتوفرة لخادم

ه	about:bl	ank - Mici	rosoft Inl	ernet Ex	plore	۲		
E	jie <u>E</u> dit	<u>V</u> iew F	<u>a</u> vorites	<u>T</u> ools	<u>H</u> elp			
G)Back 👻	🕘 🔹 🖹	2 🐔) 🔎 Sea	arch	📌 Favorite:	s 🔗	
Ag	<u>i</u> dress 🦉	http://172	2.16.5.1/o	ertsrv				
								_
	Con	nect to 17	2.16.5.1				? ×	1
	f							
		11						
	Co	nnecting to	172.16.5.	1				
	Use	er name:	ſ	vpnserv	/er		▼ <u>.</u>	
	Pas	sword:	-	•••••	,		_	
				Dememb	er my n	accword		
				Kememb	сі шу р	/d35///01/d		
					ОК	Ca	ncel	
_القر فوق تنزيل شهادة تقريما ليتنبيا ي شمادة	ة التشفيريا:	اتحديد طبية	Base 64	د در در در م		CRI alIs		
لفر علی ترین شهری	۵۰۱۰سعیر	للحديد طرية	Dage 04	د رر رادیو	، ىم ~		the summer	المرجع
							· (المصدق



File Download - Security

اسم	استخدام	لکمبیوتر ہ	<u>علی ا</u>	لمصدق	لمرجع ا	ئىها <u>دة ا</u>	بحفظ ب	فم
¥arning						×		

	Do you	want to open or save this file?	
		Name: certnew.cer Type: Security Certificate, 1.64 KB From: 172.16.5.1	
		<u>Open</u> <u>S</u> ave Cancel	
	٩	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>	
			.certnew.cer
		كان الذي قمت فيه بحفظ شهادة المرجع المصدق.	9. تصفح إلى الم
ل إلى	واختر إرسا	ستخدام محرر نصوص، مثل Notepad. (انقر بزر الماوس الأيمن فوق الملف،	10. افتح الملف با

Notepad .)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)
.)</

🛿 certnew.cer - Notepad <u>File E</u>dit F<u>o</u>rmat <u>H</u>elp --BEGIN CERTIFICATE--MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0BAQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT BqoJkiaJk/IsZAEZFqVUU1dlyjEMMAoGA1UEAxMDQ0ExMB4xDTA3MTIxNDA2MDE0 M1o×DTEyMTI×NDA2MTA×NVowUTETMBEGCqmSJomT8i×kARkWA2NvbTEVMBMGCqmS jomT8ixkARkwBWNpc2NvMRUwEwYKCZImiŹPyLGQBGRYFVFNXZWIXDDAKBgNVBĀMT AONBMTCCASIwDQYjKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seuvvyiLmA9 BSGzMz3sCtR9TCMwOx7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vŴeMijcQnŵdOq+ Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7kZf4dbQI y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXwKh4uC04xxQmr//Sct1tdwQcvk2V µBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSSz+TlDhXx wPXR018CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsGA1UdDwQE AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3mYfNQJ pAP1wDccAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsawM]MjBLZXk]MjBTZXJ2aWN]cyxD Tj1TZXJ2aWN]cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNpc2NvLERD PŴNvbT9jZXJ0aŴZpYŹF0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JgZWN0Q2xhc3M9 Y1JMRGlzdHJpYnV0aw9uUG9pbnSGNwh0dHA6Ly90cy13MmszLwFjcy50c3dlYi5j aXNjby5jb20vQ2vydEvucm9sbC9DQTEuY3JsMBAGC5sGAQQBgjcVAQQDAgEAMA0G CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4MicbXJeKr L6z86JGw1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZwAgfmGUm++HMljnw8liyIF þcNwxlqxsDT+n9Yok6bnG6uof4SgETNrN8EyYVrSGKolE+oC5L+ytJvŵ19GZhlzE [OVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCqFwNcNItcufu0x]b 1xxc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149zpXv5tqT 9Ms7ABAu+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at ---END CERTIFICATE---

- 12. ضمن ASDM، انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
 - 13. قم بتوسيع **الشهادة**، واختر **المصادقة**.
- 14. انقر على زر **إدخال نص الترخيص بتنسيق سداسي عشر أو تنسيق base64**.
- 15. الصق شهادة المرجع المصدق بتنسيق base64 من محرر النصوص في منطقة النص.
 - 16. طقطقة

يصدق.

Configuration > Properties > C	artificate > Authentication
📇 🔗 Startup Wizard	Authentication
🗄 🖬 AAA Setup	
	Authenticate a CA certificate. As the result of authentication, the CA certificate will be assoc
🗷 🔯 ARP	trustpoint and installed on the device.
	Test siddless
	CA1
🖃 🔂 Certificate	
Authentication	Fingerprint (optional):
Enrollment	,
- 🔁 Import Certificate	The certificate text can be specified if the selected, trustnoint is configured for manual
	The certificate text can be specified if the selected if depoint is configured for manual
	Certificate Text
🖃 🙀 Trustpoint	
	C Import from a file: Browse
Export	
- Import	Enter the certificate text in hexadecimal or base64 format:
🗄 🌈 Device Access	
🖻 🐉 Device Administration	L6266JGVV1RbTSV Yni IrqRy6HEoirdU6CHgHUCD9/BZVVAgtmGUm++HMijnV
🗐 Banner	Authentication Successful
	wGPn149zp
CLI Prompt	C .
Clock —	The trustpoint CA1 has been authenticated.
	✓
- OP Device	
FTP Mode	OK
ICMP Rules	
- 🞯 NTP	
Password	
Secure Copy	
- 🙀 SMTP	
SNMP I	Authenticate

17. وانقر فوق OK. مثال على سطر الأوامر

Cisco ASA
CiscoASA(config)#crypto ca authenticate CA1
Initiates the prompt to paste in the base64 CA root! ! or intermediate certificate. Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itselfBEGIN CERTIFICATE MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B AQUFADBR MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21z Y28xFTAT BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx NDA2MDE0 M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV MBMGCgmS JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK BgNVBAMT A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu VvyiLmA9 BSGzMz3sCtR9TCMW0x7qM8mmiD0o70kGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij

+cQnwdOq
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
AludDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb818jq18RRD
L3mYfNQJ
pAP1WDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2
aWNlcyxD
- Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9iZXJ0aWZpY2F0ZVJ1dm9iYXRpb25MaXN0P2Jhc2U/b2JgZWN0
02xhc3M9
21JMRG1zdHJpYnV0aW9uUG9pbnSGNWh0dHA6Lv90cv13MmszLWFicv50
c3dlYi5i
aXNibv5ib20v02VvdEVucm9sbC9D0TEuY3JsMBAGCSsGA00BgicVA00D
CSGGSTb3DOEBBOUAA4TBAOAavFpAsvESTtgA+7sii/5I.+KUV34/DoE4M
icbXJeKr
L6Z86.IGW18hf5VYn1TraBy6HEo1rdII6cHaHIICD9/BZWAafmGIIm++HM1i
nW81ivTF
DcNwyloysDT+n9Y0k6bnG6u0f4SgETNrN8EyYVrSGK0lE+0C5L+yt.Jwy
John Mighbling Tohobhoodoliggininoly Tribonoli (Ocol) y com
10VIIIf Pa+PT47dmap6IIo2V2zDW5KCaVI.II8GerFd8wZDPBwMKCcFWNcNIt
1XXa68DKo7X09DBa877uTaou8aLtuiiPOmeOuzaT0Ntwa7x2FuGBa149
TARCOODROZIOSprgo//THACHCOLCHIIFOMeoyzgooN+AazazzawGrH43
2DAVJCQI 9Me7ABAutoBIoi /FfiOrMSOGF1457aIW7dv1WDto85at
JMS/ADAU+DAIOI/EIJQYMSQGFI4J/CIM/GAIVD+D6Jac
END CERTIFICATE
quit
Manually paged cortificate into CLT_INFO:
Certificate has the following attributes: Fingerprint:
09d66001 f6Ed0922 b4EEfbac d672g242 Do you aggent thig
gortificate? [weg/pe]: weg
Trustpoint (A contificate acconted
.irusipoint CA certificate accepted
Contificate suggestatully imported
Certificate successfully imported a
#(ClscoASA(config

الخطوة 6. تثبيت الشهادة

إجراء ASDM

أستخدم شهادة الهوية المقدمة من مورد الطرف الثالث لتنفيذ الخطوات التالية:

- 1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
- 2. قم بتوسيع **الشهادة**، ثم أختر **إستيراد الشهادة**.
- 3. انقر زر **إدخال نص الترخيص بتنسيق** لاسلكي **Base64 أو سداسي عشر**، وقم بلصق شهادة هوية Base64 في حقل النص.

Configuration > Properties	> Certificate > Import Certificate	
Startup Wizard	Import Certificate	u (CA) in response to
Anti-Spoofing	enrollment request.	y (CM) intesponse to
🔤 🛃 Client Update	Tructorint Name:	UR Nores
E 🔁 Certificate		л тчечч
 Authentication 		
Enrollment	Certificate Text	
Import Certificate	Pleas information	Browse
📲 Manage Certifica		
🖯 🖗 Trustpoint	to the	rmat:
💮 Configuratio	Certificate import succeeded.	
		hEMIYmVOtx/oKmYS
		ArhjjFENDdfoq6tDke
E-12 Device Access	[minimum minimum mi	zJyrbUZaJRsBfistKF
🖃 🎯 Device Administratio	<u> </u>	EarqvtxCUvk6nm2
- 🗐 Banner		INIGUSTEGYU4msBUs
		olm==
		-

4. انقر فوق **إستيرا**د، ثم انقر فوق **موافق**. **مثال على سطر الأوامر**

Cisco ASA

	CiscoASA(config)#crypto ca import CA1 certificate
	Initiates prompt to paste the base64 identity! certificate ! provided by the 3rd party vendor. % The
	fully-qualified domain name in the certificate will be:
	CiscoASA.cisco.com Enter the base 64 encoded
	certificate. End with the word "quit" on a line by
	itself ! Paste the base 64 certificate provided by
	the 3rd party vendorBEGIN CERTIFICATE
	MIIFpzCCBI+gAwIBAgIKYR71mwAAAAAABzANBgkqhkiG9w0BAQUFADBR
	MRMwEQYK
	CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY21zY28xFTAT
	BgoJkiaJ
	k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
	OVoXDTA5
	MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRc
	IENhcm9s
	aW5hMRAwDgYDVQQHEwdSYWx1aWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0
	ZW1zMSQw
	IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ
	KoZIhvcN
	AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
	qB9j3HpX
	BmfXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCC
	sS8iqxqC
	2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
	CaeqnGRN
	AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ21z
	Y29BU0Eu
	Y21zY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
	BgNVHSME
	GDAWgBTZrb818jq18RRDL3mYfNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCE
	9aCB8qCE
	74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCXL
	TilOdWJs
1	-J-2

aWM1MjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1
cmF0aW9u
LERDPVRTV2VilERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJ1dm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbnSG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3d1Yi5jaXNjby5jb20vQ2VydEVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibG1jJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXN1P29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
$d{\tt D} {\tt A} {\tt B} {\tt g} {\tt E} {\tt A} {\tt Y} {\tt I} {\tt 3} {\tt F} {\tt A} {\tt I} {\tt E} {\tt F} {\tt B} {\tt 4} {\tt S} {\tt A} {\tt F} {\tt C} {\tt A} {\tt Z} {\tt Q} {\tt B} {\tt y} {\tt A} {\tt H} {\tt A} {\tt Z} {\tt A} {\tt H} {\tt A} {\tt Z} {\tt A} {\tt H} {\tt A} {\tt Z} {\tt A} {\tt $
EwEB/wQC
MAAwEwYDVR01BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/02xDB
7wXQaGph
${\tt zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8}$
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/034wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc
=1L5nuPsd8MaexBc
END CERTIFICATE
quit
INFO: Certificate successfully imported
#(CiscoASA(config

<u>الخطوة 7. تكوين شبكة VPN للوصول عن بعد (IPSec) لاستخدام الشهادة المثبتة حديثا</u>

إجراء ASDM

أتمت هذا steps in order to شكلت الوصول عن بعد VPN:

1. أخترت **تشكيل > VPN > IKE > سياسات > إضافة** in order to خلقت ISAKMP سياسة 65535 كما هو موضح في هذه الصورة.

🗯 Add IKE Policy				
Priority:	65535	Authentication:	rsa-sig 💌	
Encryption:	3des 💌	D-H Group:	2 💌	
Hash:	md5	Lifetime:	C Unlimited	seconds 💌
	ок	Cancel	Help	

- 2. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.
- 3. أخترت **تشكيلً > VPN > IPSec > مجموعات تحويل >إضافة** in order to خلقت مجموعة تحويل (*myset*) كما هو موضح في هذه

		نے دی عدہ	هو موح
🔯 Add Transform Set			
Set Name:	yset		
Mode:	• Tunnel • O	Transport	
ESP Encryption: ESP Authenticati	on:	▼	
ок	Cancel	Help	الصمرة.

- 4. طقطقت **ok**، وبعد ذلك **طبقت**
- 5. أختر **تكوين > VPN > IPSec > قواعد IPSec >إضافة** لإنشاء خريطة تشفير باستخدام سياسة ديناميكية للأولوية 10 كما هو موضح في هذه الصورة:

💼 Create IPSec Rule	
Tunnel Policy (Crypto Map) - Basic Tunnel Policy (Crypto Map) - Advanced Traffic Select	tion
Interface: outside 💌 Policy Type: dynamic 💌	Priority: 10
Transform Sets	
Transform Set to Be Added: myset	
Add >>	Move Up
Remove	Move Down

- 6. طقطقت **ok**، وبعد ذلك **طبقت**
- 7. أخترت **تشكيل>VPN>عام>مجموعة سياسة>إضافة داخلي مجموعة سياسة** in order to خلقت مجموعة ت**قصيرGroup** كما هو موضح في هذه

🚰 Add Interr	nal Group Policy		
Name:	Defaultgrou	9	
General	PSec Client Co	nfiguration Client	Firewall Ha
Check	an Inherit checkb	ox to let the corres	ponding settir
Tunne	eling Protocols:	🔽 Inherit	🗖 IPSe
Filter:		🔽 Inherit	
-Conn Ac	ection Settings cess Hours:	🔽 Inherit	

🔂 Ad	dd Internal G	iroup Policy			
	Name:	Defaultgroup			
	General	ec Client Confi	guration Client Firewall	Hardware Client	NAC Webv
	Check an I	nherit checkbox	to let the corresponding se	atting take its value	e from the def
	General Cl	lient Parameters	Cisco Client Parameters	Microsoft Client F	Parameters
	Banner	:		🔽 Inherit	
	Default	Domain:		🗆 Inherit 🤇	cisco.com

8. طقطقت o<mark>k</mark>، وبعد ذلك **طبقت**

9. أخترت **تشكيل>VPN>IP عنوان إدارة>IP بركة>يضيف** in order to شكلت العنوان بركة VPNpool ل ال VPN

🎼 Add IP Pool			
Name:	vpnpool		
Starting IP Address:	10.5.5.10		
Ending IP Address:	10.5.5.20		
Subnet Mask:	255.255.255.0	•	
ок	Cancel	Help	
			زبون مستعمل ان يكون عينت ديناميكيا.
			10. طقطقت ok ، وبعد ذلك طبقت

11. أخترت **تشكيل>VPN>عام>مستعمل>يضيف** in order to خلقت مستعمل حساب **vpn** ل VPN زبون

💼 Add User Account		
(Identity) VPN Policy	WebVPN	
	Username:	vpnuser
	Password:	*****
	Confirm Password:	*****
	🔲 User authentica	ted using MSCHAP
	Privilege level is used wi	th command authorization.
	Privilege Level:	

12. إضافة هذا المستخدم إلى DefaultRAGoroup

				auli vogioup
F	Add User Account			
	Identity VPN Policy VVebVPN			
	Check an Inherit checkbox to let the co	rresponding settin	g take its valu	ue from the group
	Group Policy:	🔽 İnherit		
		_	<u></u>	_
	Tunneling Protocols:	🔽 Inherit	PSec [VVebVPN
	Filter:	🔽 Inherit		
	Tunnel Group Lock:	🗆 Inherit 🌔	DefaultRA	Group
	Store Password on Client System:	🔽 Inherit	C Yes	C No

- 13. طقطقت o**k**، وبعد ذلك **طبقت**
- 14. تحرير DefaultRagGroup كما هو موضح في هذا الإجراء:أخترت **تشكيل>VPN>عام > مجموعة نفق >** ت**حرير**.أختر **DefaultGroup** من القائمة المنسدلة "نهج

1	🖆 Edit Tunnel Group	
	Name: DefaultRAGroup Type: ipsec-ra	
	Configure general access attributes from the following sub-tabs. Basic Authentication Authorization Accounting Client Address	
	يوعة". Group Policy: Defaultgroup	المجم
<u> </u>	 قائمة المنسدلة لمجموعة خوادم	من ال
🧰 E e	dit Tunnel Group	
	Name: DefaultRAGroup Type: ipsec-ra	
	Configure general access attributes from the following sub-tabs. Basic Authentication Authorization Accounting Client Address Assig	
	To set authentication server group per interface, go to the Advanced ta	
أخترت	Authentication Server Group: LOCAL	المصا
-	vpn من الزبون عنوان تنازل قائمة ميلان إلى	Pool

🞼 Edit Tunnel Group
Name: DefaultRAGroup Type: jpsec-ra
General IPSec PPP
Configure general access attributes from the following sub-tabs.
Basic Authentication Authorization Accounting Client Address Assignmer
To specify whether to use DHCP or address pools for address assignme > IP Address Management > Assignment. DHCP Servers
IP Address: Add >> Delete
Address Pools
To configure interface-specific address pools, go to the Advanced ta
Available Pools Assigned
Add >>

15. طقطقت ok، وبعد ذلك **طبقت**. **مثال على سطر الأوامر**

Cisco ASA
CiscoASA(config)#crypto isakmp enable outside
CiscoASA(config)#crypto isakmp policy 65535
CiscoASA(config-isakmp-policy)#authentication rsa-sig
CiscoASA(config-isakmp-policy)#encryption 3des
CiscoASA(config-isakmp-policy)#hash md5
CiscoASA(config-isakmp-policy)#group 2
CiscoASA(config-isakmp-policy)#lifetime 86400
CiscoASA(config-isakmp-policy)# exit
CiscoASA(config)#crypto isakmp identity auto
Phase 1 Configurations CiscoASA(config)#crypto!
ipsec transform-set myset esp-3des esp-md5-hmac
CiscoASA(config)#crypto dynamic-map outside_dyn_map 10

set transform-set myset
CiscoASA(config)#crypto map outside_map 65535 ipsec-
isakmp dynamic outside_dyn_map
CiscoASA(config)#crypto map outside_map interface
outside
<pre>Phase 2 Configurations CiscoASA(config)#group!</pre>
policy defaultgroup internal
CiscoASA(config)#group-policy defaultgroup attributes
CiscoASA(config-group-policy)#default-domain value
cisco.com
CiscoASA(config-group-policy)# exit
Create a group policy "Defaultgroup" with domain!
name ! cisco.com CiscoASA(config)#username vpnuser
password password123
CiscoASA(config)# username vpnuser attributes
CiscoASA(config-username)# group-lock value
DefaultRAGroup
CiscoASA(config-username)# exit
Create an user account "vpnuser" and added to!
"DefaultRAGroup" CiscoASA(config)#tunnel-group
DefaultRAGroup general-attributes
The Security Appliance provides the default tunnel!
groups ! for remote access (DefaultRAGroup).
CiscoASA(config-tunnel-general)# address-pool vpnpool
Associate the vpnpool to the tunnel group using the!
address pool. CiscoASA(config-tunnel-general)#default-
group-policy Defaultgroup
Associate the group policy "Defaultgroup" to the!
<i>tunnel group</i> . CiscoASA(config-tunnel-general)# exit
CiscoASA(config)#tunnel-group DefaultRAGroup ipsec-
attributes
CiscoASA(config-tunnel-ipsec)# trust-point CA1
CiscoASA(config-tunnel-ipsec)# exit
Associate the trustpoint CA1 for IPSec peer!
authentication

<u>ملخص تکوین ASA</u>

Cisco ASA Cisco ASA Cisco ASA Cisco ASA Saved : (ASA Version 7.2(2 1 hostname Cisco ASA domain-name cisco.com enable password 8Ry2YjIyt7RRXU24 encrypted names 1 interface Ethernet0/0 nameif outside security-level 0 ip address 192.168.1.5 255.255.255.0

```
I
                                   interface Ethernet0/1
                                                shutdown
                                          nameif inside
                                     security-level 100
                      ip address 10.2.2.1 255.255.255.0
                                                        !
                                   interface Ethernet0/2
                                             nameif DMZ
                                       security-level 90
               ip address 10.77.241.142 255.255.255.192
                                                        1
                                   interface Ethernet0/3
                                                shutdown
                                              no nameif
                                      no security-level
                                          no ip address
                                                        !
                                 interface Management0/0
                                                shutdown
                                              no nameif
                                      no security-level
                                          no ip address
                                                        1
                       passwd 2KFQnbNIdI.2KYOU encrypted
                        boot system disk0:/asa722-k8.bin
                                         ftp mode passive
                             dns server-group DefaultDNS
                                  domain-name cisco.com
             access-list 100 extended permit ip 10.2.2.0
                    255.255.255.0 10.5.5.0 255.255.255.0
                                          pager lines 24
                                        mtu outside 1500
                                         mtu inside 1500
                                            mtu DMZ 1500
          ip local pool vpnpool 10.5.5.10-10.5.5.20 mask
                                            255.255.255.0
                                              no failover
              icmp unreachable rate-limit 1 burst-size 1
                          asdm image disk0:/asdm-522.bin
                                  no asdm history enable
                                        arp timeout 14400
                          nat (inside) 0 access-list 100
      route outside 10.1.1.0 255.255.255.0 192.168.1.1 1
    route outside 172.16.5.0 255.255.255.0 192.168.1.1 1
               route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
                                    timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                             icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
                                0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                  sip-disconnect 0:02:00
                          timeout uauth 0:05:00 absolute
                      group-policy Defaultgroup internal
                    group-policy Defaultgroup attributes
                         default-domain value cisco.com
    username vpnuser password TXttW.eFqbHusJQM encrypted
                             username vpnuser attributes
                        group-lock value DefaultRAGroup
                                      http server enable
                            http 0.0.0.0 0.0.0.0 outside
                                http 0.0.0.0 0.0.0.0 DMZ
                                 no snmp-server location
```

no snmp-server contact snmp-server enable traps snmp authentication linkup linkdown coldstart crypto ipsec transform-set myset esp-3des esp-md5-hmac crypto dynamic-map outside_dyn_map 10 set transform-set myset crypto map outside_map 65535 ipsec-isakmp dynamic outside dyn map crypto map outside_map interface outside crypto ca trustpoint CA1 enrollment terminal subject-name cn=CiscoASA.cisco.com OU=TSWEB, O=Cisco ,Systems C=US,St=North Carolina,L=Raleigh keypair my.CA.key crl configure crypto ca certificate chain CA1 certificate 3f14b70b0000000001f 308205eb 308204d3 a0030201 02020a3f 14b70b00 00000000 1f300d06 092a8648 86f70d01 01050500 30513113 3011060a 09922689 93f22c64 01191603 636f6d31 0a099226 8993f22c 64011916 05636973 15301306 636f3115 3013060a 09922689 93f22c64 01191605 54535765 62310c30 0a060355 04031303 43413130 1e170d30 3033365a 170d3038 31323236 37313430 37313232 31343030 33365a30 67311330 11060a09 92268993 f22c6401 19160363 6f6d3115 3013060a 09922689 93f22c64 6f311530 13060a09 92268993 63697363 01191605 f22c6401 19160554 53576562 310e300c 06035504 03130555 73657273 31123010 06035504 03130976 706e7365 30819f30 0d06092a 864886f7 0d010101 72766572 05000381 8d003081 89028181 00b8e20a a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7 545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905 5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2 d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001a382 03313082 032d300b 0603551d 0f040403 02052030 34060355 1d11042d 302ba029 060a2b06 01040182 37140203 a01b0c19 76706e73 65727665 5765622e 63697363 6f2e636f 6d301d06 72405453 03551d0e 04160414 2c242ddb 490cdela fe2d63e3 le1fb28c 974c4216 301f0603 551d2304 18301680 14d9adbf 08f23a88 f114432f 79987cd4 09a403e5 58308201 03060355 1d1f0481 fb3081f8 3081f5a0 81f2a081 ef8681b5 6c646170 3a2f2f2f 434e3d43 41312c43 4e3d5453 2d57324b 332d4143 532c434e 3d434450 2c434e3d 5075626c 69632532 304b6579 6365732c 434e3d53 65727669 65727669 25323053 6365732c 434e3d43 6f6e6669 74696f6e 2c44433d 54535765 622c4443 67757261 3d636973 636f2c44 433d636f 6d3f6365 72746966 69636174 65526576 6f636174 696f6e4c 6973743f 62617365

3f6f626a 65637443 6c617373 3d63524c 44697374 72696275 74696f6e 506f696e 7474703a 2f2f7473 2d77326b 332d6163 74863568 732e7473 7765622e 63697363 6f2e636f 6d2f4365 7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06 010f3082 010b3081 a906082b 01010482 01050507 06010505 07300286 819c6c64 61703a2f 2f2f434e 3d434131 2c434e3d 4149412c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f634143 65727469 66696361 74653f62 6173653f 6f626a65 6374436c 6173733d 63657274 69666963 6174696f 6e417574 686f7269 7479305d 06082b06 3a2f2f74 732d7732 68747470 30028651 01050507 6b332d61 63732e74 73776562 2e636973 636f2e63 6f6d2f43 65727445 6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e 63697363 6f2e636f 6d5f4341 312e6372 74301506 092b0601 1e060045 00460053 300c0603 14020408 04018237 551d1301 01ff0402 30003015 0603551d 25040e30 0c060a2b 06010401 82370a03 04304406 092a8648 86f70d01 090f0437 3035300e 06082a86 4886f70d 03020202 0080300e 06082a86 4886f70d 06052b0e 03020730 0a06082a 00803007 03040202 864886f7 0d030730 0d06092a 864886f7 0d010105 05000382 010100bf 99b9daf2 e24f1bd6 ce8271eb 908fadb3 772df610 0e78b198 f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e 20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427 fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1 2355c358 a22af8bb e5194b42 69a7c2f6 c5a116f6 d9d77fb3 a7f3d201 e3cff8f7 48f8d54e 243d2530 31a733af 0e1351d3 9c64a0f7 4975fc66 a017627c cfd0ea22 2992f463 9412b388 84bf8b33 bd9f589a e7087262 a4472e69 775ab608 e5714857 4f887163 705220e3 aca870be b107ab8d 73faf76d b3550553 la2b873f 156f9dff 5386c839 1380fda8 945a7f6c c2e9d5c8 83e2e761 394dd4da 63eaefc6 a44df5 quit certificate ca 7099f1994764e09c4651da80a16b749c 3082049d 30820385 a0030201 02021070 99f19947 64e09c46 51da80a1 6b749c30 0d06092a 864886f7 0d010105 05003051 31133011 060a0992 268993f2 2c640119 1603636f 6d311530 13060a09 92268993 f22c6401 19160563 6973636f 31153013 060a0992 268993f2 2c640119 16055453 57656231 0c300a06 03550403 13034341 31301e17 0d303731 32313430 36303134 335a170d 31323132 31343036 31303135 5a305131 13301106 0a099226 8993f22c 64011916 03636f6d 31153013 060a0992 268993f2 2c640119 16056369 73636f31 15301306

0a099226 8993f22c 64011916 6562310c 300a0603 55040313 03434131 05545357 30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101 00ea8fee c7ae56fc a22e603d 0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d 28ece906 02902f9a d1eb2b8d f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd ale906ec 88b32a19 38e5353e 6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621 876bd678 c8a37109 f074eabe 2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7 24b9e054 063c60a4 9b8d3c09 351bc630 05f69357 833b9197 f875b408 cb71a814 69alf331 bleb2b35 0c469443 1455c210 db308bf0 a9805758 a878b82d 38c71426 afffd272 dd6d7564 1cbe4d95 b81c02b2 9b56ec2d 5a913a9f 9b95cafd dfffcf67 94b97ac7 63249009 fa05ca4d 6f13afd0 968f9f41 e492cfe4 e50e15f1 c0f5d13b 5f020301 0001a382 016f3082 016b3013 06092b06 01040182 37140204 061e0400 43004130 0b060355 1d0f0404 300f0603 551d1301 01ff0405 30030101 03020186 ff301d06 03551d0e 04160414 d9adbf08 f23a88f1 14432f79 987cd409 a403e558 30820103 0603551d 1f0481fb 3081f830 81f5a081 f2a081ef 8681b56c 6461703a 2f2f2f43 4e3d4341 312c434e 3d54532d 57324b33 2d414353 2c434e3d 4344502c 434e3d50 75626c69 63253230 4b657925 32305365 72766963 65732c43 4e3d5365 72766963 65732c43 4e3d436f 6e666967 75726174 696f6e2c 44433d54 53576562 2c44433d 63697363 6f2c4443 3d636f6d 3f636572 74696669 63617465 5265766f 63617469 6f6e4c69 73743f62 6173653f 6f626a65 6374436c 6173733d 63524c44 69737472 69627574 696f6e50 6f696e74 86356874 74703a2f 2f74732d 77326b33 2d616373 2e747377 65622e63 6973636f 2e636f6d 2f436572 74456e72 6f6c6c2f 4341312e 63726c30 1006092b 00300d06 092a8648 04030201 82371501 06010401 86f70d01 01050500 03820101 001abc5a 40b32112 22da80fb bb228bfe 4bf8a515 df8fc3a0 4e0c89c6 d725e2ab 2fa67ce8 9196d516 dfe55627 953aea47 2e871289 6b754e9c 1e01d408 3f7f0595 8081f986 526fbe1c c9639d6f 258b2205 0dc370c6 5431b034 fe9fd60e 93a6e71b ab8e7f84 a011336b 37c13261 5ad218a3 a513e382 e4bfb2b4 9bf0d7d1 99865cc4 94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92 860152d4 f06b2b15 df306433 c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196 34f693ea f3beee4d aa2ef1c2 edba288f 3a678ecb 3809d0df b1699c76 13018f9f 5e3dce95 efe6da93 f4cb3b00 102efa94 48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad quit crypto isakmp enable outside crypto isakmp policy 65535

```
authentication rsa-sig
                                encryption 3des
                                       hash md5
                                        group 2
                                 lifetime 86400
                    crypto isakmp identity auto
 tunnel-group DefaultRAGroup general-attributes
                          address-pool vpnpool
             default-group-policy Defaultgroup
   tunnel-group DefaultRAGroup ipsec-attributes
                                trust-point CA1
                                telnet timeout 5
                                   ssh timeout 5
                               console timeout 0
                                               !
                   class-map inspection_default
              match default-inspection-traffic
                                               !
                                               !
     policy-map type inspect dns preset_dns_map
                                     parameters
                   message-length maximum 512
                       policy-map global_policy
                      class inspection_default
                   inspect dns preset_dns_map
                                   inspect ftp
                            inspect h323 h225
                             inspect h323 ras
                               inspect netbios
                                   inspect rsh
                                  inspect rtsp
                                inspect skinny
                                 inspect esmtp
                                inspect sqlnet
                                inspect sunrpc
                                 inspect tftp
                                   inspect sip
                                 inspect xdmcp
                                               !
            service-policy global_policy global
                        prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0
                                           end :
                                       #CiscoASA
```

<u>تكوين عميل شبكة VPN</u>

أتمت هذا steps in order to شكلت ال VPN زبون:

1. حدد Start **(البدء) > Programs (البرامج) > Cisco Systems VPN Client (عميل الشبكة الخاصة الظاهرية** (VPN)>من أجل تشغيل برنامج عميل شبكة VPN.

	-		
na	***	Programs	
Si.		Documents	Cisco Systems VPN Client Uninstall VPN Client
fes	5	Settings	VPN Client
Ы		Search	Cisco Systems Inc. VPN Client
800			
SI	~	Help	
ą	<u>Z.</u>	Run	
M		Shut Down	
1	itart	🖸 🥭 🐺 🔂 🕴	🖾 C:\WINNT\sys 🔄 Prabu 🖉 Microsoft Certi 🖓 untitled - Paint 🧔
_	cisco	 ورکبت هو في vPN o	. أتمت هذا steps in order to جلبت ال CA شهادة من ال CA نادل يعين CA1
	E.	ندم المتوفرة ل	زبون:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام تكوينات المستخ
		ile Edit View	Favorites Tools Help
	4		R AL @ Search GR Equaritan @ Madia / ALE
			P P A Quearch M Favorices Symeola S I E
	C	ddress 🙋 http://17	2.16.5.1/certsrv
		Enter No	twork Password
		<u> ()</u>	Please type your user name and password.
			Cite: 1721651
			User Name
			Password xxxxxx
			Domain
			Save this password in your password list
خاة	م ام		OK Carl youl lear
	∟مد <i>ح</i>) أو	ِ فوق تنزیل شهادة CA	تأكد من وجود حساب مستخدم لمستخدم عميل شبكة VPN مع خادم CA.انقر

: تاكد من وجود حساب مستخدم لمستخدم عميل شبكة VPN مع خادم CA.انقر فوق **تنزيل شهادة CA او سلسلة شهادات أو CRL** ، ثم حدد زر راديو Base 64 لتحديد طريقة التشفير.انقر على **تنزيل شهادة المرجع المصدق**.



قم بحفظ شهادة المرجع المصدق على الكمبيوتر باستخدام اسم **certnew.cer**. بشكل افتراضي، يحفظ الملف

File Dow	nload
?	Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open o save this file.
	File name: certnew.cer
	File type: Security Certificate
	From: 172.16.5.1
	This type of file could harm your computer if it contains malicious code.
	Would you like to open the file or save it to your computer?
à	<u>Open</u> <u>Save</u> Cancel <u>M</u> ore Info

client.انقر فوق **استيراد**.يظهر مربع حوار يوضح أن الشهادة تم إستيرادها.

C:\Program Files\Cisco Systems\VPN

👌 sta	atus: Disc	onnected	VPN Clie	ent - Ve	ersion 4.	8.02.00)10			
Conne	ection Entr	ies Status	Certificat	es Log	Option:	s Help				
Vi	iew	F E	Export		≕ ■ Enroll	V eri	ify	XX Delete		
Conne	ection Ent	ries Certi	ficates	Log						
Numb	er	Certi	ficate				Store	Δ	Key Size	
0	👌 VPN (Client Iı	mport Cer	tificat	e					
	⊙ Imp	ort from <u>F</u> ile								
		Import <u>P</u> ath	ram Files\	Cisco S	ystems\V	PN Clier	nt\certne	w.cer	<u>B</u> rowse	
	Impor	rt P <u>a</u> ssword:		Client						
	C Imp	ort from <u>M</u> icr	ʻ 🚺	Certil	ficate suc	cessfully	/ importe	ed.		
Not co	Impor	rt C <u>e</u> rtificate:		·	ОК				v	
	Enter identi	ing a new pa ity certificate	a :s					sswo	rd protect	
	<u>Ν</u> ε	ew Password	±:							
	<u>C</u> onfi	rm Password	±							
						[<u>I</u> mp	ort	Cancel	جاح.
							ي صفحة	CA Cer ف	tificates CA1 ات.	ظهر 1 شهاد
Connection	n Entries S	tatus Certifica	ates Log Op	otions He	elp					
View) 🚺	rt Expor	t Enro		San	XX Delete			սի 619	uli sco
Connectio	on Entries	Certificates	Log							
umber		Certificate			Store	Δ	Key Si	ize	Validity	

ملاحظة: تأكد من تحديد خيار **عرض شهادات CA/RA**، وإلا فإن شهادات CA لن تظهر في نافذة

14

🤪 status: Disconnect	ted ¥PN Clie	nt - Version 4.8	.02.0010
<u>Connection Entries</u> Sta	itus C <u>e</u> rtificato	s Log Options	<u>H</u> elp
	<u>⊻</u> iew.		
View Import	Impo	rt	
Connection Entries	Certif E <u>x</u> po	rt	
Number	Enrol		H
0 C	A1 Verify	<u>.</u>	ľ
	D <u>e</u> let	e	Π
	⊆han	ge Certificate Pas	sword
	<u>R</u> etri	eve Approved Cer	rtificate
	Show	CA/RA Certificat	es

3. أتمتّ هذا steps in order to جلبت الهوية شهادة وركبت هو في ال VPN زبون:في CA Server CA1، أختر **طلب شهادة > طلب شهادة متقدم > إنشاء طلب وإرساله إلى هذا CA** للتسجيل لشهادة الهوية.انقر على **إرسال**.

Certificate Template:	
User	
Key Options:	
Create new key set O Use existing	key set
CSP: Microsoft Enhanced Cryptographic Provide	er v1.0 💌
Key Usage: 🔎 Exchange	
Key Size: 1024 Min: 384 Max:16384 ^{(common key sizes: 512} 10	024 2048 4096 8192 16384)
O U	ser specified key container na
Mark keys as exportable Export keys to file	
Enable strong private key protection	
Store certificate in the local computer of Stores the certificate in the local comp instead of in the user's certificate store install the root CA's certificate. You m administrator to generate or use a key machine store.	ertificate store outer store e. Does not ust be an r in the local
Additional Options:	
Request Format: © CMC © PKCS10	
Hash Algorithm: MD5 💌 Only used to sign request.	
Save request to a file	
	انقر فوق نعم السليمة
Potential Scripting Violation	للمتابعة. 2
This Web site is requesting a new certificate on your behalf. You should allow only tr Do you want to request a certificate now?	rusted Web sites to request a certificate for you
Yes No	
Cortificate laguad	
The certificate you requested was issued to	o you.
<u>انقر</u> <u>Install this certificate</u>	انقر على تثبيت هذه الشهادة .لــــــــ

			للمتابعة.
Potential Scripting Violation			
This Web site is adding one or more certificates to security risk. The Web site could install certificate computer and gain access to your data Do you want this program to add the certificates	to this computer. Allowing an un es you do not trust, which could : now? Click.Yes if you trust this	ntrusted Web site to u d allow programs that : Web site. Otherwise,	pdate your certificates is a vou do not trust to run on this , click No.
	Yes No		
	هو موضح في هذه	شهادة المثبتة كما	بحب أن تتلقى رسالة الب
Microsoft Certific	ate Services CA	A1	
Certificate Inst	talled		
Your pow cortifu	cato hac hoon c	uccoccfully	inctalled
our new cerum اقم بالخروج ثم اعادة	cale has been s	accessiuny	الصورة:
دمة التيويب "الشفادات" الخاصة يعميا . VPN	ية المثبتة بالظمور في علا	ماح لشفادة القور	ر. تشغيا عميا ، VPN للس
			کما هو موضح في هذه
			الصورة [.] الصورة
Connection Entries Status Certificates Log Option	s Help		العقورة.
View Import Export Enroll	Verifu Delete		ahaha cisco
Connection Entries Certificates Eby			(
Number Certificate	Store 🛆	Key Size	Validity
CA1	CA.	2048	until Dec 14. 2012 11:40
Users + vpnuser	Microsoft	1024	until Dec 25, 2008 18:27:

4. أتمت هذا steps in order to خلقت توصيل مدخل (*vpnUser*):انقر على علامة تبويب إدخالات الاتصال ثم انقر على **جديد**.أدخل عنوان IP للنظير البعيد (الموجه) في حقل المضيف.حدد زر **مصادقة الشهادة**، واختر شهادة الهوية من القائمة المنسدلة.طقطقة

Connection Entry, vpnuser Description: Host 192.168.1.5 Authentication Transport Backup Servers Dial-Up G Group Authentication Name: Password: Confirm Password: Confirm Password: Send CA Certificate Chain Erase User Password Save Cancel Connection Entries Status Certificates Log Options Help	er Ration pnuser (Microsoft) te Chain Save Cancel bas Save Cancel bas Version 4.8.02.0010 og Options Help Nodiy Delete
Description:	81.5 sport Backup Servers Dial-Up n Mutual Group Authentication ation pruser (Microsoft) te Chain Save Cancel Save Cancel Save Cancel Version 4.8.02.0010 recut: Modify Delete
Host: 192.168.1.5 Authentication Transport Backup Servers Dial-Up Group Authentication Mutual Group Authentication Name: Password: Confirm Password: Confirm Password: Certificate Authentication Name: Name: U-Users + vpruser (Microsoft) Send CA Certificate Chain Save Cancel Save Status: Disconnected VPN Client - Version 4.8.02.0010 Image: Connection Entries Status: Status Certificates Log Options Help	1.5 sport Backup Servers Dial-Up n Mutual Group Authentication ation pnuser (Microsoft) ▼ the Chain Save Cancel back Save Cancel
Authentication Transport Backup Servers Dial-Up Group Authentication Mutual Group Authentication Name: Password: Confirm Password: Confirm Password: Confirm Password: Save Cancel Save Erase User Password Save Cancel Status: Disconnected VPN Client - Version 4.8.02.0010	sport Backup Servers Dial-Up n Mutual Group Authentication ation pnuser (Microsoft) حفظ ate Chain Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel
Certificate Authentication Name: Password: Confirm Password: Confirm Password: Send CA Certificate Chain Erase User Password Save Cancel Concel Connection Entries Status Certificates Log Options Help	n Mutual Group Authentication ation pnuser (Microsoft) ب ate Chain Save Cancel Save Cancel Save Save Cancel Save Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel Save Cancel
Name: Password: Confirm Password: Confirm Password: Confirm Password: Send Cathentication Name: Users + vpnuser (Microsoft) Send CA Certificate Chain Erase User Password Save Cancel status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Certificates Log Options Help	ation pnuser (Microsoft) ate Chain Save Cancel babes Save Cancel Save Cancel Save Cancel کو علی Save Cancel
Password: Confirm Password: Certificate Authentication Name: 0 · Users + vpnuser (Microsoft) Send CA Certificate Chain Erase User Password Save Cancel Save Cancel Connection Entries Status Certificates Log Options Help	ation pnuser (Microsoft) te Chain Save Cancel Save Cancel Save Cancel Save Cancel Cancel د انقر علی Save Cancel د انقر علی Save Cancel د انقر علی Save Cancel
Confirm Password: Certificate Authentication Name: U - Users + vpnuser (Microsoft) Send CA Certificate Chain Erase User Password Save Cancel Save Save Cancel Connection Entries Status Certificates Log Options Help	eation pnuser (Microsoft) te Chain Save Cancel Save Cancel ste Juint Cisco Lebes Lebes Lebes Lebes Lebes Lebes
Certificate Authentication Name: D-Users + vpnuser (Microsoft) Send CA Certificate Chain Erase User Password Save Cancel Lancel Save Cancel Connection Entries Status Certificates Log Options Help Connection Entries Status Certificates Log Options Help	eation pnuser (Microsoft) whe Chain Save Cancel Save Cancel
Name: U-Users + vpnuser (Microsoft) Send CA Certificate Chain Erase User Password Save Cancel Save Cancel Status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Certificates Log Options Help	aation pnuser (Microsoft) Inte Chain Save Cancel Save Cancel List Save Save Cancel List Save Cancel List Save Cancel List Save Cancel List Save Cancel List Save Cancel List Save Cancel List Save Cancel List Cancel List Cancel C
Send CA Certificate Chain Erase User Password Save Cancel Save Cancel Save Cancel Connection Entries Status Certificates Log Options Help Save Cancel Connection Entries Status Certificates Log Options Help Connection Entries Status Certificates Log Options Help	Alte Chain Save Cancel Save Cancel
Erase User Password Save Cancel	Save Cancel حفظ. 5. انقر على 5. انقر على Version 4.8.02.0010 مع Options Help مع المالي Modify Delete
Erase User Password Save Cancel علی status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Certificates Log Options Help	حفظ. Save Cancel
Status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Certificates Log Options Help	حفظ Cancel جفظ Save Cancel 5. انقر علی Tersion 4.8.02.0010 مع Options Help مع المال Modify Delete
کلی Status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Certificates Log Options Help	tie, على توصيل. Version 4.8.02.0010 مو Options Help Modify Delete L
Status: Disconnected VPN Client - Version 4.8.02.0010 Connection Entries Status Connection Entries Sta	Version 4.8.02.0010
Connectorizates Status Certaintates Eug Options help	Modify Delete CISCO
	Modify Delete CISCO
Cancel Connect New Import Modify Delete CISC	
Connection Entry A Host Transport	Host Transport
vpnuser 192.168.1.5 IPSec/UDP	192.168.1.5 IPSec/UDP

6. أدخل معلومات اسم المستخدم وكلمة المرور للإرسال عند طلبها، ثم انقر على **موافق** للاتصال بالشبكة

Enter Username and CISCO SYSTEMS	d Password. Username: 🕅 Password: 🏾	/pnuser	OK		Cano	el	ä. – II
		یح فی هذه	A کما هو موض	مع ASA	ية VPN	میل شبک	، ببعیده 7. یتصل ع
	status: Con	nected \	PN Clienty - V	ersion	4.8.01	.0300	
9	onnection Entr	ies <u>S</u> tatus	Certificates	Log	Options	Help	الصورة:

<u>التحقق من الصحة</u>

على ال ASA أنت يستطيع استعملت عدة عرض أمر في الأمر خط in order to دققت الحالة من شهادة.

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

```
• show crypto ca trustPoint_يعرض نقاط الثقة التي تم تكوينها.
                                      CiscoASA#show crypto ca trustpoints
                                                           :Trustpoint CA1
                                                         :Subject Name
                                                                cn=CA1
                                                              dc=TSWeb
                                                              dc=cisco
                                                                dc=com
                Serial Number: 7099f1994764e09c4651da80a16b749c
                                               .Certificate configured
          • show crypto ca certificate—يعرض جميع الشهادات المثبتة على النظام.
                                     CiscoASA#show crypto ca certificates
                                                               Certificate
                                                       Status: Available
                        Certificate Serial Number: 3f14b70b0000000001f
                                          Certificate Usage: Encryption
                                       (Public Key Type: RSA (1024 bits
                                                            :Issuer Name
                                                                cn=CA1
                                                              dc=TSWeb
                                                              dc=cisco
                                                                dc=com
                                                           :Subject Name
                                                          cn=vpnserver
                                                              cn=Users
                                                              dc=TSWeb
                                                              dc=cisco
                                                                dc=com
                               PrincipalName: vpnserver@TSWeb.cisco.com
                                                :CRL Distribution Points
,ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services
                                                                  [1]
                                     CN=Services, CN=Configuratio
  =n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass
                                                 cRLDistributionPoint
          http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl [2]
                                                          :Validity Date
                                 start date: 14:00:36 UTC Dec 27 2007
```

date: 14:00:36 UTC Dec 26 2008

end

```
Associated Trustpoints: CA1
                                                                CA Certificate
                                                           Status: Available
                 Certificate Serial Number: 7099f1994764e09c4651da80a16b749c
                                                Certificate Usage: Signature
                                            (Public Key Type: RSA (2048 bits
                                                                 :Issuer Name
                                                                     cn=CA1
                                                                  dc=TSWeb
                                                                  dc=cisco
                                                                    dc=com
                                                                :Subject Name
                                                                    cn=CA1
                                                                  dc=TSWeb
                                                                  dc=cisco
                                                                    dc=com
                                                    :CRL Distribution Points
     ,ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services [1]
                                          CN=Services, CN=Configuratio
        =n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass
                                                      cRLDistributionPoint
                http://ts-w2k3-acs.tsweb.cisco.com/CertEnroll/CA1.crl [2]
                                                               :Validity Date
                                      start date: 06:01:43 UTC Dec 14 2007
                                      end date: 06:10:15 UTC Dec 14 2012
                                                 Associated Trustpoints: CA1
              • show crypto ca crl—يعرض قوائم إبطال الشهادات المخزنة مؤقتا (CRL).
  • show crypto key mypubkey rsa— يعرض جميع أزواج مفاتيح التشفير التي تم إنشاؤها.
                                         CiscoASA#show crypto key mypubkey rsa
                           Key pair was generated at: 01:43:45 UTC Dec 11 2007
                                                    <Key name: <Default-RSA-Key
                                                   Usage: General Purpose Key
                                                    Modulus Size (bits): 1024
                                                                     :Key Data
     30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00d4a509
     99e95d6c b5bdaa25 777aebbe 6ee42c86 23c49f9a bea53224 0234b843 1c0c8541
     f5a66eb1 6d337c70 29031b76 e58c3c6f 36229b14 fefd3298 69f9123c 37f6c43b
     4f8384c4 a736426d 45765cca 7f04cbal 29a95890 84d2c5d4 adeeb248 a10b1f68
2fe4b9b1 5fa12d0e 7789ce45 55190e79 1364aba4 7b2b21ca de3af74d b7020301 0001
                           Key pair was generated at: 06:36:00 UTC Dec 15 2007
                                                           Key name: my.CA.key
                                                   Usage: General Purpose Key
                                                    Modulus Size (bits): 1024
                                                                     :Key Data
     30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00b8e20a
     a8332356 b75b6600 735008d3 735d23c5 295b9247 2b5e02a8 1f63dc7a 570667d7
     545e7f98 d3d4239b 42ab8faf 0be8a5d3 94f80d01 a14cc01d 98b1320e 9fe84905
     5ab94b18 ef308eb1 2f22ab1a 8edb38f0 2c2cf78e 07197f2d 52d3cb73 91a9ccb2
d903f722 bd414b0a 3205aa05 3ec45e24 6480606f 8e417f09 a7aa9c64 4d020301 0001
                           Key pair was generated at: 07:35:18 UTC Dec 21 2007
                                                                      #CiscoASA
                            • show crypto isakmp sa— يعرض معلومات نفق IKE 1.
                                                CiscoASA#show crypto isakmp sa
                                                               Active SA: 1
   (Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
                                                               Total IKE SA: 1
```

Type

: user

IKE Peer: 10.1.1.5

Role : responder

1

```
Rekey
                                     : no
                                                       State
                                                               : MM_ACTIVE

    IPSec ipSec sa - يعرض معلومات نفق IPSec.

                                                 CiscoASA#show crypto ipsec sa
                                                             interface: outside
              Crypto map tag: dynmap, seq num: 10, local addr: 192.168.1.5
                (local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0
     (remote ident (addr/mask/prot/port): (10.5.5.10/255.255.255.255/0/0
                               current_peer: 10.1.1.5, username: vpnuser
                                    dynamic allocated peer ip: 10.5.5.10
                      pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0#
                pkts decaps: 144, #pkts decrypt: 144, #pkts verify: 144#
                              pkts compressed: 0, #pkts decompressed: 0#
  pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0#
    pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                        send errors: 0, #recv errors: 0#
        local crypto endpt.: 192.168.1.5, remote crypto endpt.: 10.1.1.5
                        path mtu 1500, ipsec overhead 58, media mtu 1500
                                          current outbound spi: FF3EEE7D
                                                          :inbound esp sas
                                            (spi: 0xEFDF8BA9 (4024404905
                                transform: esp-3des esp-md5-hmac none
                                      { ,in use settings ={RA, Tunnel
                           slot: 0, conn_id: 4096, crypto-map: dynmap
                       sa timing: remaining key lifetime (sec): 28314
                                                     IV size: 8 bytes
                                          replay detection support: Y
                                                          :outbound esp sas
                                            (spi: 0xFF3EEE7D (4282314365
                                transform: esp-3des esp-md5-hmac none
                                      { ,in use settings ={RA, Tunnel
                           slot: 0, conn_id: 4096, crypto-map: dynmap
                       sa timing: remaining key lifetime (sec): 28314
                                                     IV size: 8 bytes
                                          replay detection support: Y
```

تدعم <u>أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر</u> show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر show .

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

فيما يلي بعض الأخطاء المحتملة التي قد تواجهها:

- خطأ: فشل تحليل الشهادة المستوردة أو التحقق منها</mark>يمكن أن يحدث هذا الخطأ عندما تقوم بتثبيت شهادة الهوية وليس لديك شهادة CA الوسيطة أو الجذر الصحيحة التي تم مصادقتها مع TrustPoint المقترنة. يجب عليك إزالة وإعادة المصادقة باستخدام شهادة CA الوسيطة أو الجذر الصحيحة. اتصل بمورد الجهة الخارجية للتحقق من أنك إستلمت شهادة المرجع المصدق الصحيحة.
- لا تحتوي الشهادة على مفتاح عام للأغراض العامة</mark>قد يحدث هذا الخطأ عند محاولة تثبيت شهادة هويتك في TrustPoint غير صحيح. تحاول تثبيت شهادة هوية غير صحيحة، أو أن زوج المفاتيح المقترن ب TrustPoint لا يطابق المفتاح العام الموجود في شهادة الهوية. أستخدم الأمر show crypto ca certificates للتحقق من تثبيت شهادة هويتك على TrustPoint الصحيح. ابحث عن السطر الذي يحدد **نقاط**

الثقة المقترنة. إذا تم سرد نقطة الثقة الخطأ، فاستخدم الإجراءات الموضحة في هذا المستند لإزالة نقطة الثقة المناسبة وإعادة تثبيتها. تحقق أيضا من عدم تغيير زوج المفاتيح منذ إنشاء CSR.

• خ**طاً: ASA/PIX. SEV=Warning/3 IKE/0xE300081 معرف شهادة عن بعد غير صالح:**أنت أمكن إستلمت هذا خطأ في ال VPN زبون إن يقع مشكلة مع الشهادات أثناء صحة هوية. لحل هذه المشكلة، أستخدم الأمر ASA/PIX في تكوين crypto isakmp identity auto.

معلومات ذات صلة

- <u>صفحة دعم أجهزة الأمان المعدلة من Cisco</u>
 - <u>صفحة دعم عميل شبكة VPN من Cisco</u>
- أجهزة الأمان Cisco PIX 500 Series Security Appliances أجهزة الأمان
 - مراجع أوامر جدار حماية PIX الآمن من <u>Cisco</u>
 - <u>الإعلامات الميدانية لمنتج الأمان (بما في ذلك PIX)</u>
 - <u>طلبات التعليقات (RFCs)</u>
 - <u>الدعم التقني والمستندات Cisco Systems</u>

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