مصادقة IPSec لعميل ASA/PIX 7.x و VPN باستخدام شهادات رقمية باستخدام مثال تكوين Microsoft CA

المحتويات

المقدمة

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

المتطلبات الأساسية

المتطلبات

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 و VeriSign.

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

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

المكونات المستخدمة

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

- ASA 5510 الذي يشغل الإصدار 7.2(2) من البرنامج و ASDM الإصدار 5.2(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.

المنتجات ذات الصلة

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

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

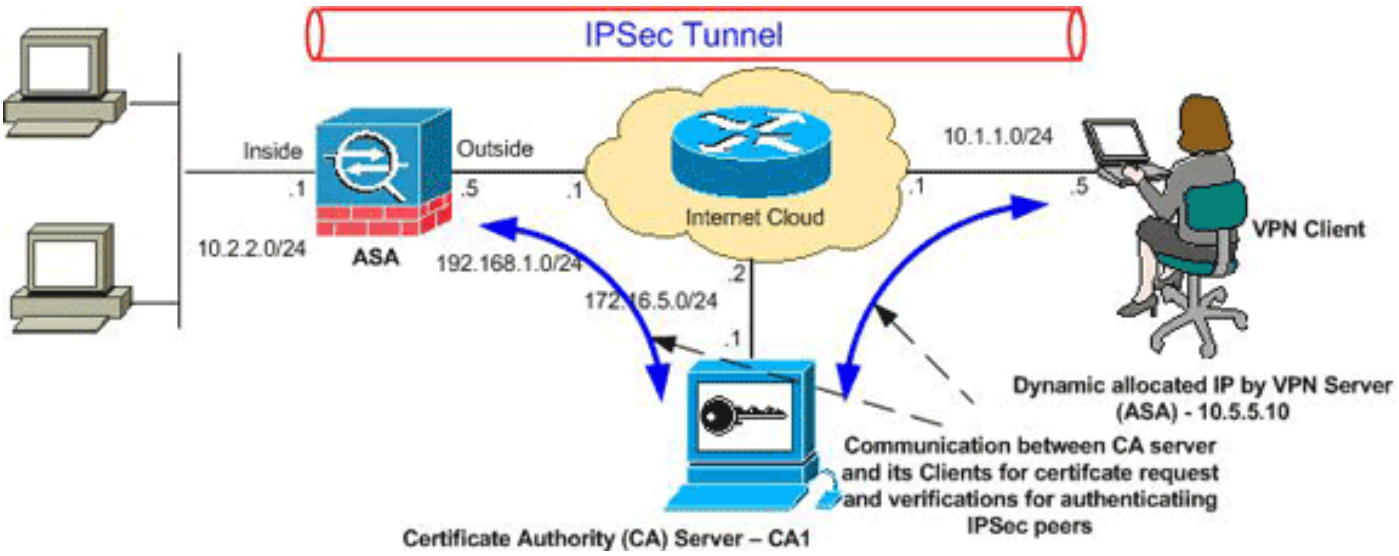
التكوين

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

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

الرسم التخطيطي للشبكة

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.

التكوينات

يستخدم هذا المستند التكوينات التالية:

تكوين ASA

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

الخطوة 1. التحقق من دقة قيم التاريخ والوقت والمنطقة الزمنية

الخطوة 2. إنشاء زوج مفاتيح RSA

الخطوة 3. قم بإنشاء TrustPoint.

الخطوة 4. إنشاء تسجيل الشهادة.

الخطوة 5. مصادقة TrustPoint

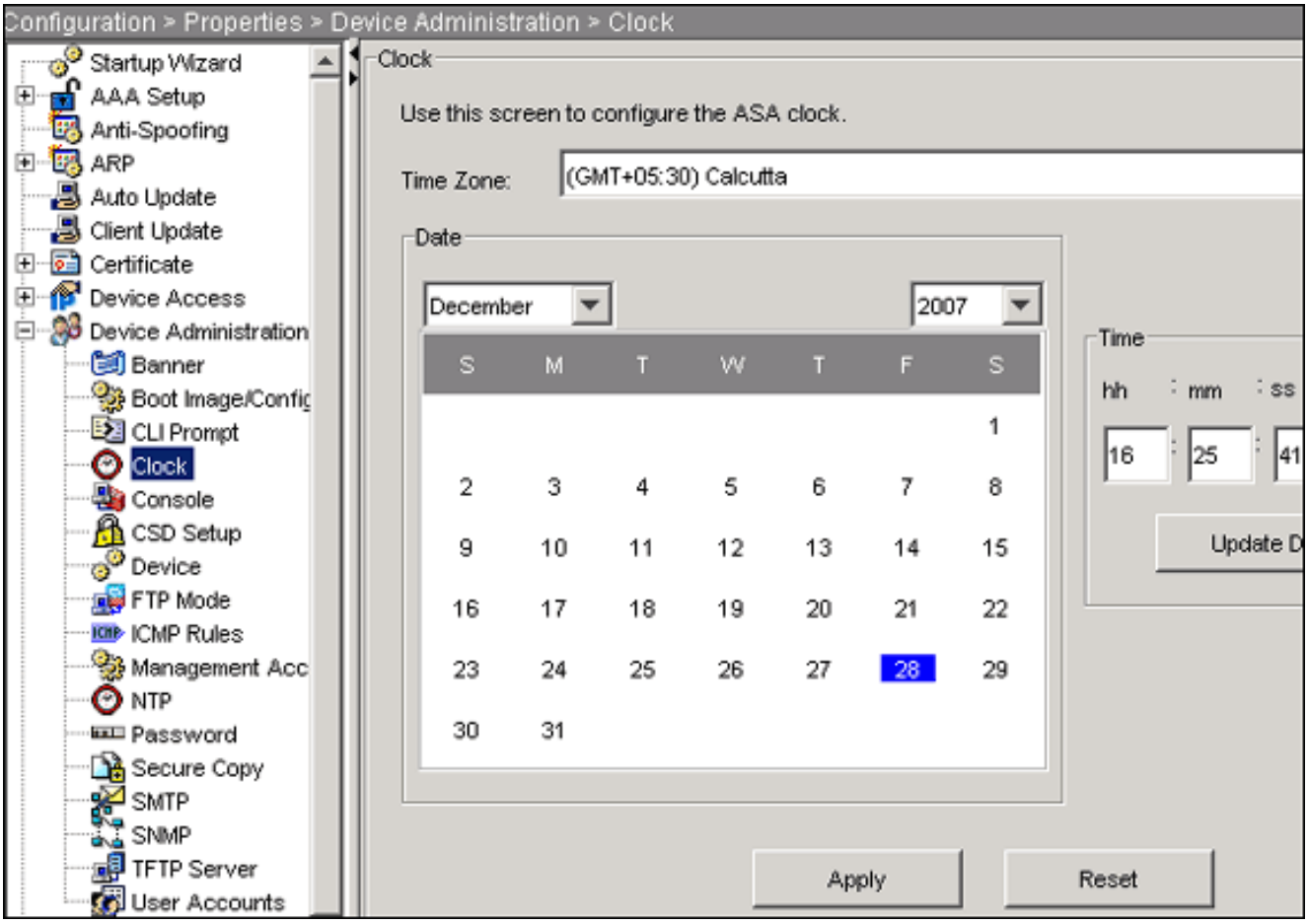
الخطوة 6. تثبت الشهادة

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

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.



مثال على سطر الأوامر

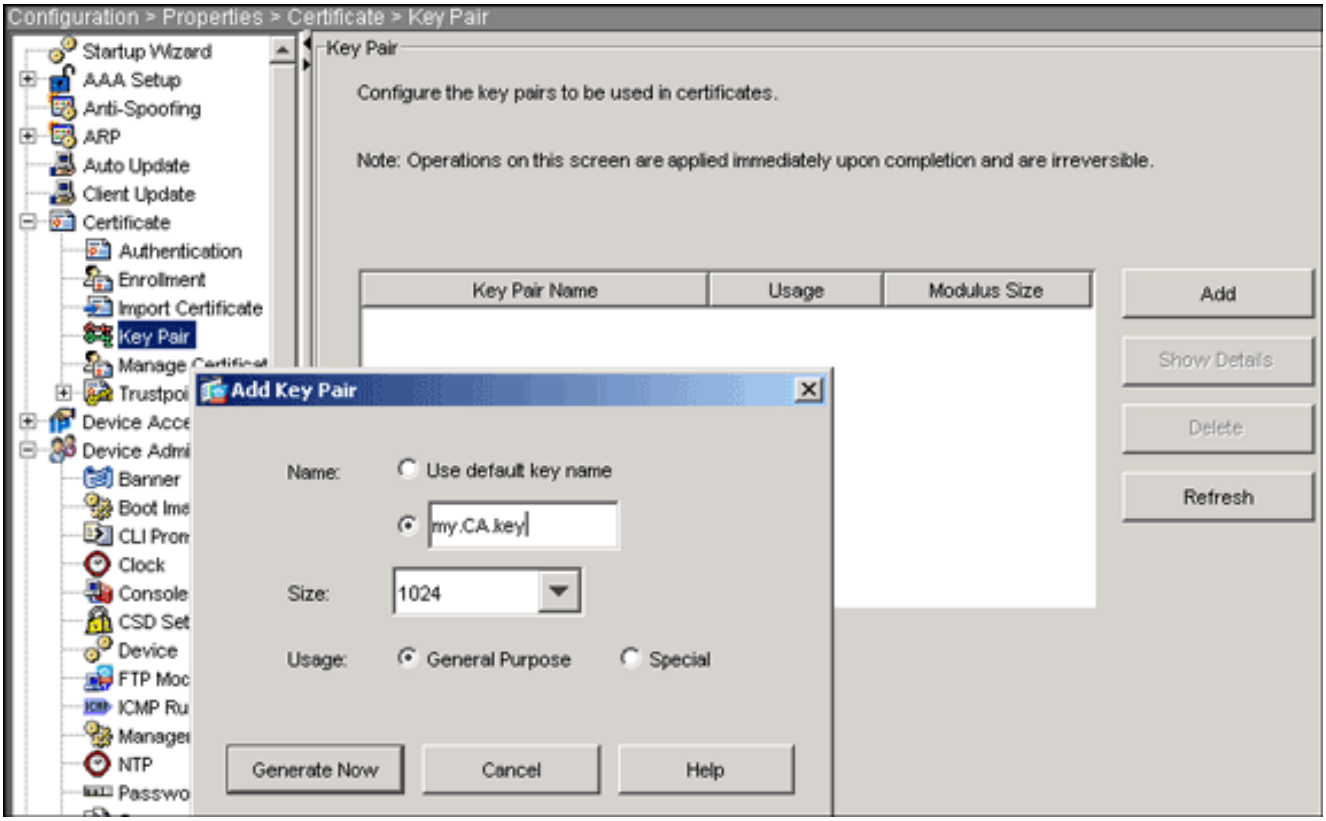
Cisco ASA
CiscoASA#**show clock** IST Fri Dec 28 2007 16:25:49.580

الخطوة 2. إنشاء زوج مفاتيح RSA

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).



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

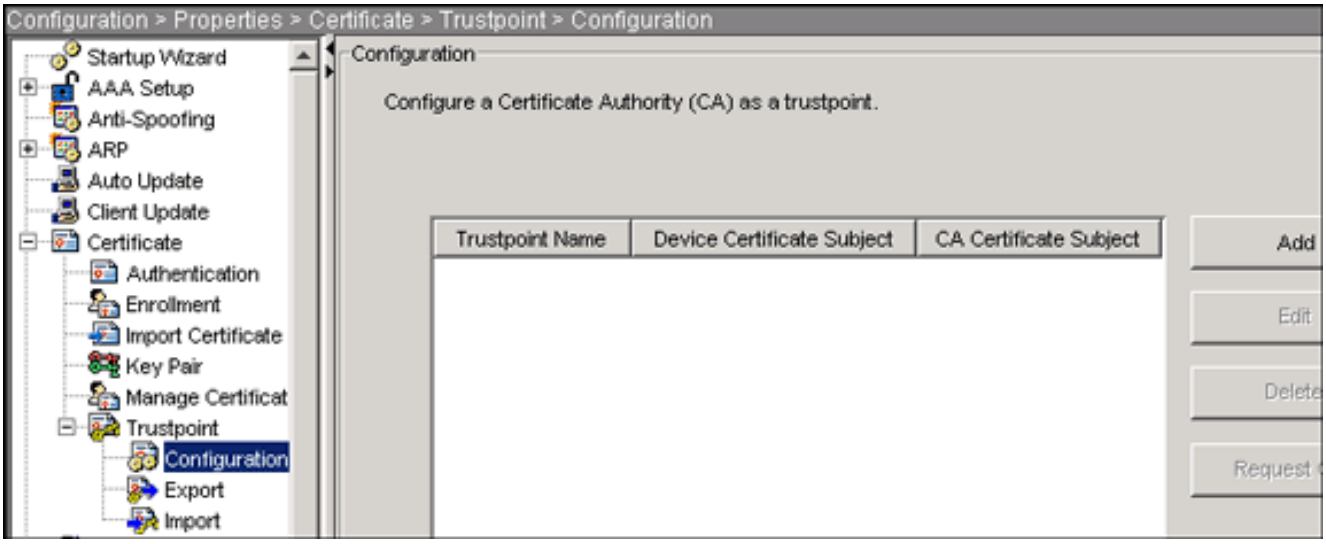
Cisco ASA
CiscoASA#**configure terminal** CiscoASA(config)#**crypto key generate rsa label my.CA.key modulus 1024** *Generates 1024 bit RSA key pair. "label" defines ---! the name of the key pair.* INFO: The name for the keys will be: my.CA.key Keypair generation process begin. #(Please wait... ciscoasa(config

الخطوة 3. إنشاء TrustPoint

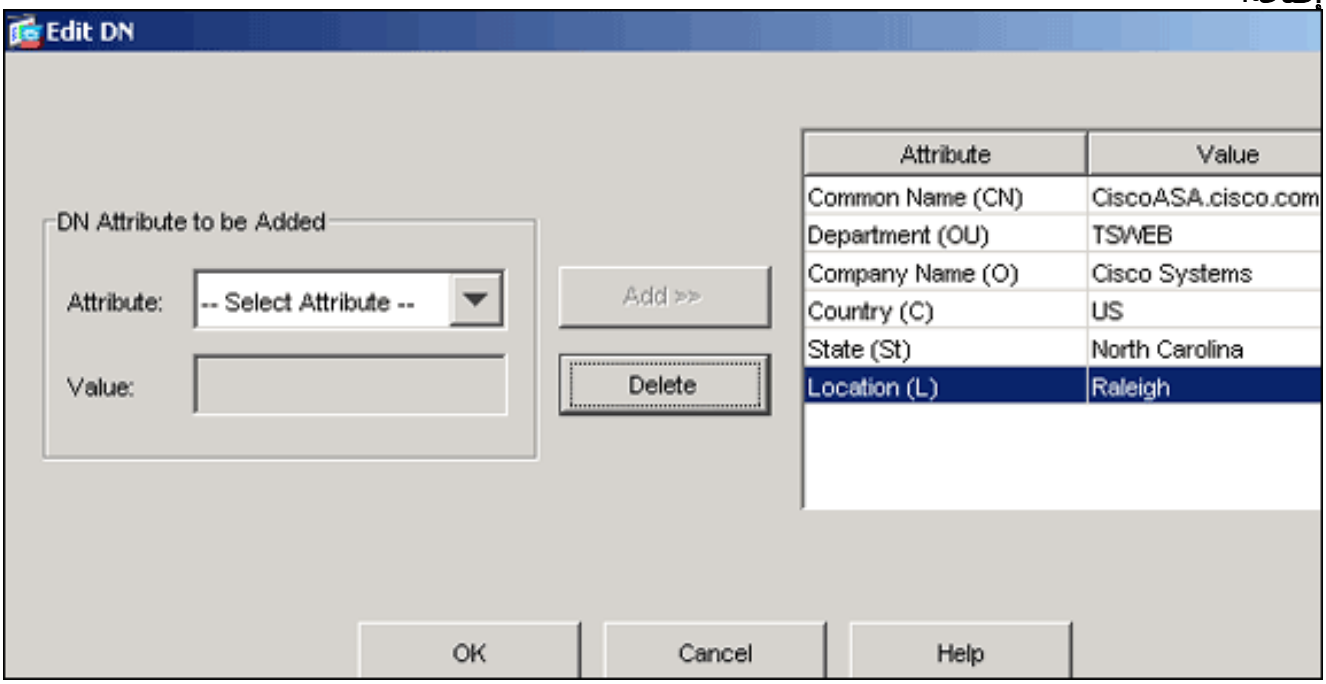
يلزم توفر نقاط الثقة لإعلان المرجع المصدق (CA) الذي سيستخدمه ASA.

إجراء ASDM

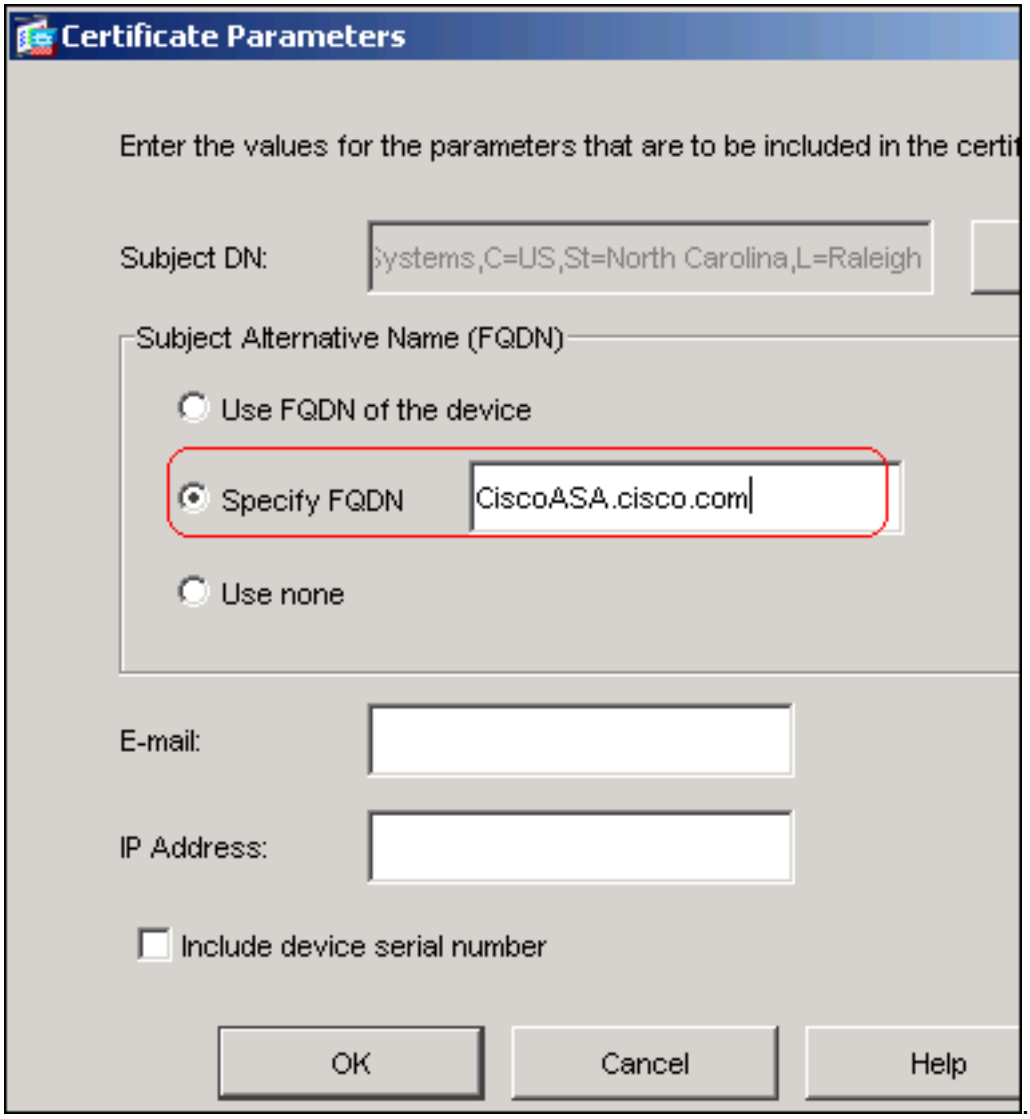
1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، ثم قم بتوسيع **TrustPoint**.
3. أخترت **تشكيل**، وبعد ذلك طقطقت **يضيف**.



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 الخطوة 2 (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**.

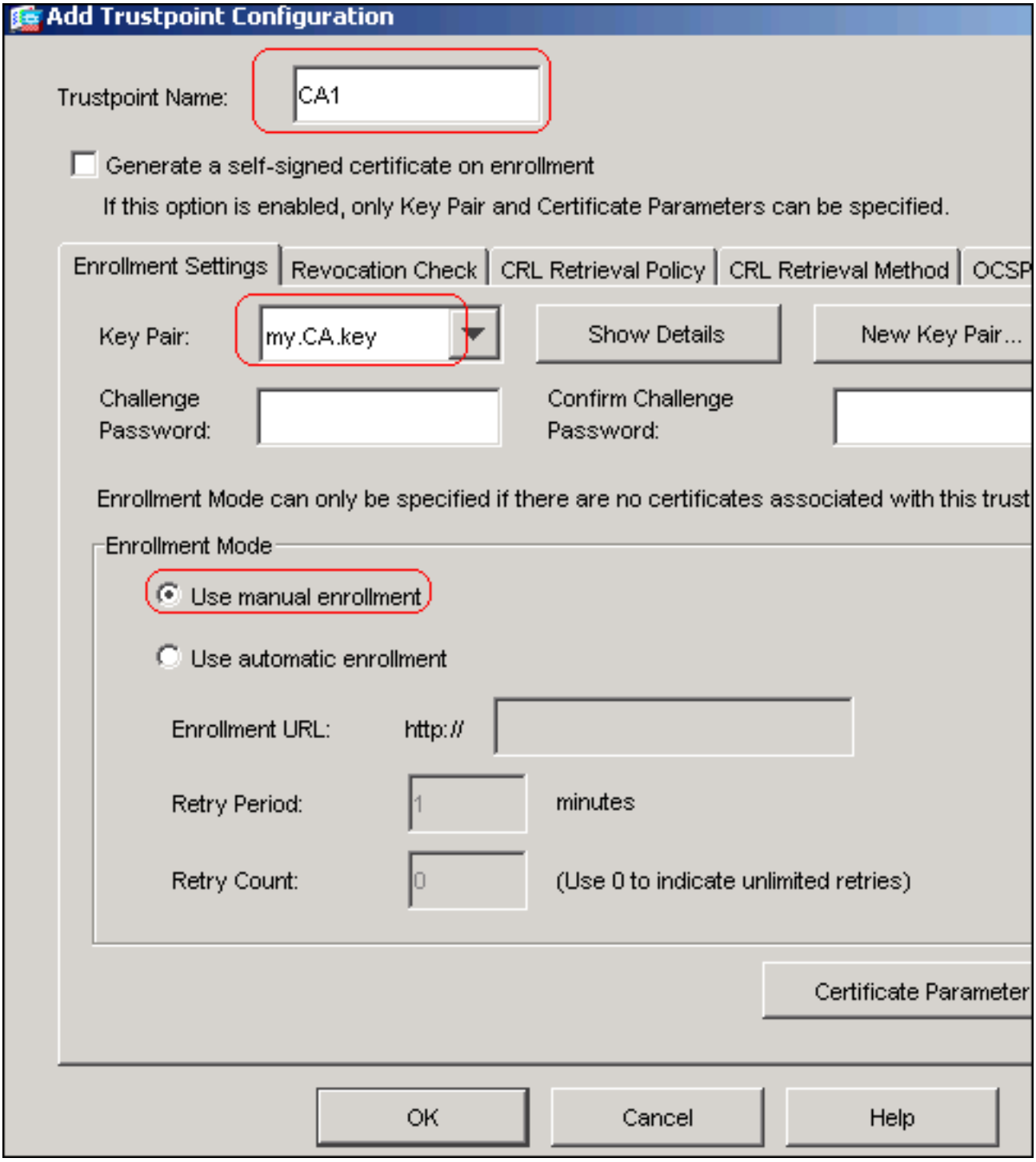


8. بمجرد إضافة القيم المناسبة، انقر فوق **موافق**.
9. في شاشة معلمات الشهادة، أدخل FQDN في حقل تحديد FQDN.يجب أن تكون هذه القيمة نفس FQDN التي أستخدمتها للاسم الشائع



(CN).

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**.



مثال على سطر الأوامر

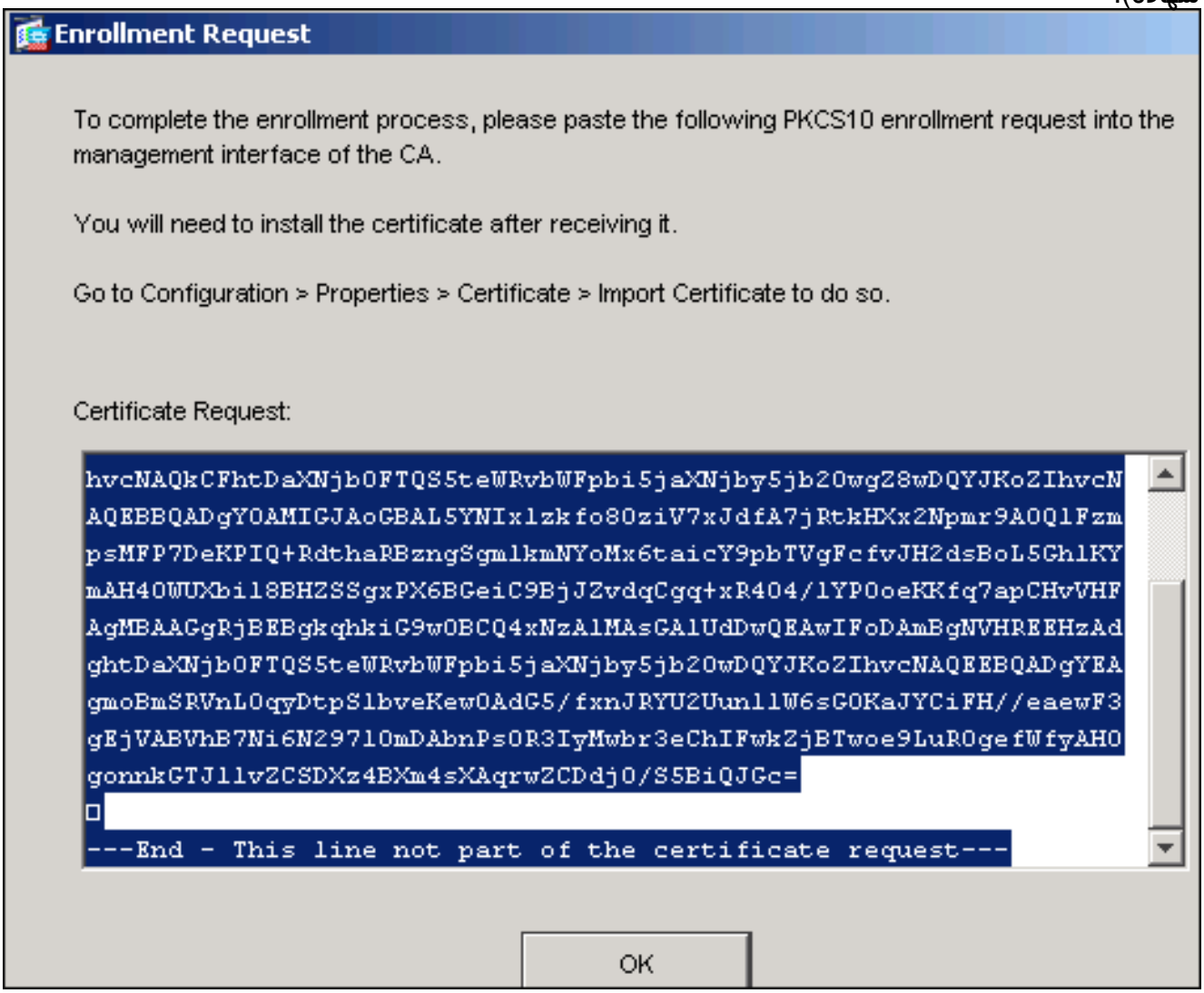
Cisco ASA
CiscoASA(config)#**crypto ca trustpoint CA1** *Creates the trustpoint.* CiscoASA(config-ca- *---!* trustpoint)#**enrollment terminal** *Specifies cut and paste enrollment with this ---!* *trustpoint.* CiscoASA(config-ca-trustpoint)#**subject-name** **,CN=wepvpn.cisco.com,OU=TSWEB** **O=Cisco**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

```
ca-trustpoint)#keypair my.CA.key

                                    Specifies key pair generated in Step 2. ---!
CiscoASA(config-ca-trustpoint)#fqdn CiscoASA.cisco.com


                                    Specifies subject alternative name (DNS:). ---!
CiscoASA(config-ca-trustpoint)#exit
```

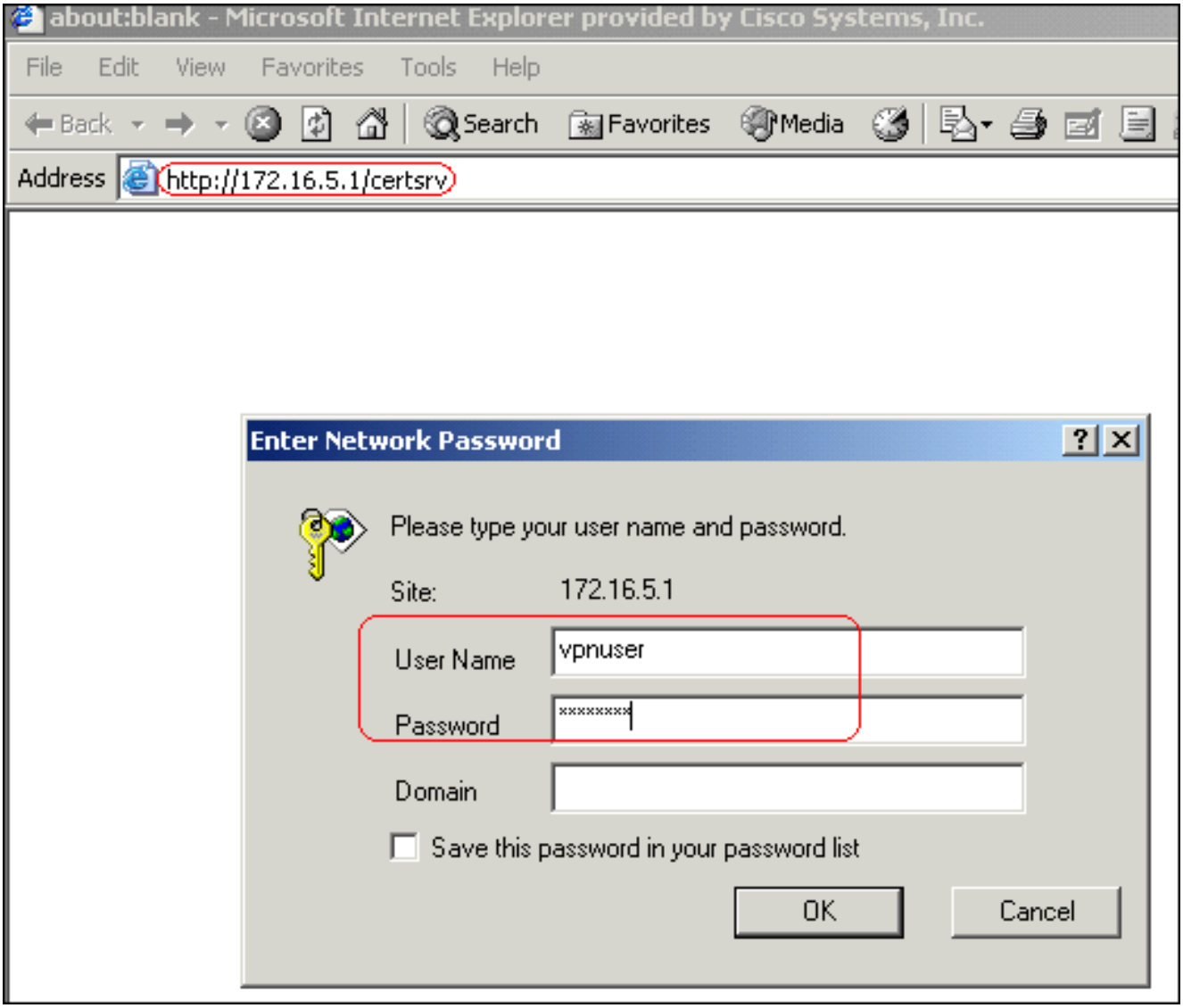
الخطوة 4. إنشاء تسجيل الشهادة

إجراء ASDM

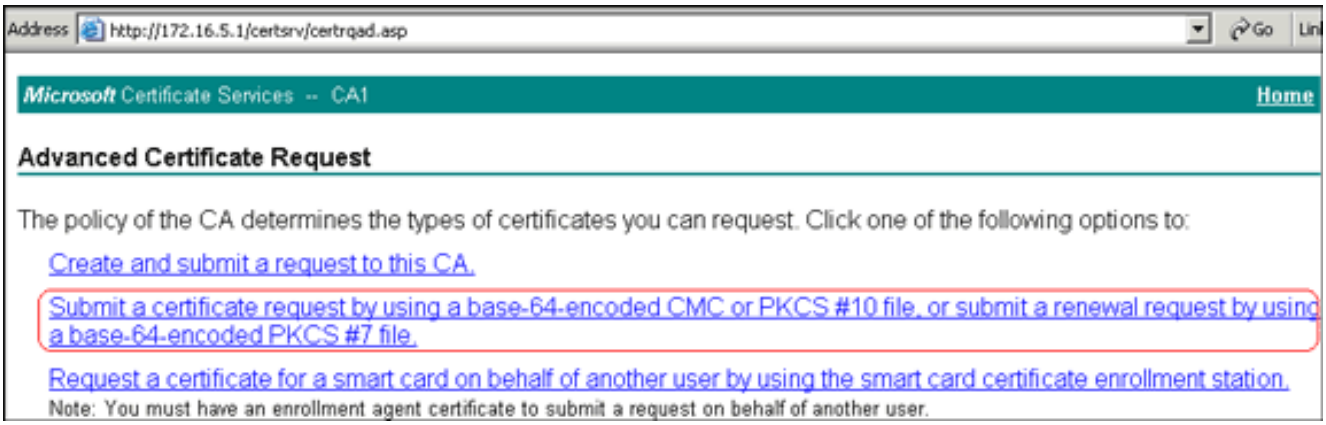
1. انقر فوق **تكوين**، ثم انقر فوق **خصائص**.
2. قم بتوسيع **الشهادة**، واختر **التسجيل**.
3. تحقق من تحديد TrustPoint الذي تم إنشاؤه في الخطوة 3، وانقر فوق **تسجيل**.يظهر مربع حوار يسرد طلب تسجيل الشهادة (يشار إليه أيضا باسم طلب توقيع شهادة).



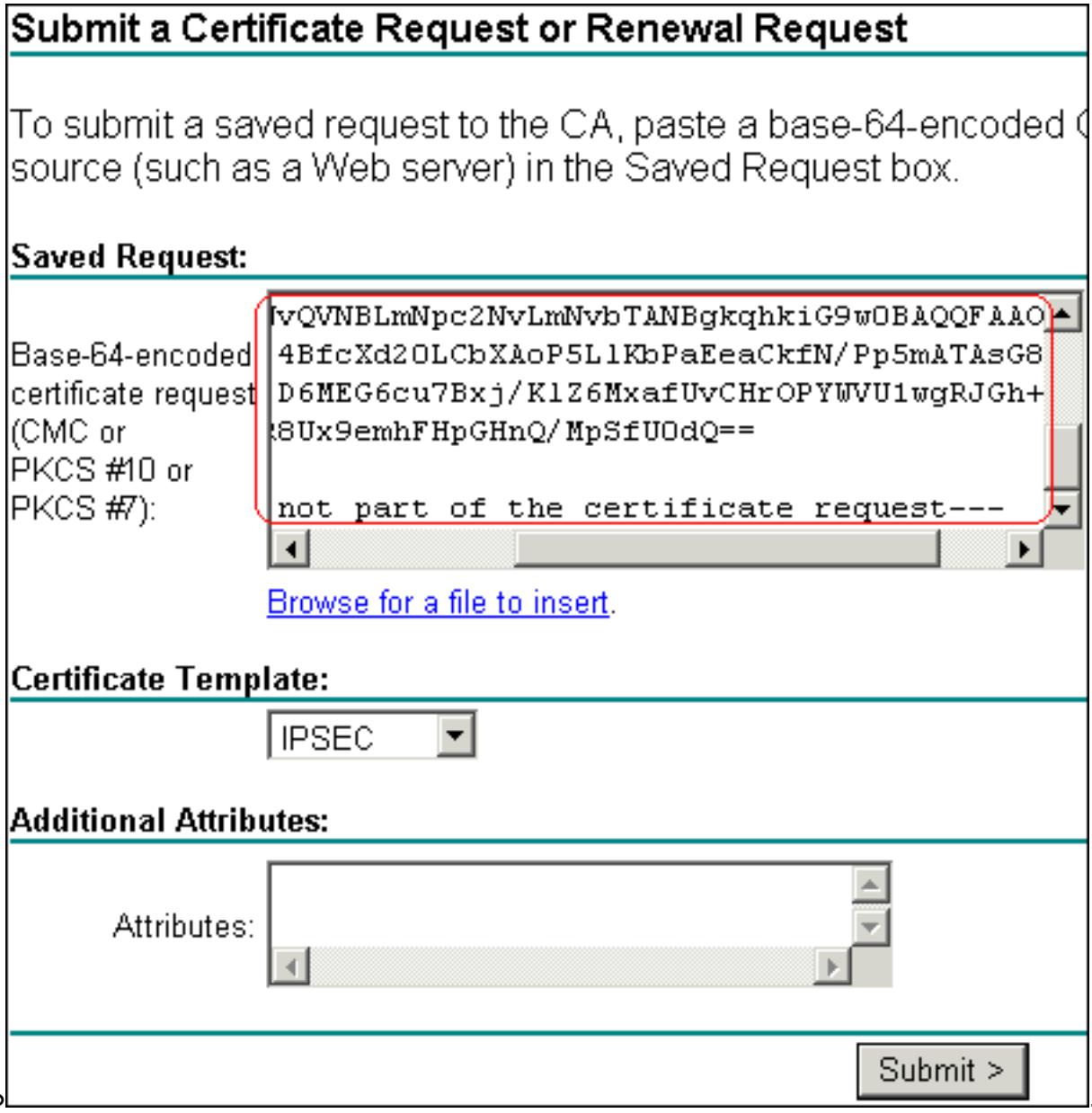
4. انسخ طلب تسجيل PKCS#10 إلى ملف نصي، ثم أرسل CSR المحفوظ إلى مورد الطرف الثالث (مثل Microsoft CA) كما هو موضح في هذا الإجراء:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام بيانات المستخدم المتوفرة لخادم VPN.



ملاحظة: تأكد من وجود حساب مستخدم لخادم VPN) ASA) مزود بخادم CA.انقر فوق **طلب شهادة > طلب 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-64.**

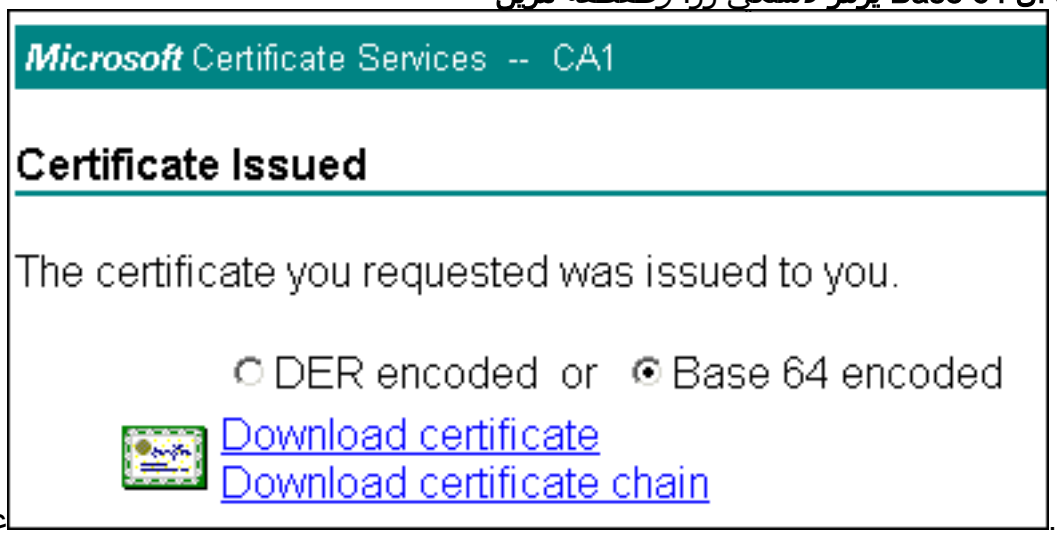


انسخ المعلومات التي تم ترميزها ولصقها في حقل نص **الطلب المحفوظ**، وانقر



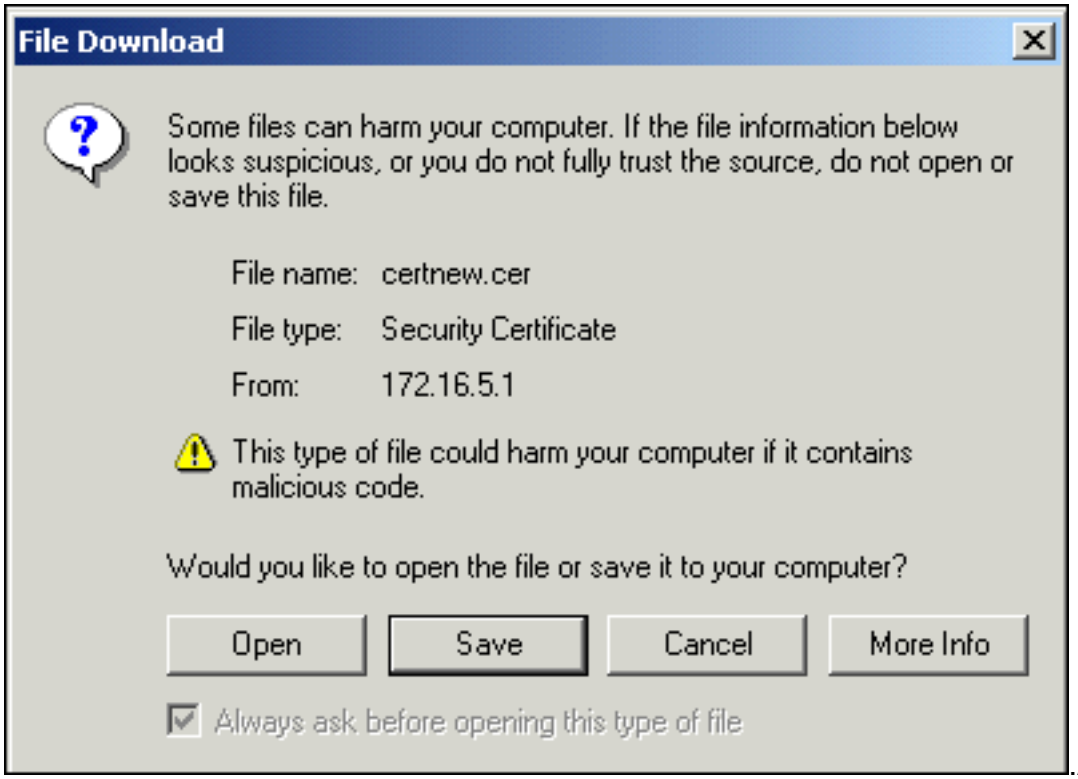
ط**إرسال**.

قطقت ال **Base 64 يرمز** لاسلكي زر، وطقطقة **تنزيل**



عندما يظهر **شهادة**.

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



.ASA

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
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
                                                  dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
                                                  bTEhMB8G
CSqGSIb3DQEJAhYSY2lzY29hc2EuY2lzY28uY29tMIGfMA0GCSqGSIb3
                                                  DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
                                                  9M4yTx5b
Fm886s8F73WsfQPynBDfBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
                                                  3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
                                                  gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBBYw
```

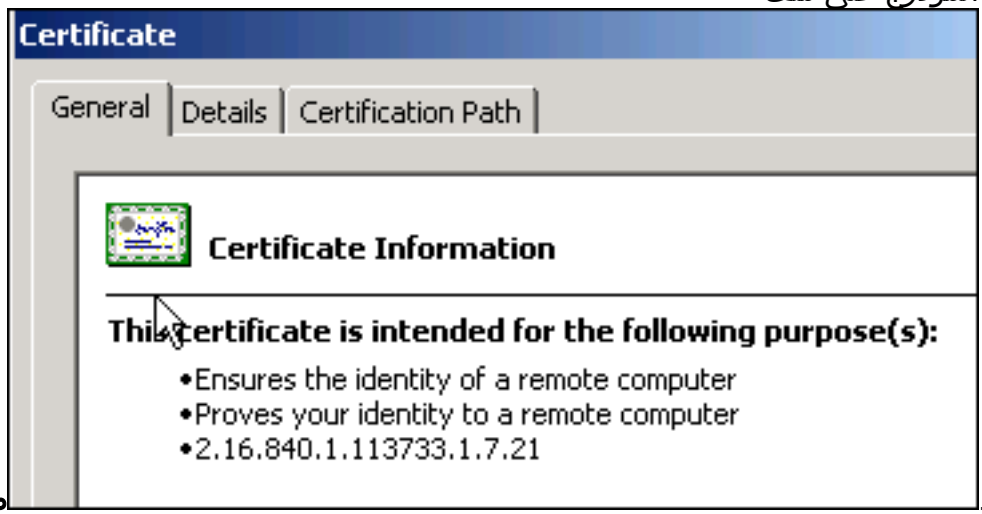
```
                                                                FIISY2lz
Y29hc2EuY2lzY28uY29tMA0GCSqGSIb3DQEBBAUAA4GBABrxpY0q7SeO
                                                                HZf3yEJq
po6wG+oZpsvpYI/HemKUlaRc783w4BMO5lulIEnHgRqAxrTbQn0B7JPI
                                                                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
```

الخطوة 5. مصادقة TrustPoint

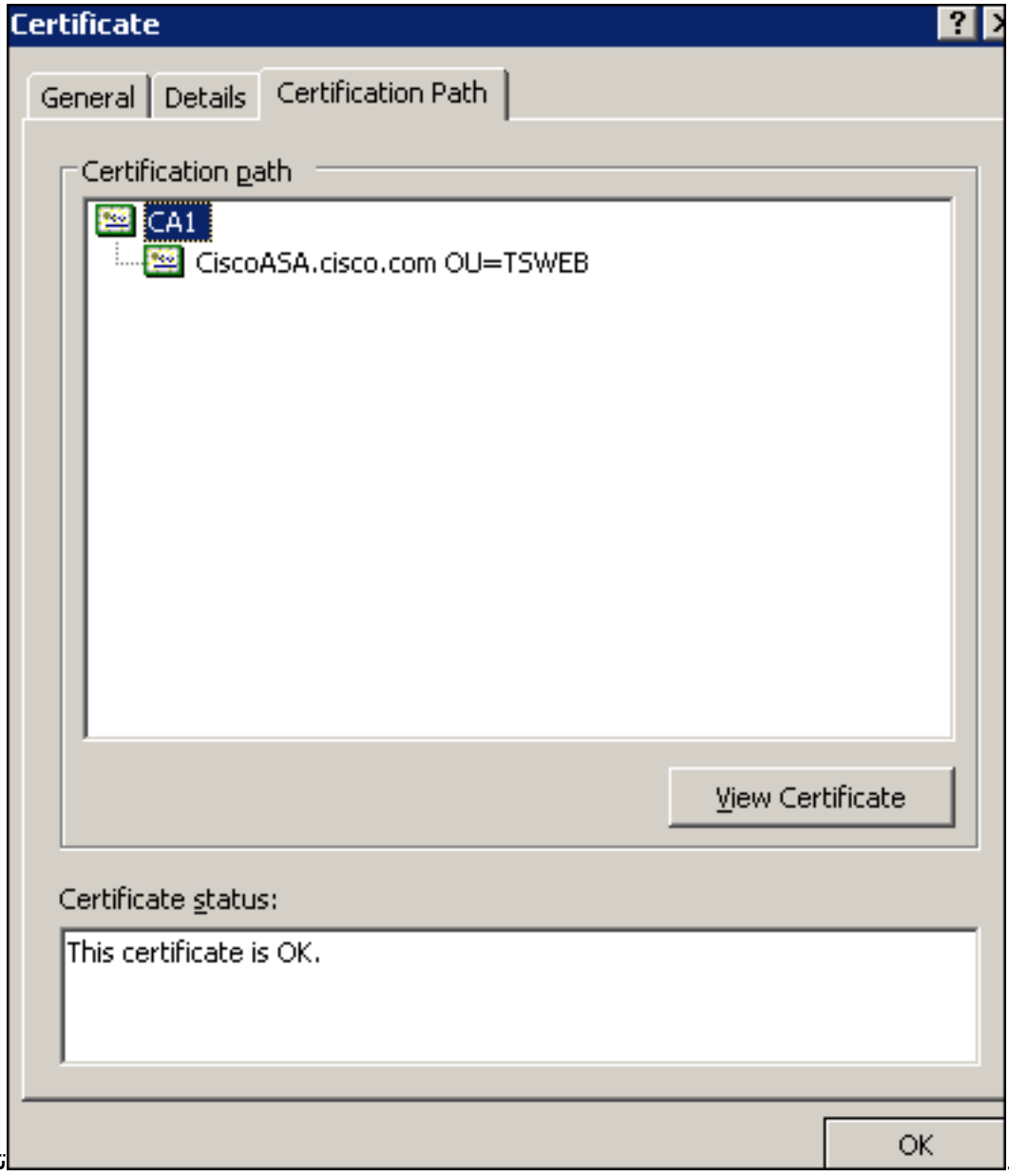
بمجرد إستلام شهادة الهوية من مورد الطرف الثالث، يمكنك المتابعة بهذه الخطوة.

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 بامتداد .cer.**ملاحظة:** بمجرد إعادة تسمية الملف بامتداد .cer، يجب أن تظهر أيقونة الملف كشهادة كما هو موضح. 

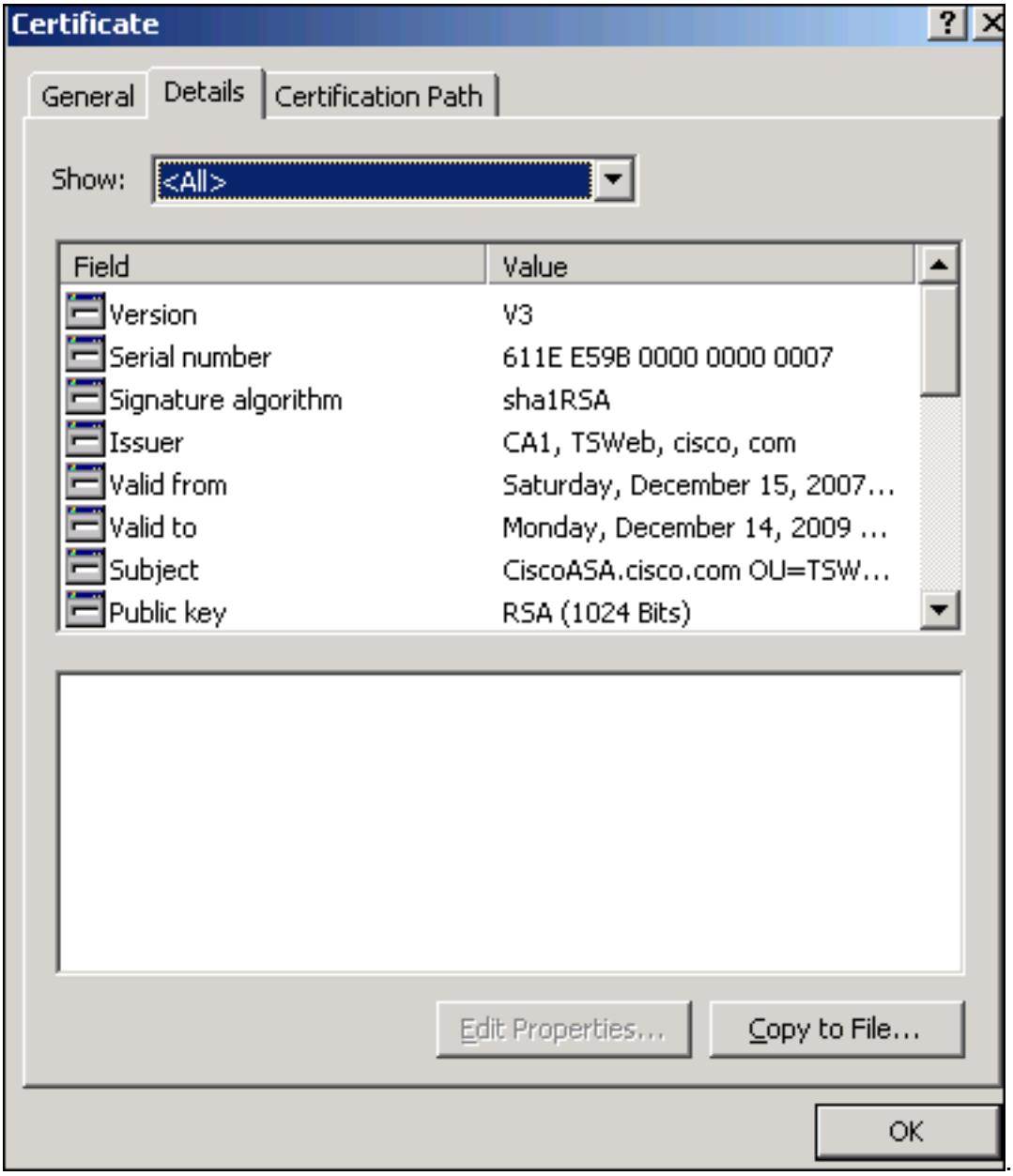
4. قم بالنقر المزدوج على ملف الترخيص. 

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**



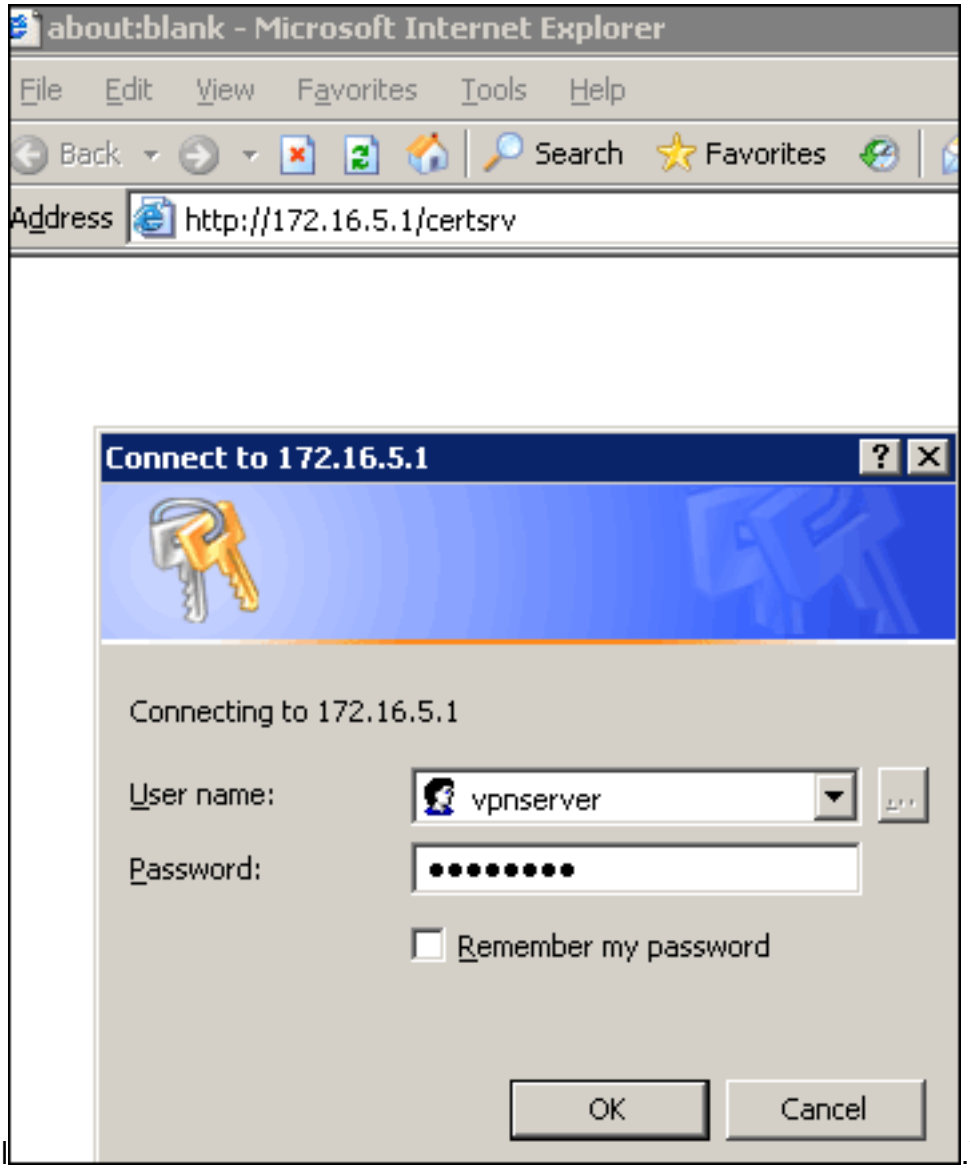
تظهر **الشهادة**. معلومات تفصيلية حول شهادة المرجع المصدق.

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

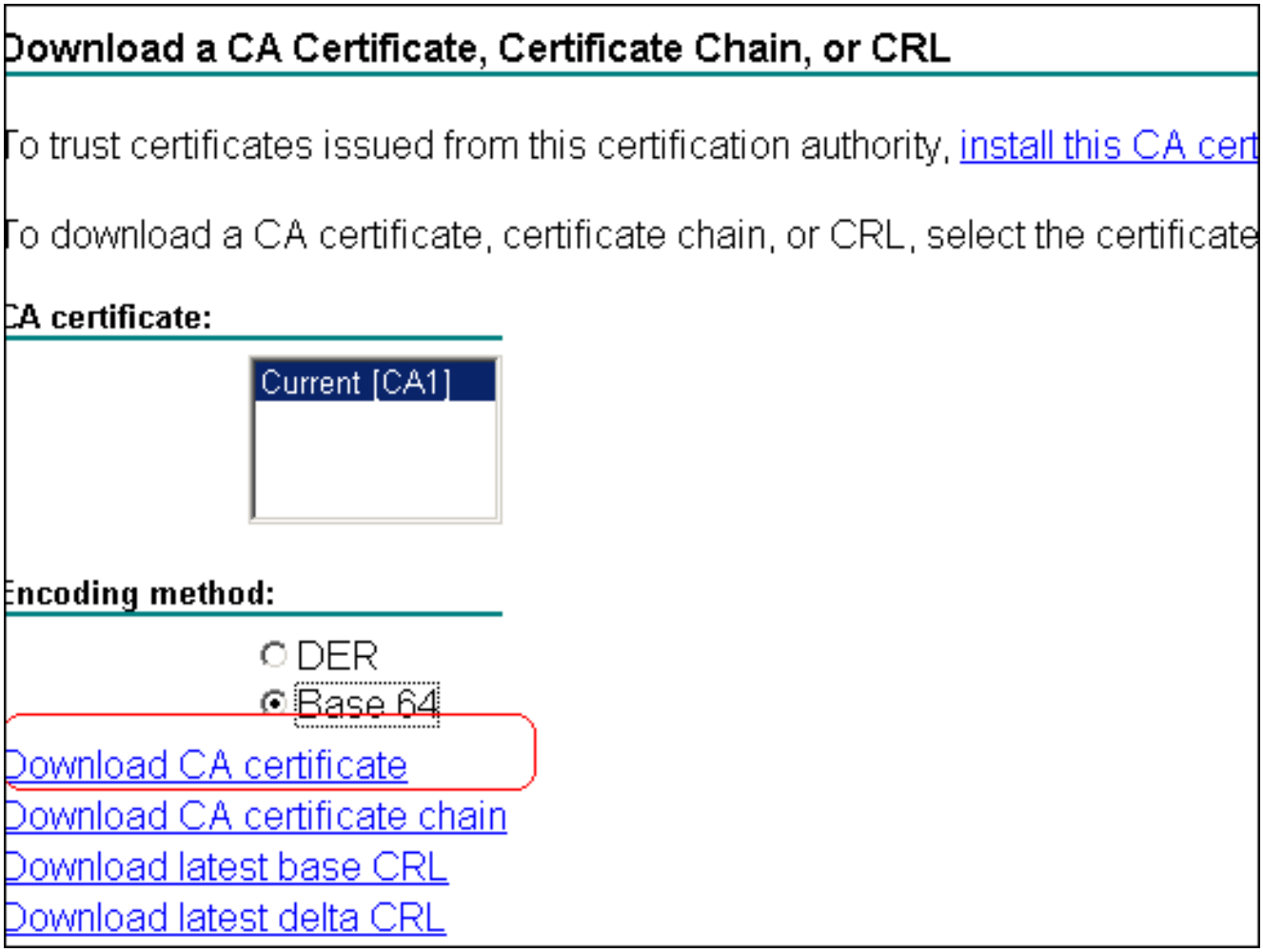


الهوية.

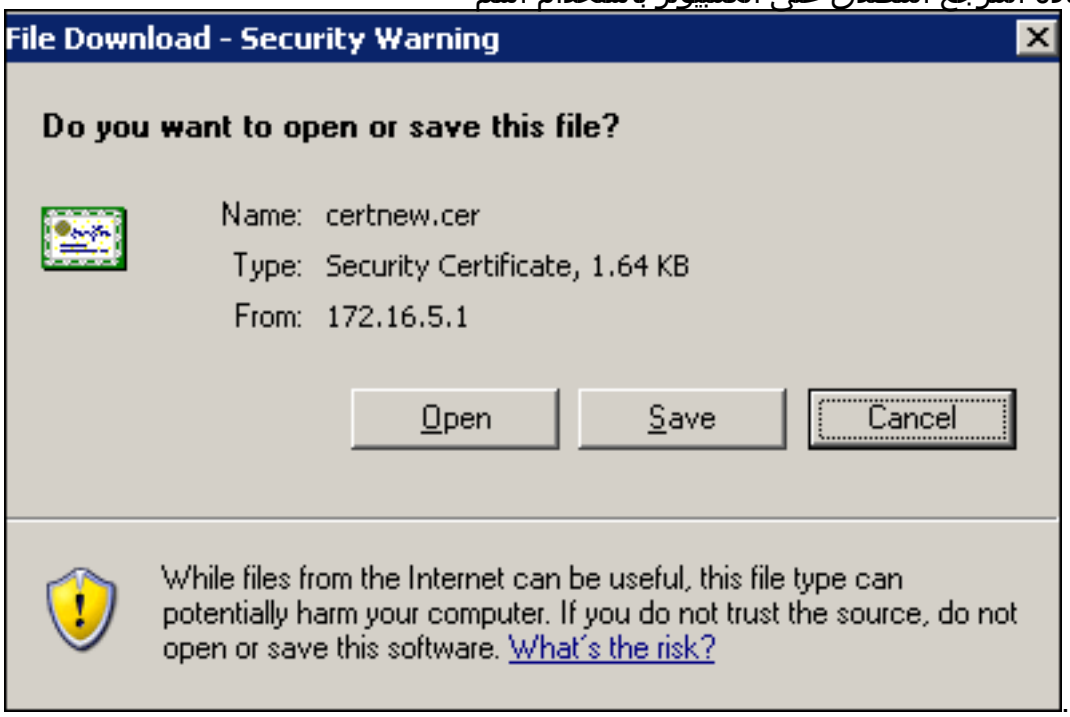
8. قبل تثبيت شهادة الهوية، يجب تنزيل شهادة المرجع المصدق من خادم CA وتثبيتها في ASA. أتمت هذا steps in order to جلبت ال CA شهادة من ال CA نادل يعين *CA1*:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام تكوينات المستخدم المتوفرة لخادم



انقر فوق **تنزيل شهادة CA أو سلسلة شهادات أو CRL** ، ثم حدد زر راديو **Base 64** لتحديد طريقة التشفير.انقر على **تنزيل شهادة المرجع المصدق**.

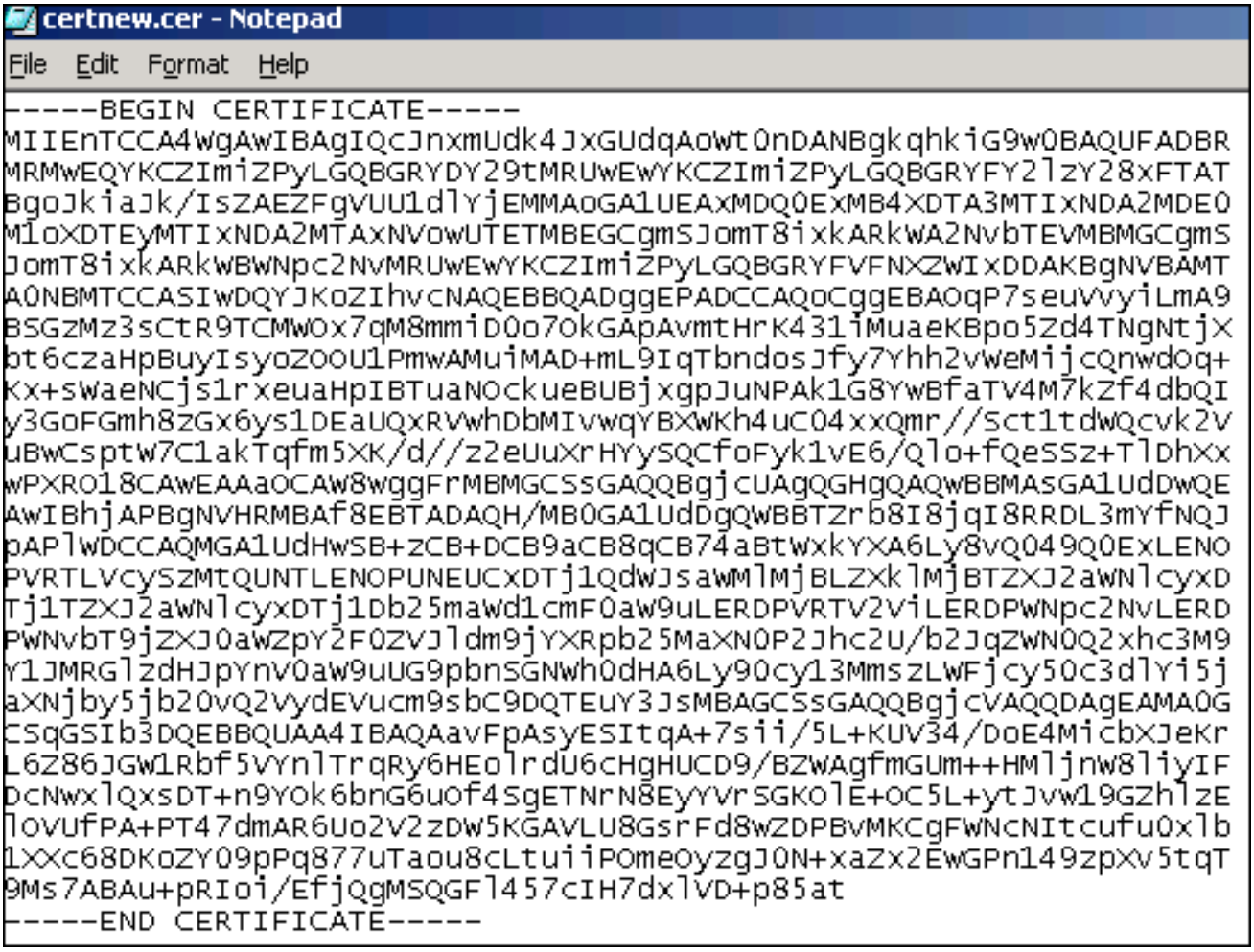


قم بحفظ شهادة المرجع المصدق على الكمبيوتر باستخدام اسم



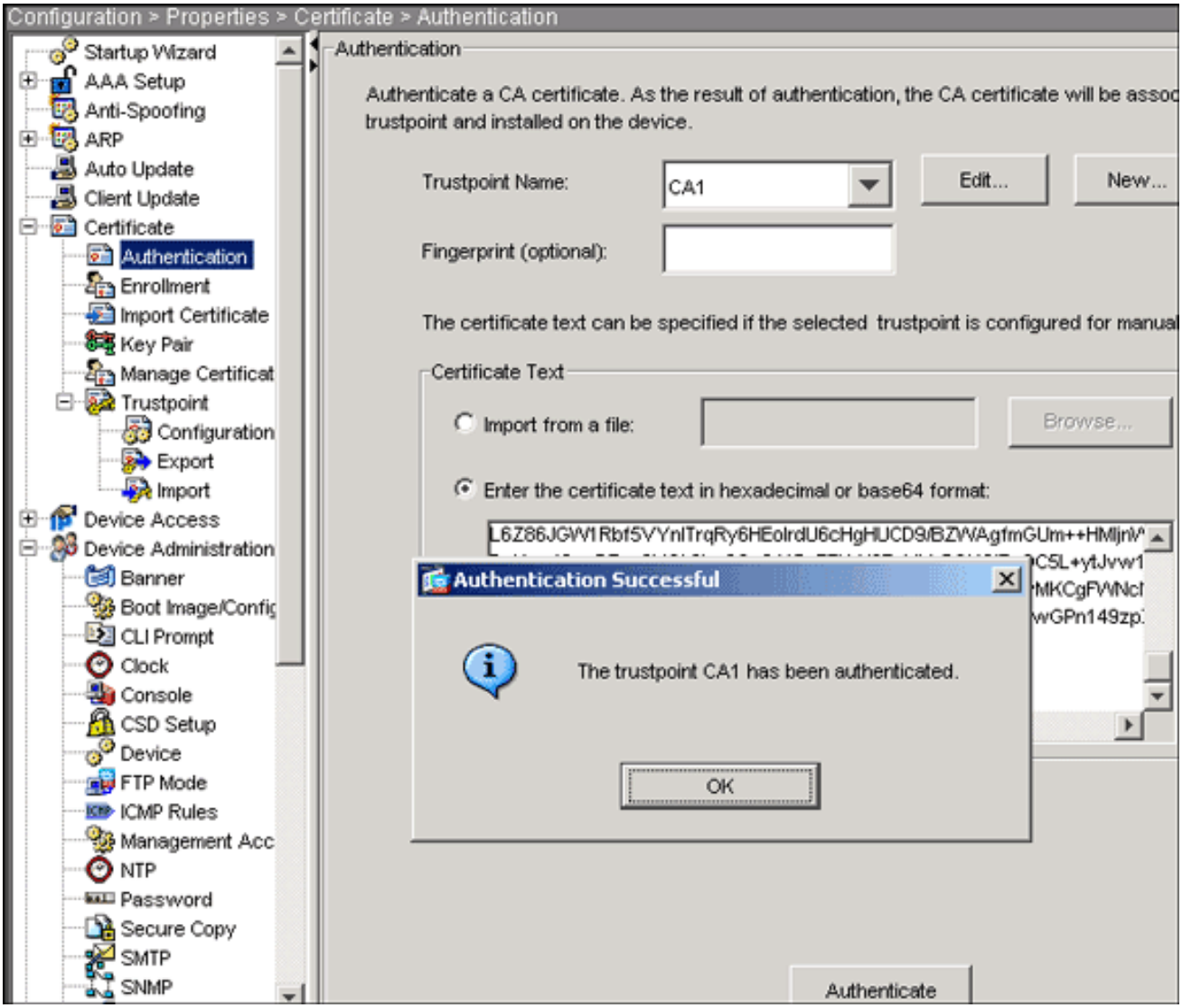
certnew.cer.

9. تصفح إلى المكان الذي قمت فيه بحفظ شهادة المرجع المصدق.
10. افتح الملف باستخدام محرر نصوص، مثل Notepad. (انقر بزر الماوس الأيمن فوق الملف، واختر **إرسال إلى > Notepad**.)
11. يجب أن تظهر الرسالة التي تم ترميزها بالأساس64 مشابهة للشهادة الموجودة في هذه الصورة:



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.



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 itself -----**BEGIN CERTIFICATE** **MIIEnTCCA4WgAwIBAgIQcJnxmUdk4JxGUdqAoWt0nDANBgkqhkiG9w0B** **AQUFADBR** **MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lz** **Y28xFTAT** **BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx** **NDA2MDE0** **M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV** **MBMGCgmS** **JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIxDDAK** **BgNVBAMT** **A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu** **VvyiLmA9** **BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd** **4TNgNtjX** **bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij**

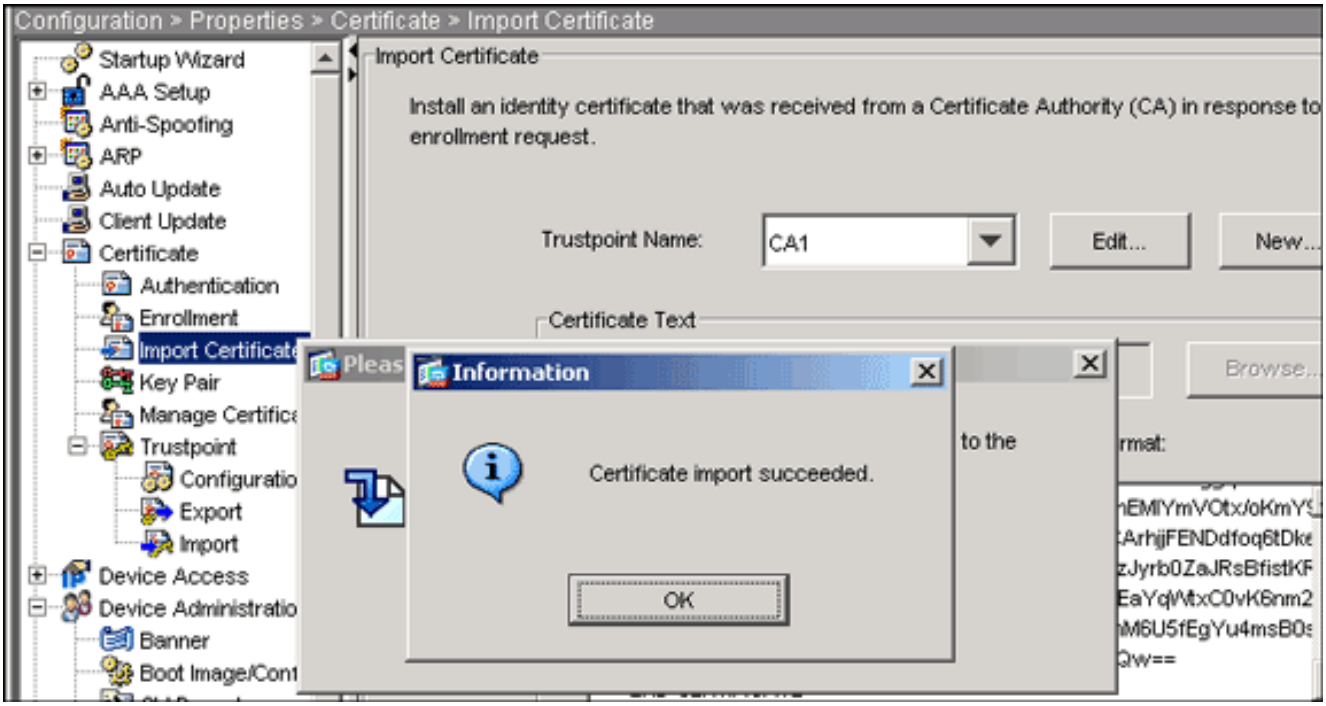
```
                                                                +cQnwdOq
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
                                                                kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
                                                                dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
                                                                z+TlDhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAgQGHgQAQwBBMAsG
                                                                A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
                                                                L3mYfNQJ
pAPlWDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
                                                                Q0ExLENO
PVRTLVcySzMtQUNTLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2
                                                                aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
                                                                c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0
                                                                Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnSGNWh0dHA6Ly90cy13MmszLWFjcy50
                                                                c3dlYi5j
aXNjby5jb20vQ2VydEVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
                                                                AgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
                                                                icbXJeKr
L6Z86JGW1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAgfmGUm++HMlj
                                                                nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOlE+OC5L+ytJvw
                                                                19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCgFWNcNIt
                                                                cufu0xlb
1XXc68DKoZY09pPq877uTaou8cLtuiiPOmeOyzgJ0N+xaZx2EwGPn149
                                                                zpXv5tqT
                                        9Ms7ABAu+pRIoi/EfjQgMSQGFl457cIH7dxlVD+p85at
                                                -----END CERTIFICATE-----
                                                                quit

        Manually pasted certificate into CLI. INFO: ---!
  Certificate has the following attributes: Fingerprint:
  98d66001 f65d98a2 b455fbce d672c24a Do you accept this
                                        certificate? [yes/no]: yes
                                .Trustpoint CA certificate accepted

                                Certificate successfully imported %
                                                        #(CiscoASA(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.



4. انقر فوق **إستيراد**، 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 vendor.* **-----BEGIN CERTIFICATE** **MIIFpzCCBI+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBR** **MRMwEQYK** **CZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2lzY28xFTAT** **BgoJkiaJ** **k/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz** **OVoXDTA5** **MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxFzAVBgNVBAgTDk5vcnRo** **IENhcm9s** **aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjbyBTeXN0** **ZW1zMSQw** **IgYDVQQDExtDaXNjb0FTQS5jaXNjby5jb20gT1U9VFNXRUIwgZ8wDQYJ** **KoZIhvcN** **AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C** **qB9j3HpX** **BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO** **sS8iqxqO** **2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/** **CaeqnGRN** **AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lz** **Y29BU0Eu** **Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAf** **BgNVHSME** **GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB** **9aCB8qCB** **74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD** **Tj1QdWJs**

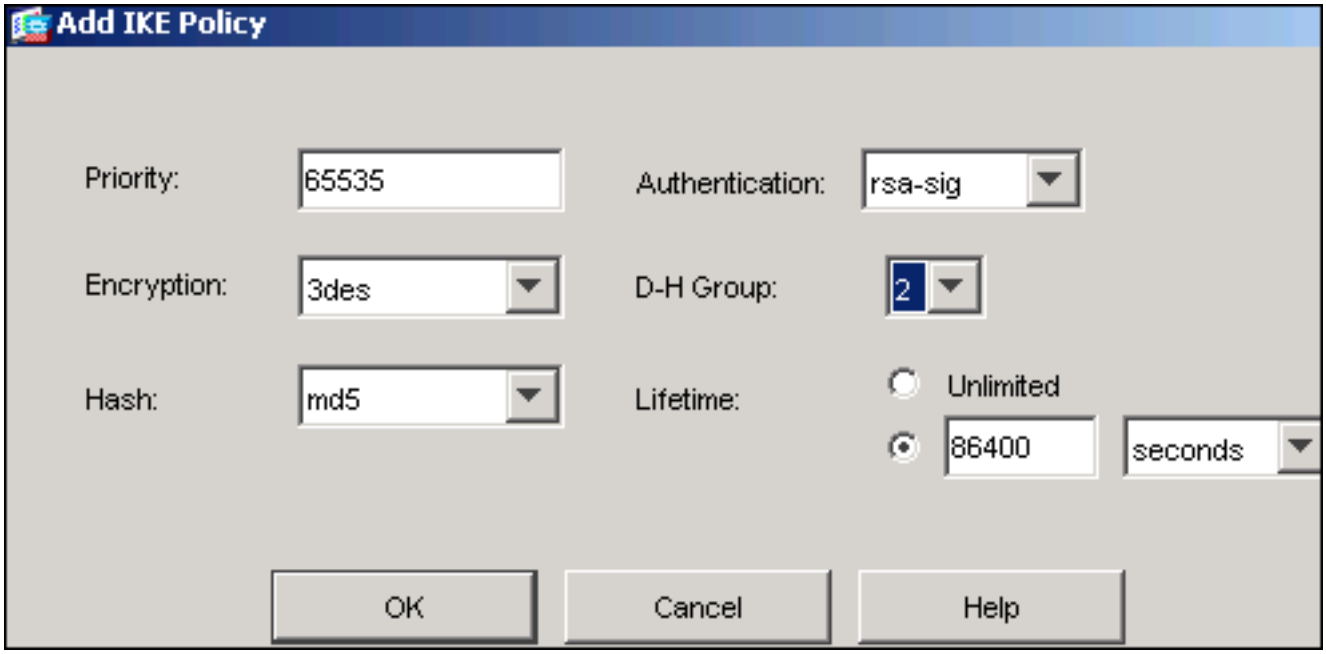
```
aWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1
                                                    cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
                                                    YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSG
                                                    NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydEVucm9sbC9D
                                                    QTEuY3Js
MIIBHQYIKwYBBQUHAQEEggEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
                                                    Oi8vL0NO
PUNBMSxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
                                                    U2Vydmlj
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
                                                    b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
                                                    dXRob3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
                                                    aXNjby5j
b20vQ2VydEVucm9sbC9UUy1XMkszLUFDUy5UU1dlYi5jaXNjby5jb21f
                                                    Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFcAZQBiAFMAZQByAHYAZQByMAwGA1Ud
                                                    EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEB
                                                    AIqCaA9G
+8h+3IS8RfVAGzcWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
                                                    7wXQaGph
zRq4dxALll1JkIjhfeQY+7VSkZlGEpuBnENTohdhthz5vBjGlcROXIs8
                                                    +3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b901516IzQP
                                                    5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
                                                    chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
                                                    t1nwLpsc
                                                =lL5nuPsd8MaexBc
                                        -----END CERTIFICATE-----
                                                        quit

                                    INFO: Certificate successfully imported
                                                    #(CiscoASA(config
```

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

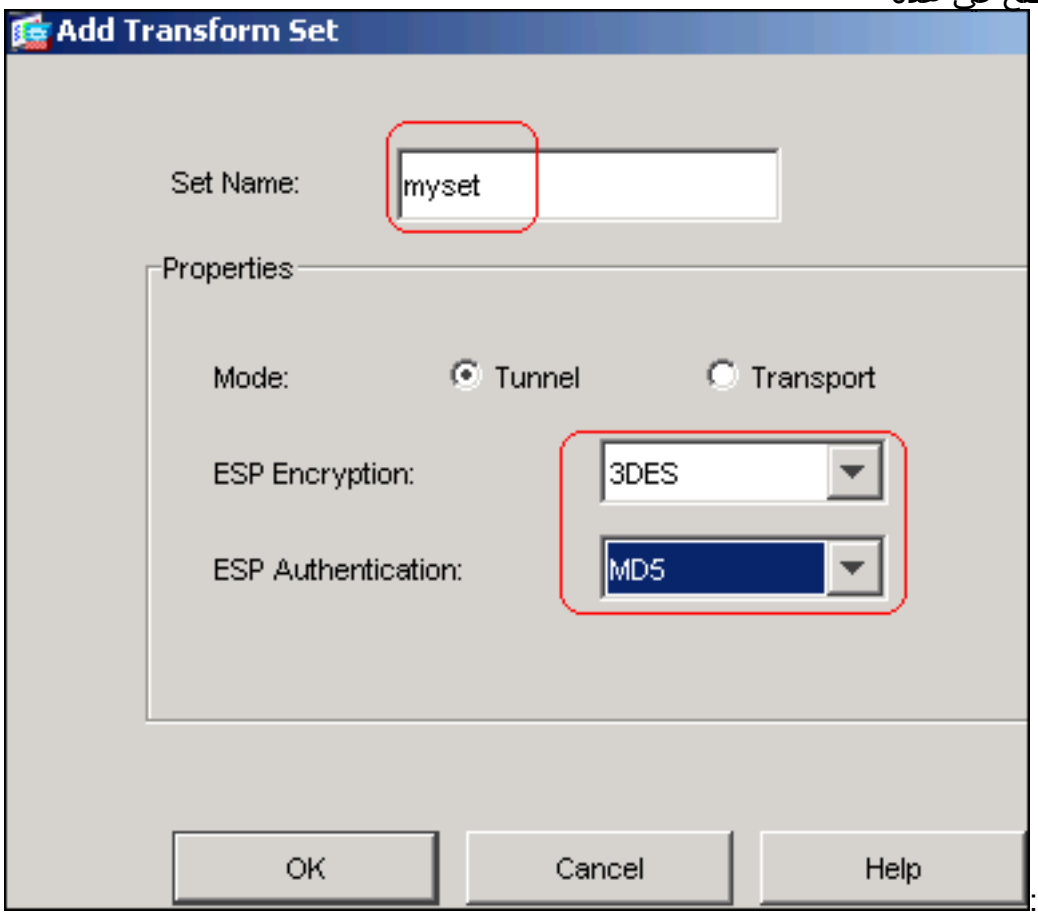
إجراء ASDM

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

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

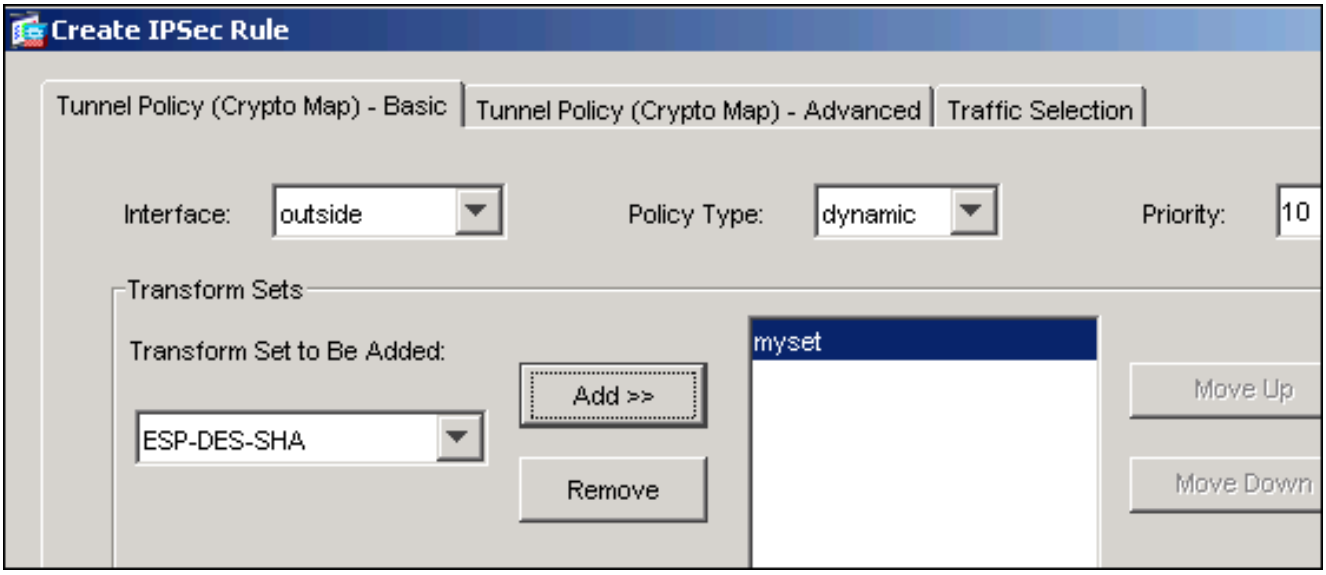


2. انقر فوق **موافق**، ثم انقر فوق **تطبيق**.
3. أخترت **تشكيل > IPSec > VPN > مجموعات تحويل >إضافة** in order to خلقت مجموعة تحويل (*myset*) كما هو موضح في هذه

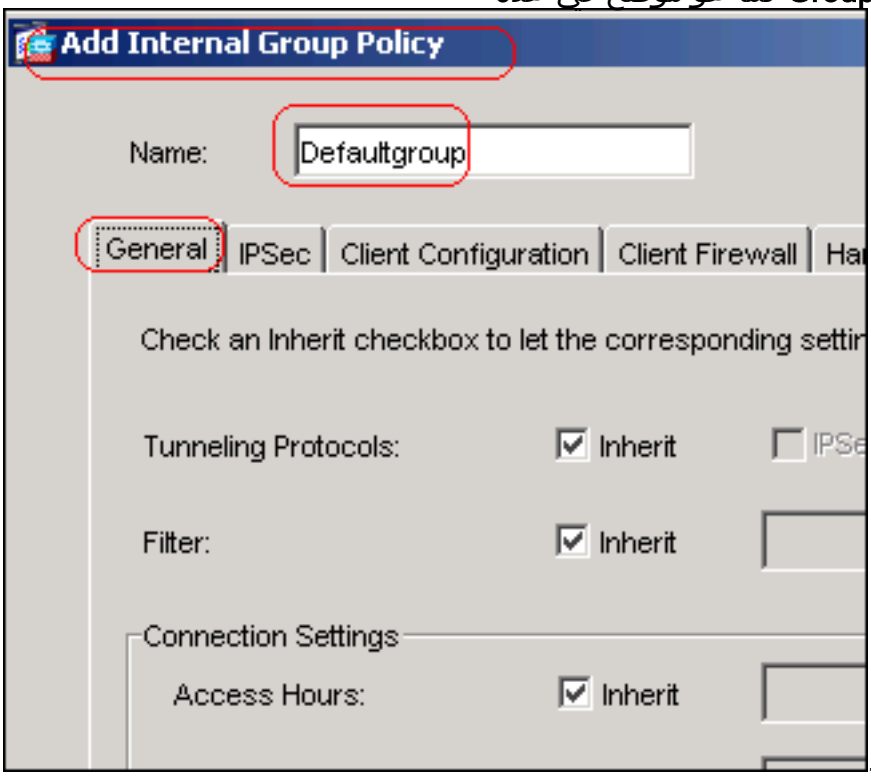


الصورة:

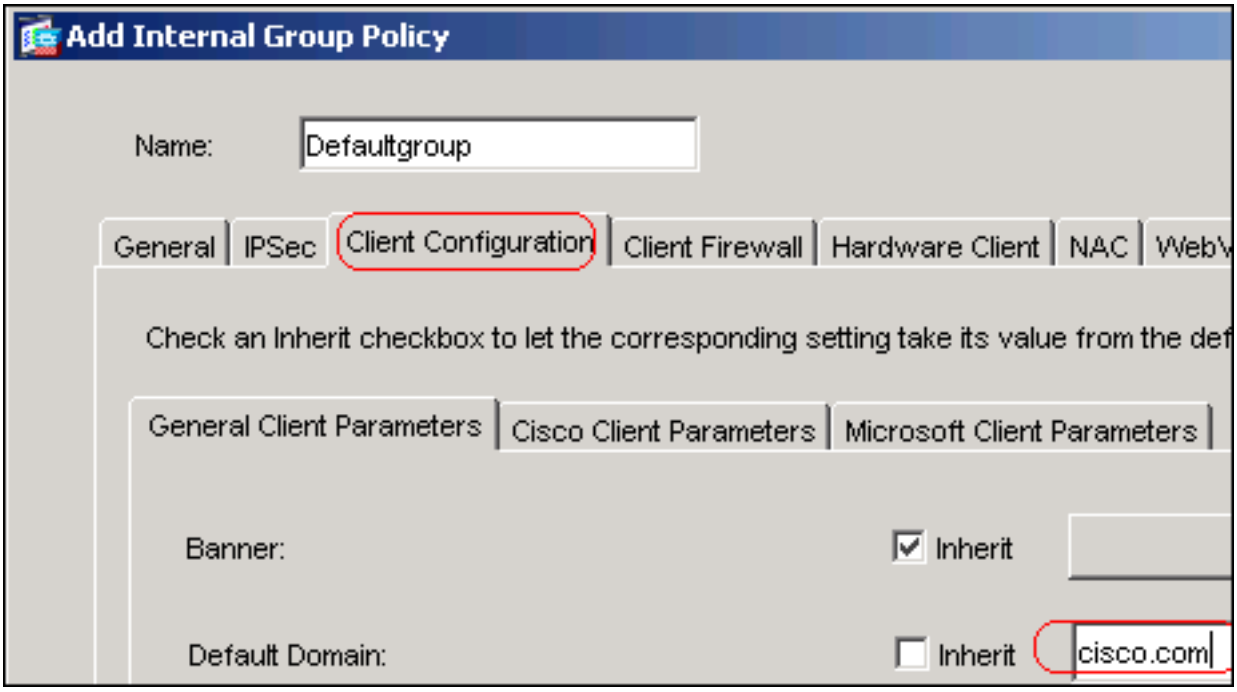
4. طقطقت **ok**، وبعد ذلك **طبقت**
5. أخترت **تكوين > IPSec > VPN > قواعد IPSec >إضافة** لإنشاء خريطة تشفير باستخدام سياسة ديناميكية للأولوية 10 كما هو موضح في هذه الصورة:



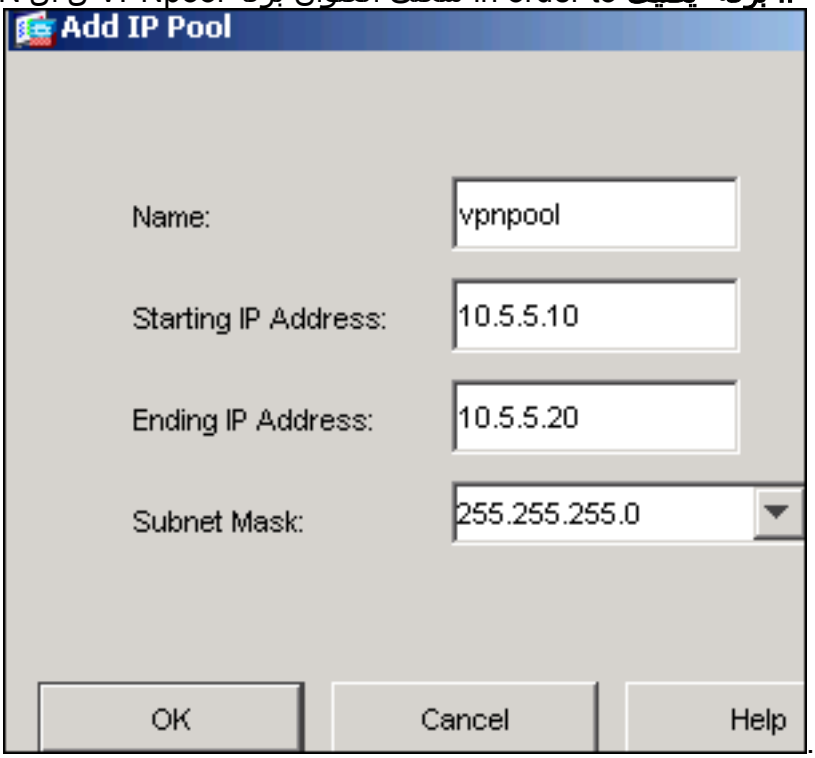
6. طقطقت **ok**، وبعد ذلك **طبقت**
7. أخترت **تشكيل>VPN>عام>مجموعة سياسة>إضافة داخلي مجموعة سياسة** in order to خلقت مجموعة **تقصيرGroup** كما هو موضح في هذه



الصور.

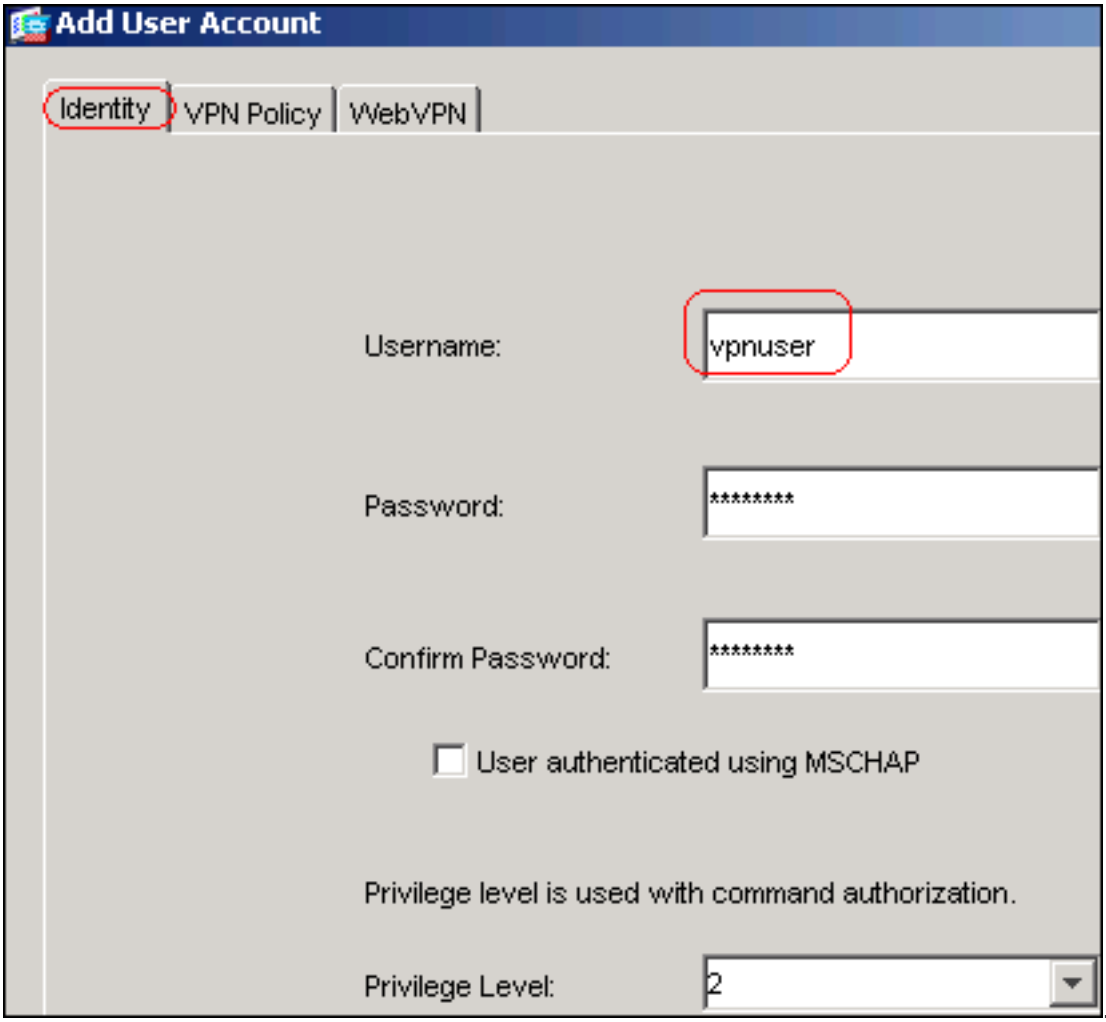


8. طقطقت **ok**، وبعد ذلك **طبقت**
9. أخترت **تشكيل>VPN>IP عنوان إدارة>IP بركة>يضيف** in order to شكلت العنوان بركة VPNpool ل ال VPN



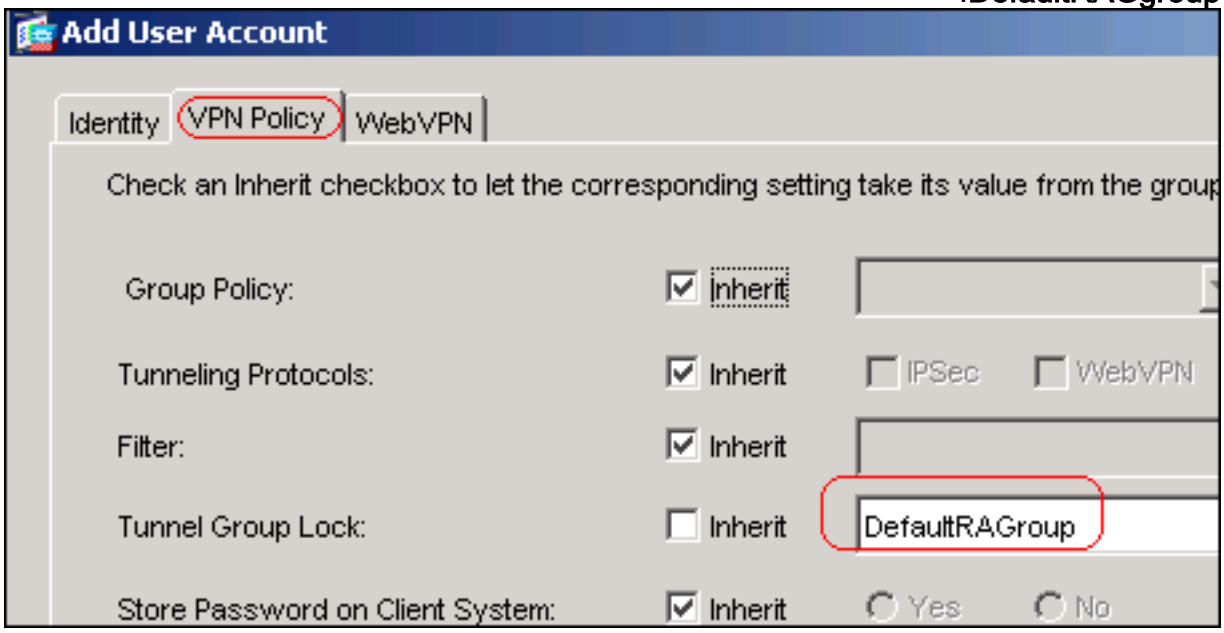
زبون مستعمل أن يكون عينت ديناميكيا.

10. طقطقت **ok**، وبعد ذلك **طبقت**
11. أخترت **تشكيل>VPN>عام>مستعمل>يضيف** in order to خلقت مستعمل حساب **vpn** ل VPN زبون



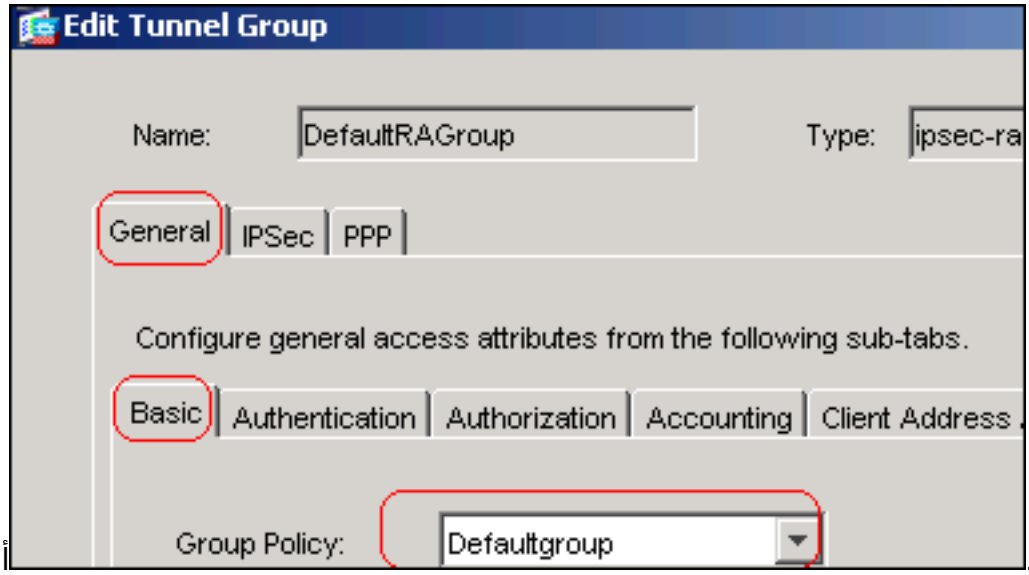
منفذ.

12. إضافة هذا المستخدم إلى **DefaultRAGgroup**.

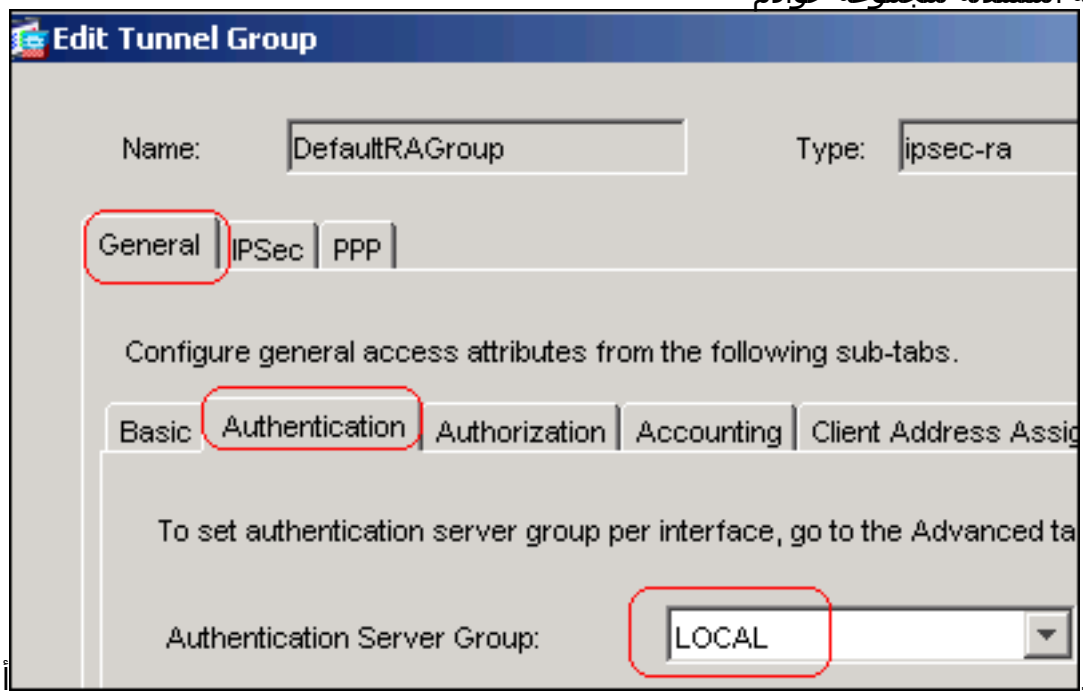


13. طقطقت **ok**، وبعد ذلك **طبقت**
14. تحرير DefaultRagGroup كما هو موضح في هذا الإجراء:أخترت **تشكيل>VPN>عام > مجموعة نفق > تحرير**.أختر **DefaultGroup** من القائمة المنسدلة "نهج

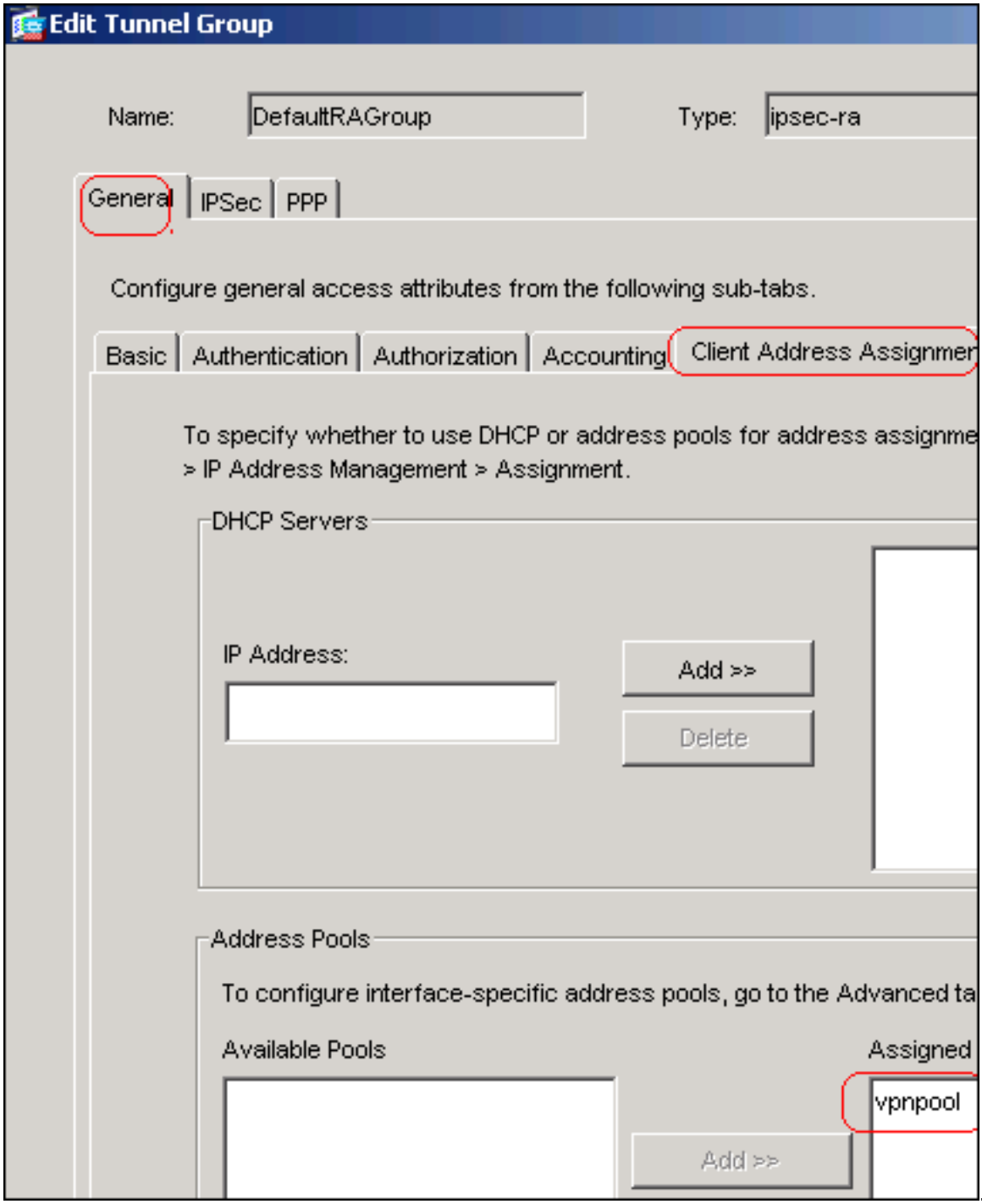
أختر **محلي** من القائمة المنسدلة لمجموعة خوادم المجموعة".



أخترت المصادقة.



vpnPool من الزبون عنوان تنازل قائمة ميلان إلى



جانب.

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

  Phase 2 Configurations CiscoASA(config)#group-  ---!
                                    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 ---!
        tunnel group. 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
```

ملخص تكوين ASA

Cisco ASA

```
                                CiscoASA#show running-config
                                                Saved :
                                                    :
                                        (ASA Version 7.2(2
                                                    !
                                      hostname CiscoASA
                                    domain-name cisco.com
                  enable password 8Ry2YjIyt7RRXU24 encrypted
                                                names
                                                    !
                                    interface Ethernet0/0
                                          nameif outside
                                       security-level 0
                    ip address 192.168.1.5 255.255.255.0
```

```
!
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
!
interface Ethernet0/3
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
shutdown
no nameif
no security-level
no ip address
!
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 3f14b70b00000000001f
       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
       490cde1a fe2d63e3 1e1fb28c 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 1a2b873f 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
```

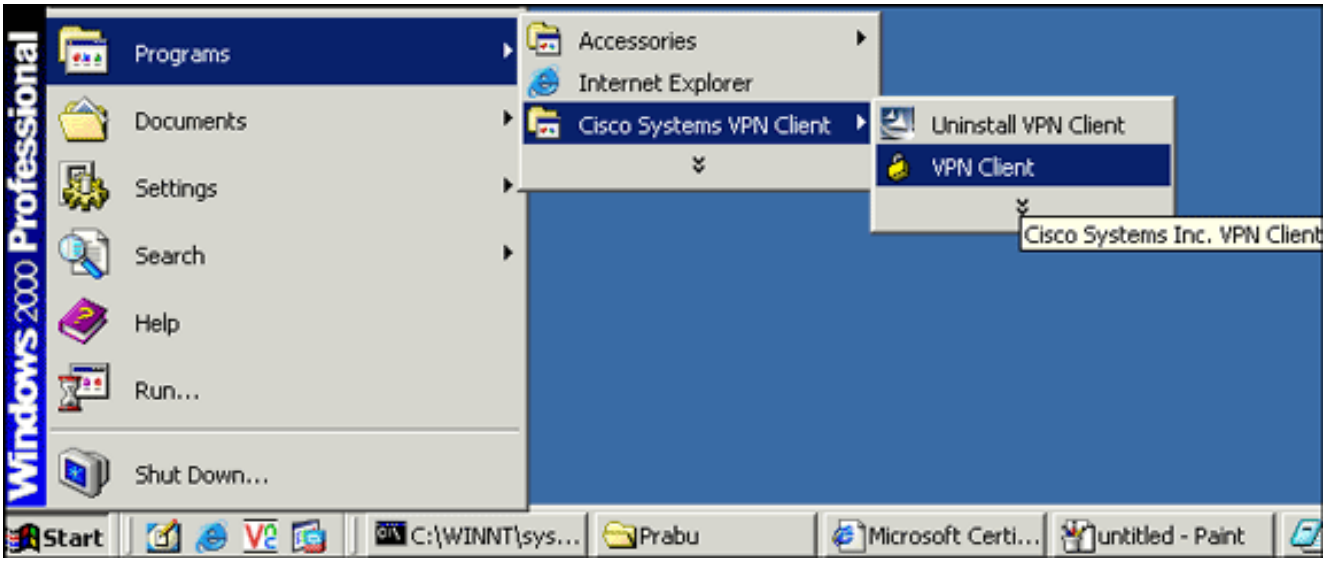
```
                                0a099226 8993f22c 64011916
        6562310c 300a0603 55040313 03434131 05545357
                                30820122 300d0609 2a864886
        f70d0101 01050003 82010f00 3082010a 02820101
                                00ea8fee c7ae56fc a22e603d
        0521b333 3dec0ad4 7d4c2316 3b1eea33 c9a6883d
                                28ece906 02902f9a d1eb2b8d
        f588cb9a 78a069a3 965de133 6036d8d7 6ede9ccd
                                a1e906ec 88b32a19 38e5353e
        6c0032e8 8c003fa6 2fd22a4d b9dda2c2 5fcbb621
                                876bd678 c8a37109 f074eabe
        2b1fac59 a78d0a3b 35af17ae 687a4805 3b9a34e7
                                24b9e054 063c60a4 9b8d3c09
        351bc630 05f69357 833b9197 f875b408 cb71a814
                                69a1f331 b1eb2b35 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
```

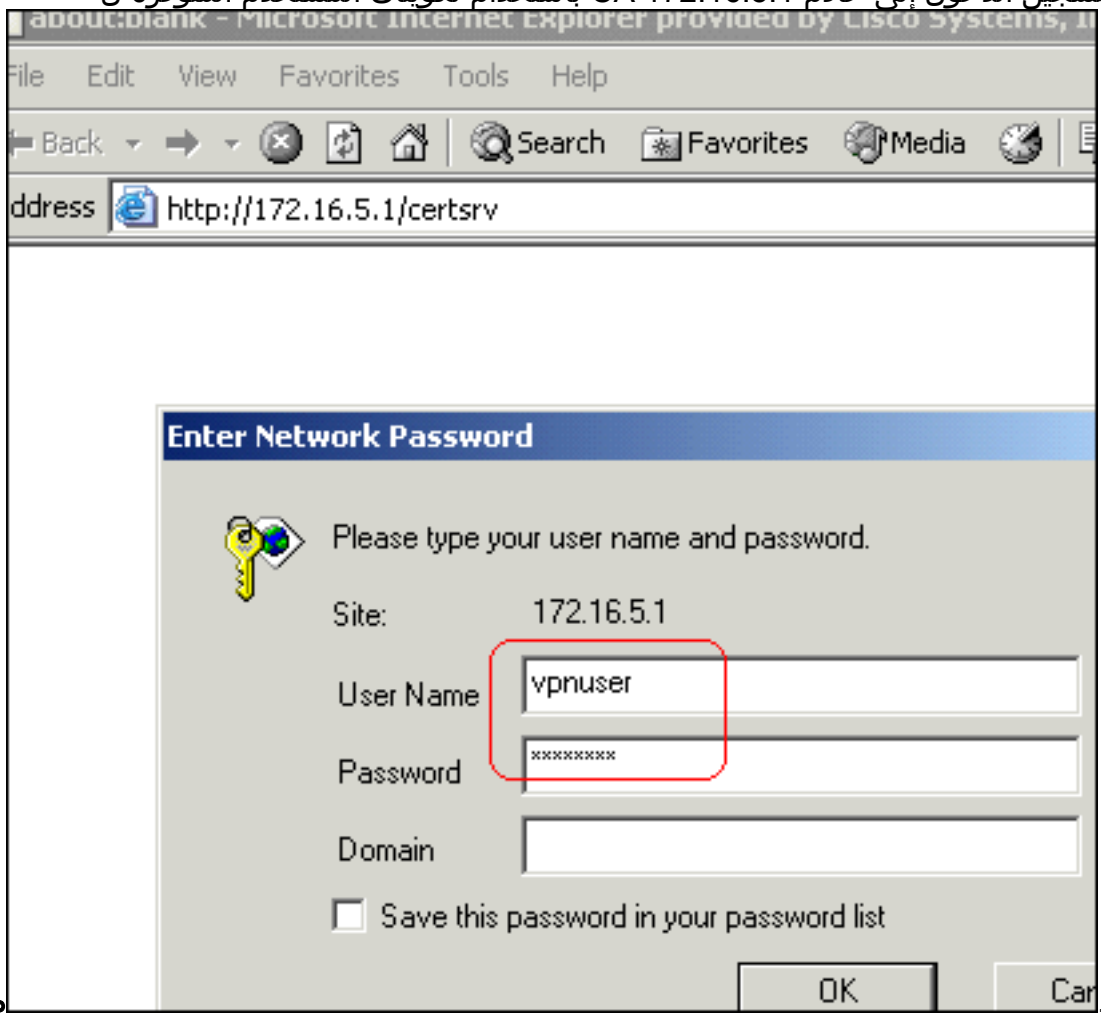
تكوين عميل شبكة VPN

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.

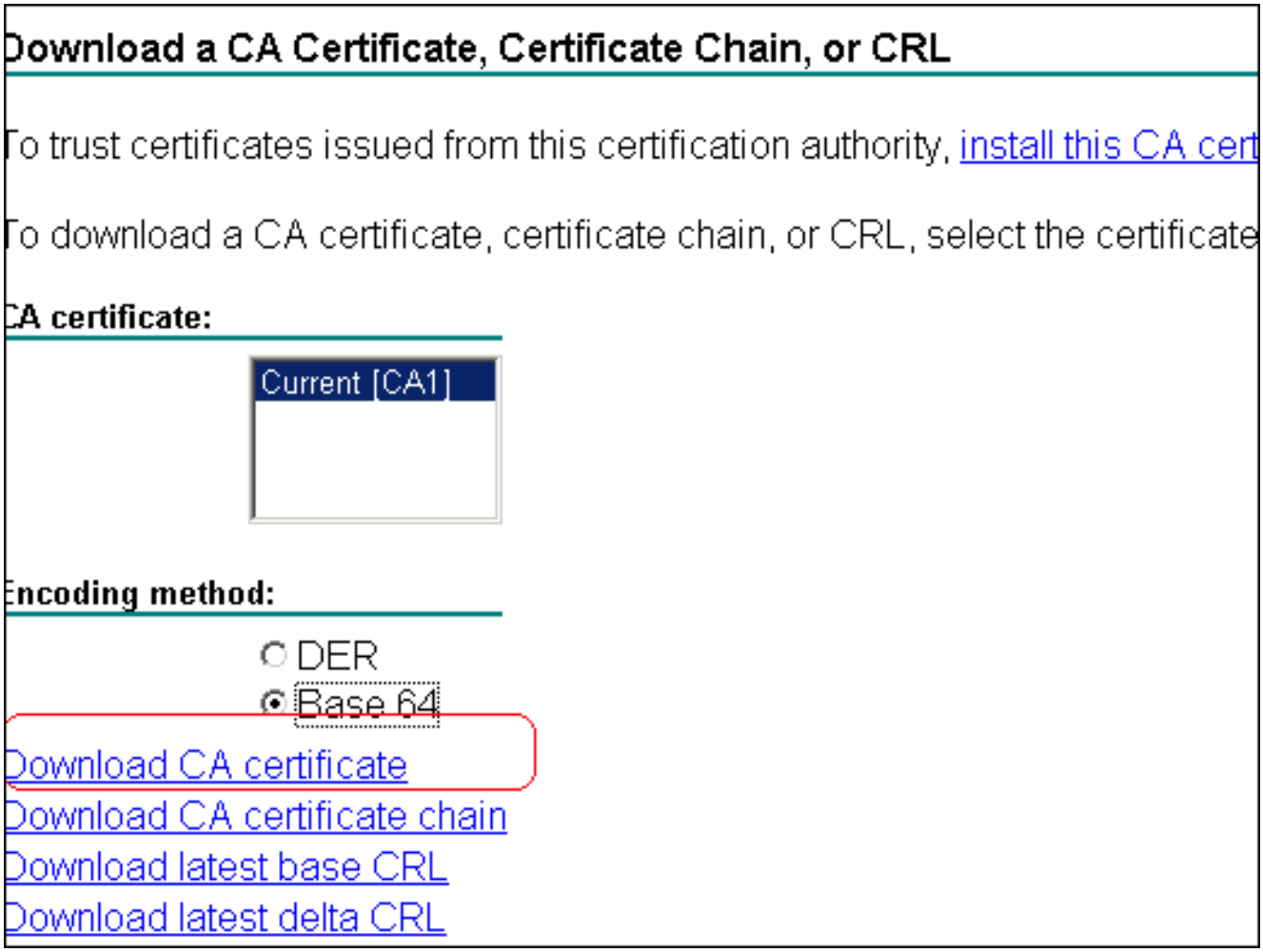


2. أتمت هذا steps in order to جلبت ال CA شهادة من ال CA نادل يعين **CA1** وركبت هو في cisco VPN زبون:قم بتسجيل الدخول إلى خادم CA 172.16.5.1 باستخدام تكوينات المستخدم المتوفرة ل

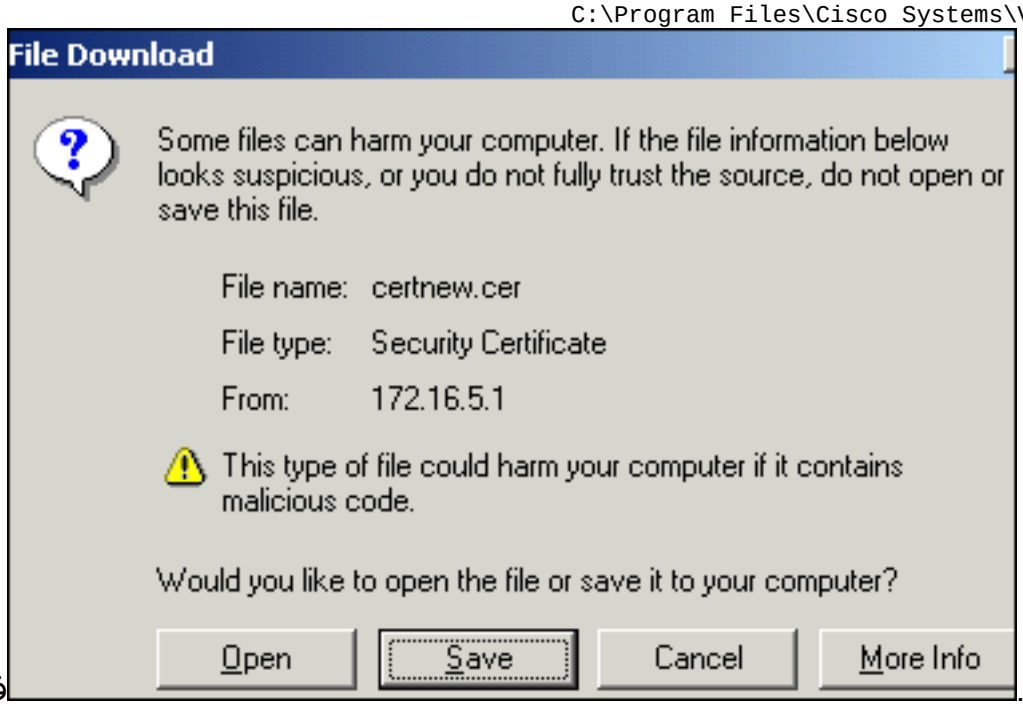


vpnUser.

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

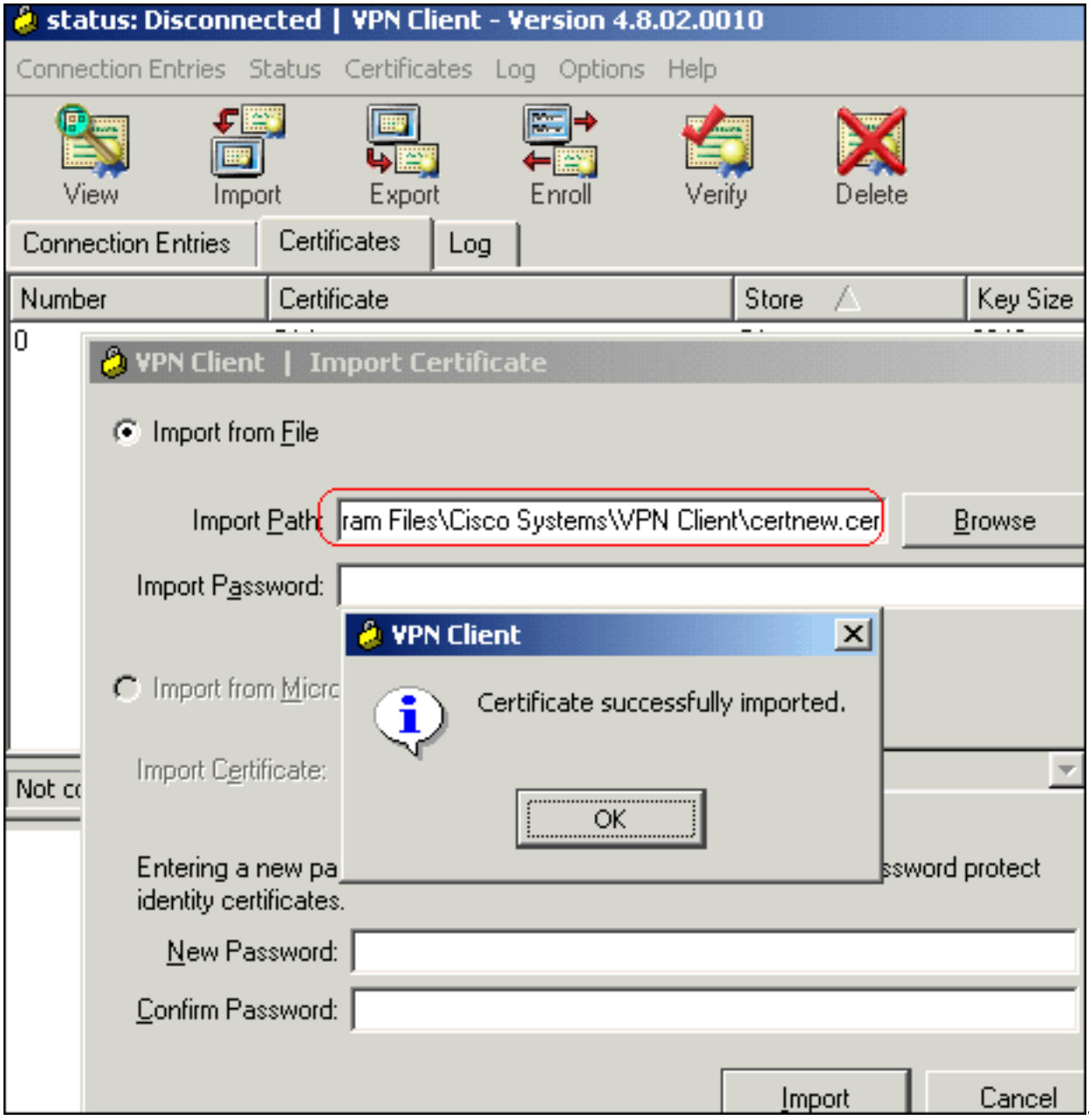


قم بحفظ شهادة المرجع المصدق على الكمبيوتر باستخدام اسم **certnew.cer**. بشكل افتراضي، يحفظ الملف إلى `C:\Program Files\Cisco Systems\VPN`



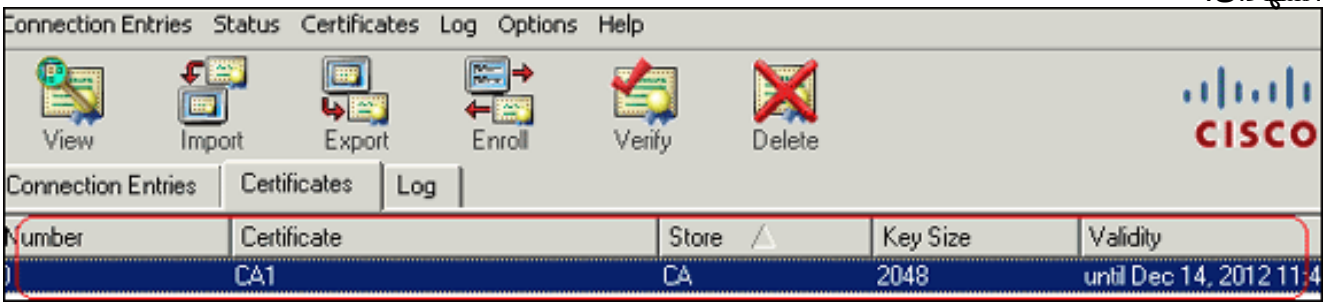
في عميل VPN، `Client`.

انقر فوق علامة التبويب **الشهادات**، ثم أختر **إستيراد**.انقر على زر **إستيراد من ملف** لاسلكي، ثم انقر على **إستعراض** لاستيراد شهادة المرجع المصدق من الموقع المخزن `C:\Program Files\Cisco Systems\VPN` `Client`.انقر فوق **استيراد**.يظهر مربع حوار يوضح أن الشهادة تم إستيرادها

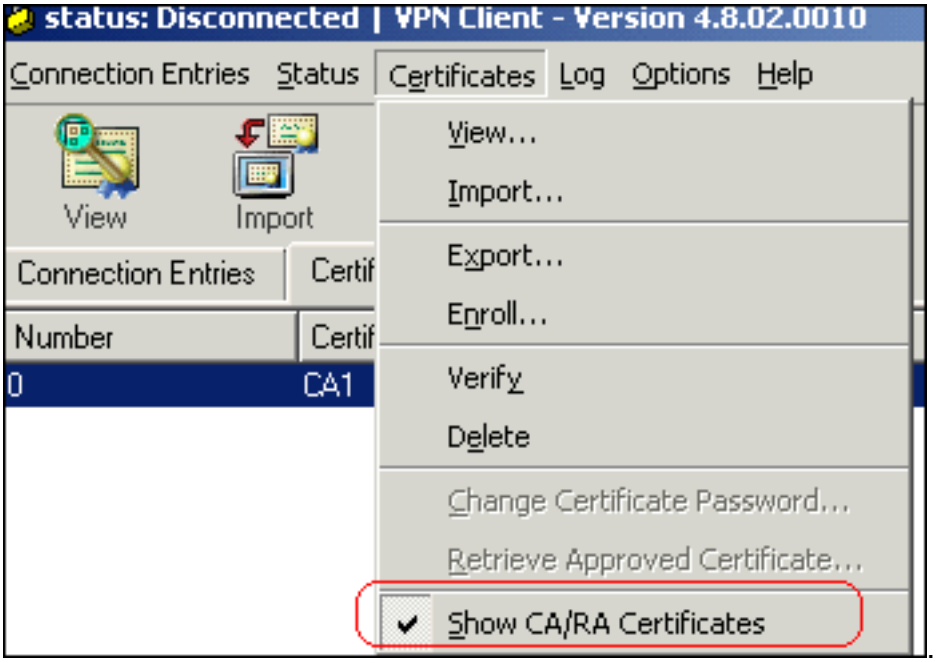


بنجاح.

يظهر CA1 Certificates CA في صفحة الشهادات.

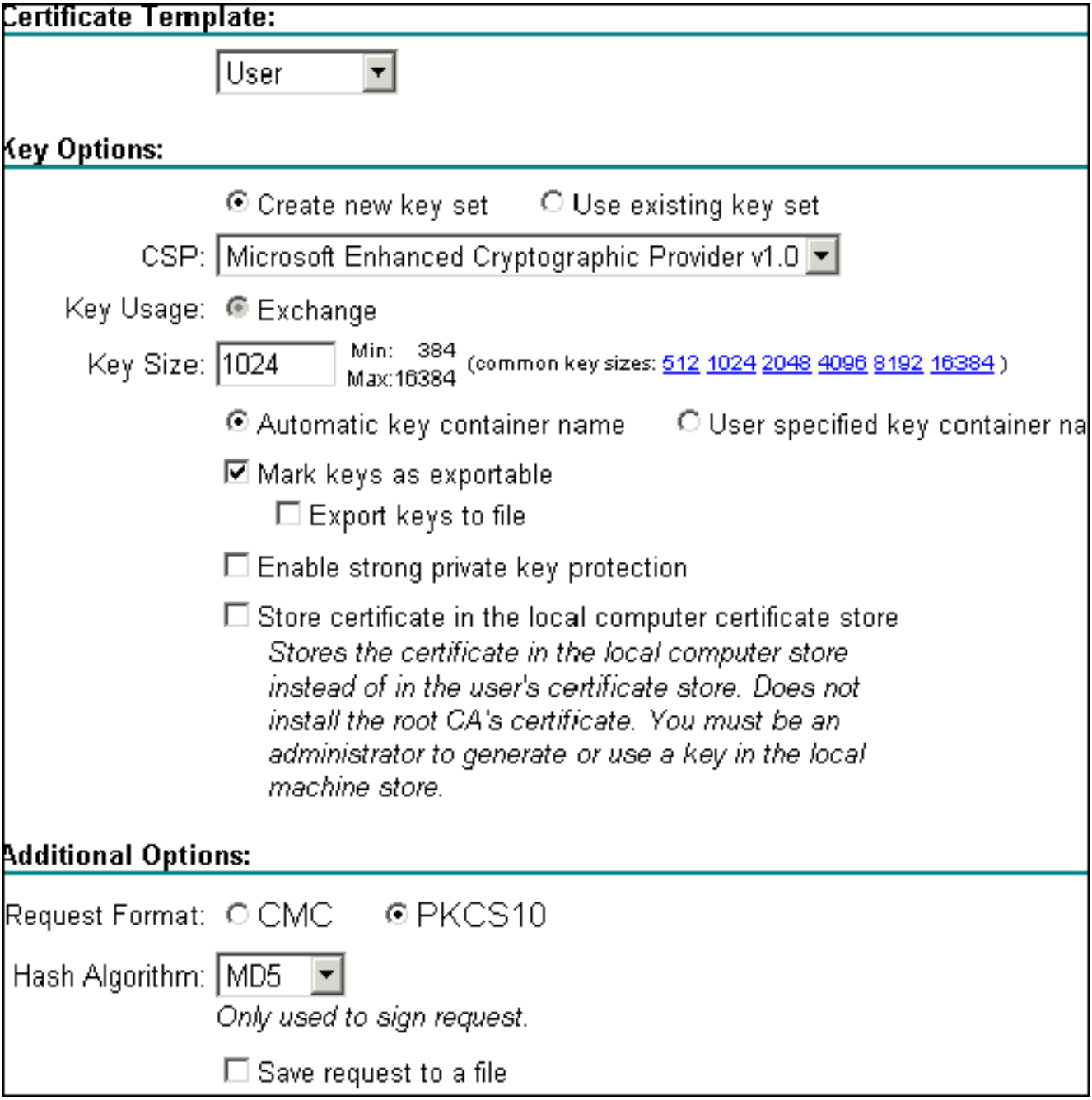


ملاحظة: تأكد من تحديد خيار **عرض شهادات CA/RA**، وإلا فإن شهادات CA لن تظهر في نافذة

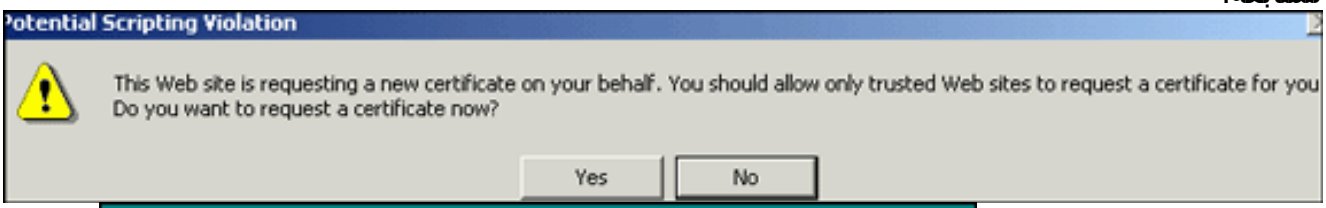


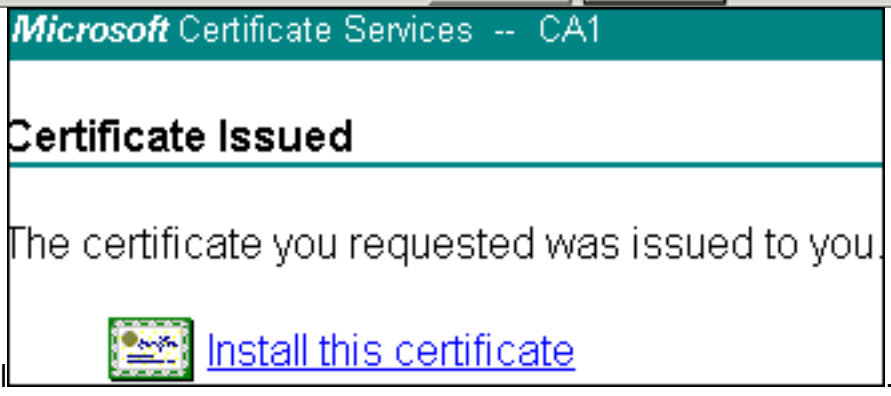
الشهادة.

3. أتمت 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**.



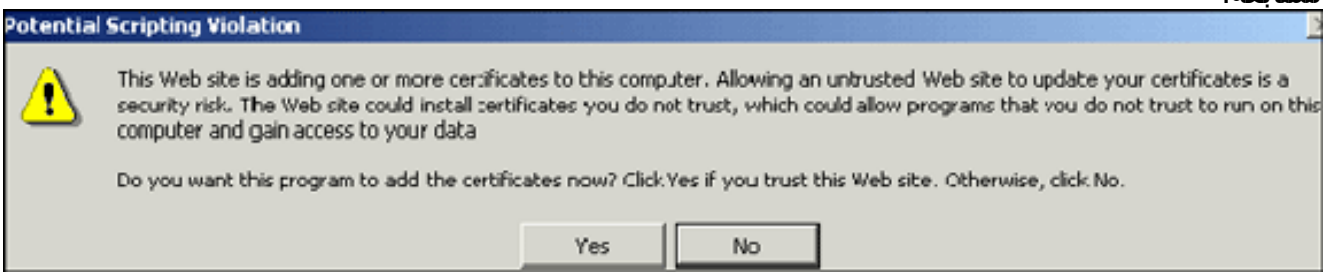
انقر فوق **نعم** للمتابعة.



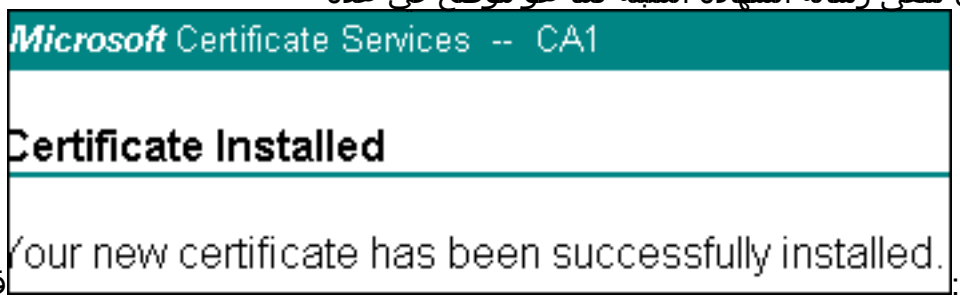


انقر على **تثبيت هذه الشهادة**. انقر فوق **نعم**

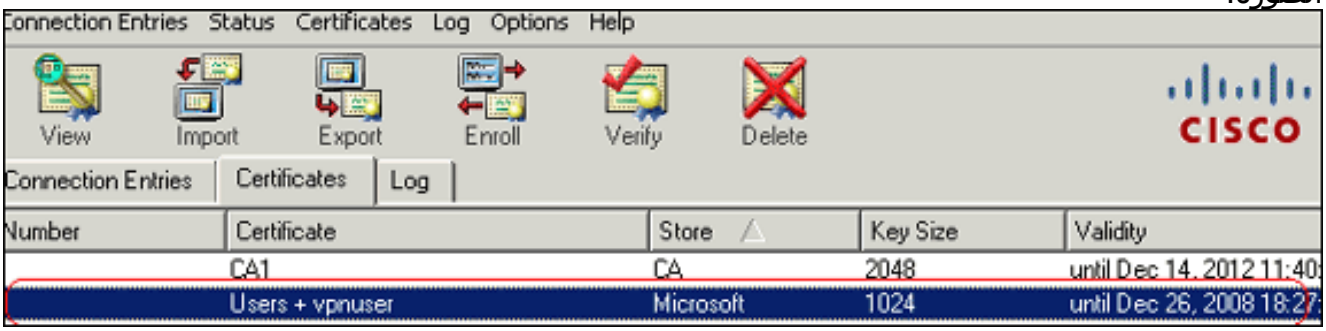
للمتابعة.



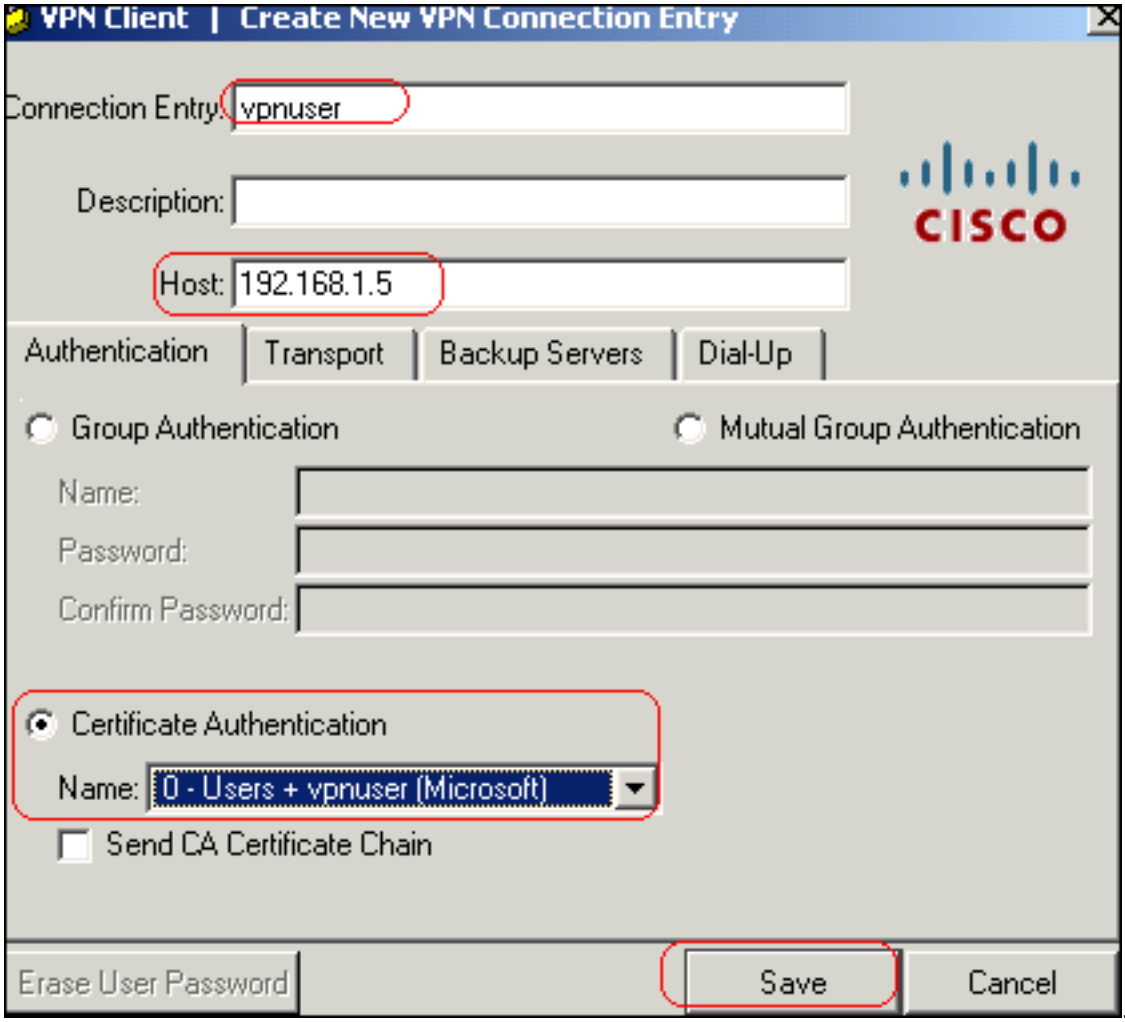
يجب أن تتلقى رسالة الشهادة المثبتة كما هو موضح في هذه



الصورة:قم بالخروج ثم إعادة تشغيل عميل VPN للسماح لشهادة الهوية المثبتة بالظهور في علامة التبويب "الشهادات" الخاصة بعميل VPN كما هو موضح في هذه الصورة:

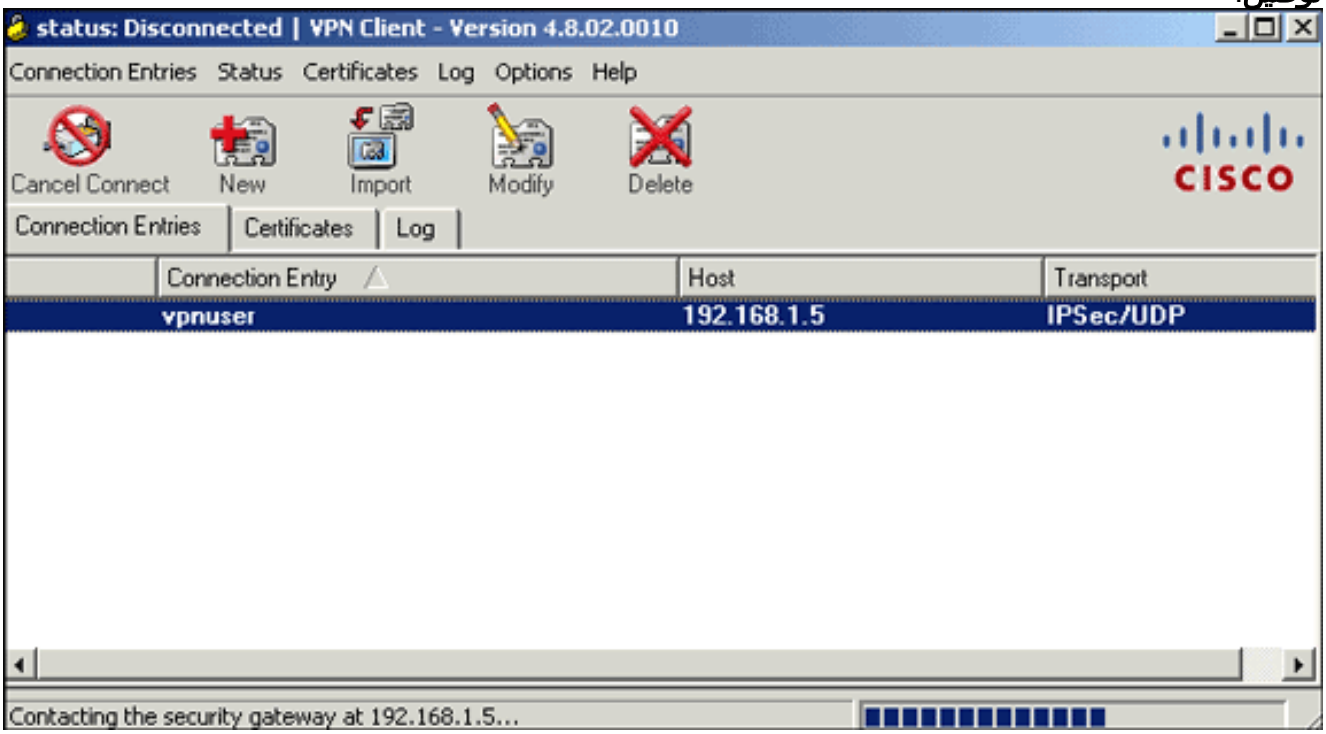


4. أتمت هذا steps in order to خلقت توصيل مدخل (*vpnUser*):انقر على علامة تبويب إدخالات الاتصال ثم انقر على **جديد**.أدخل عنوان IP للنظير البعيد (الموجه) في حقل المضيف.حدد زر **مصادقة الشهادة**، واختر شهادة الهوية من القائمة المنسدلة.طقطقة



حفظ.

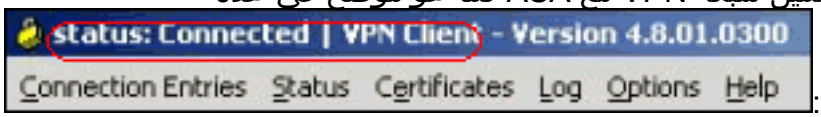
5. انقر على **توصيل**.



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

البعيدة.

7. يتصل عميل شبكة VPN مع ASA كما هو موضح في هذه الصورة:



التحقق من الصحة

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: 3f14b70b00000000001f
                              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
                       end   date: 14:00:36 UTC Dec 26 2008
```

```
                                                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 7f04cba1 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

                                                              IKE Peer: 10.1.1.5   1
                                        Type    : user            Role    : responder
```

```
Rekey   : no               State   : MM_ACTIVE
```

- **show crypto 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 أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **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**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**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** **trustPointName** 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.

- **خطأ: 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 **crypto isakmp identity auto** في تكوين ASA/PIX.

معلومات ذات صلة

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).