

Exemple de configuration d'authentification IPSec sur ASA/PIX 7.x et clients VPN à l'aide de certificats numériques avec une autorité de certification Microsoft

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Produits connexes](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration ASA](#)

[Résumé de configuration ASA](#)

[Configuration du client VPN](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment installer manuellement un certificat numérique de constructeur de tiers sur l'appliance de sécurité Cisco (ASA/PIX) 7.x, aussi bien que des clients vpn, afin d'authentifier les pairs d'IPSec avec le serveur de Microsoft Certificate Authority (CA).

[Conditions préalables](#)

[Conditions requises](#)

Ce document exige que vous avez accès à un Autorité de certification (CA) pour l'inscription de certificat. Tiers pris en charge des constructeurs que CA incluent Baltimore, Cisco, confient, iPlanet/Netscape, Microsoft, RSA, et Verisign.

Remarque: Ce document utilise le serveur Windows 2003 en tant que serveur CA pour le scénario.

Remarque: Ce document suppose qu'il n'y a aucune configuration VPN préexistante dans l'ASA/PIX.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 5510 qui exécute la version de logiciel 7.2(2) et la version 5.2(2) ASDM.
- Client VPN qui exécute la version de logiciel 4.x et plus tard.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Produits connexes

La configuration ASA peut également être utilisée avec la gamme Cisco 500 PIX qui exécute la version de logiciel 7.x.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

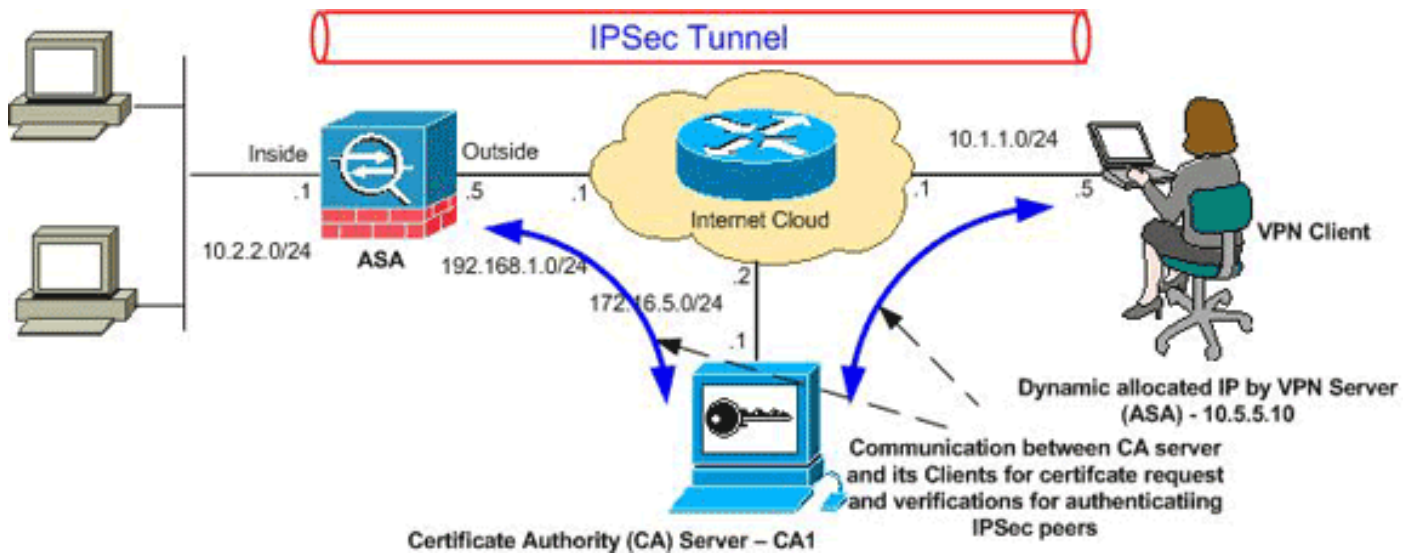
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Configurations

Ce document utilise les configurations suivantes :

- [Configuration ASA](#)
- [Résumé de configuration ASA](#)
- [Configuration du client VPN](#)

Configuration ASA

Terminez-vous ces étapes afin d'installer un certificat numérique de constructeur de tiers sur l'ASA :

[Étape 1. Vérifiez que les valeurs Date, Heure et Fuseau Horaire soient exactes](#)

[Étape 2. Générez la paire de clés RSA](#)

[Étape 3. Créez le point de confiance.](#)

[Étape 4. Générez l'inscription de certificat.](#)

[Étape 5. Authentifiez le point de confiance](#)

[Étape 6. Installez le certificat](#)

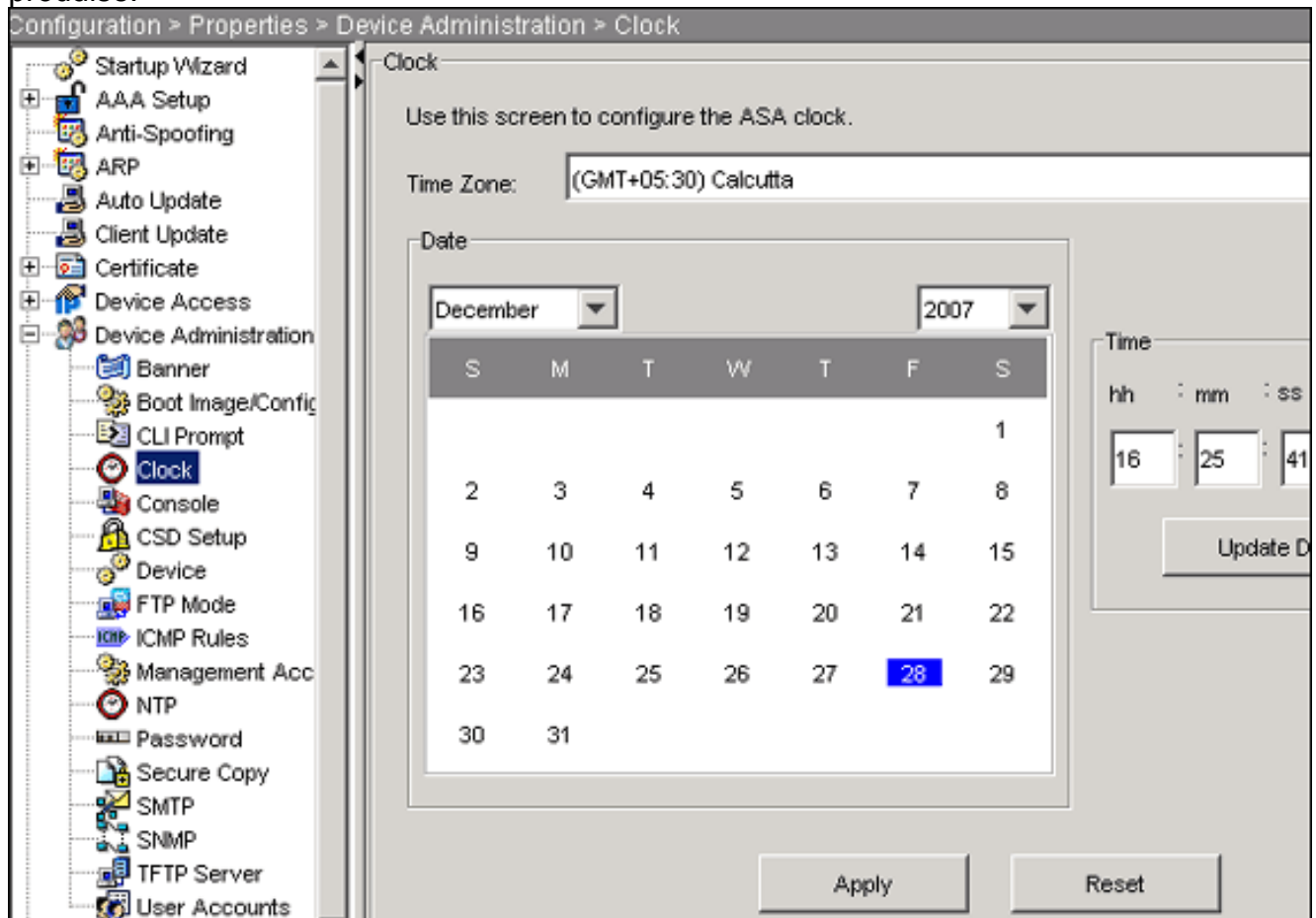
[Étape 7. Configurez l'Accès à distance VPN \(IPsec\) pour utiliser le certificat nouvellement installé](#)

[Étape 1. Vérifiez que les valeurs Date, Heure et Fuseau Horaire soient exactes](#)

Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.

2. Développez la **gestion de périphérique**, et choisissez l'**horloge**.
3. Vérifiez que les informations répertoriées sont correctes. Les valeurs pour la date, le temps, et le fuseau horaire doivent être précises pour que la validation appropriée de certificat se produise.



Exemple de ligne de commande

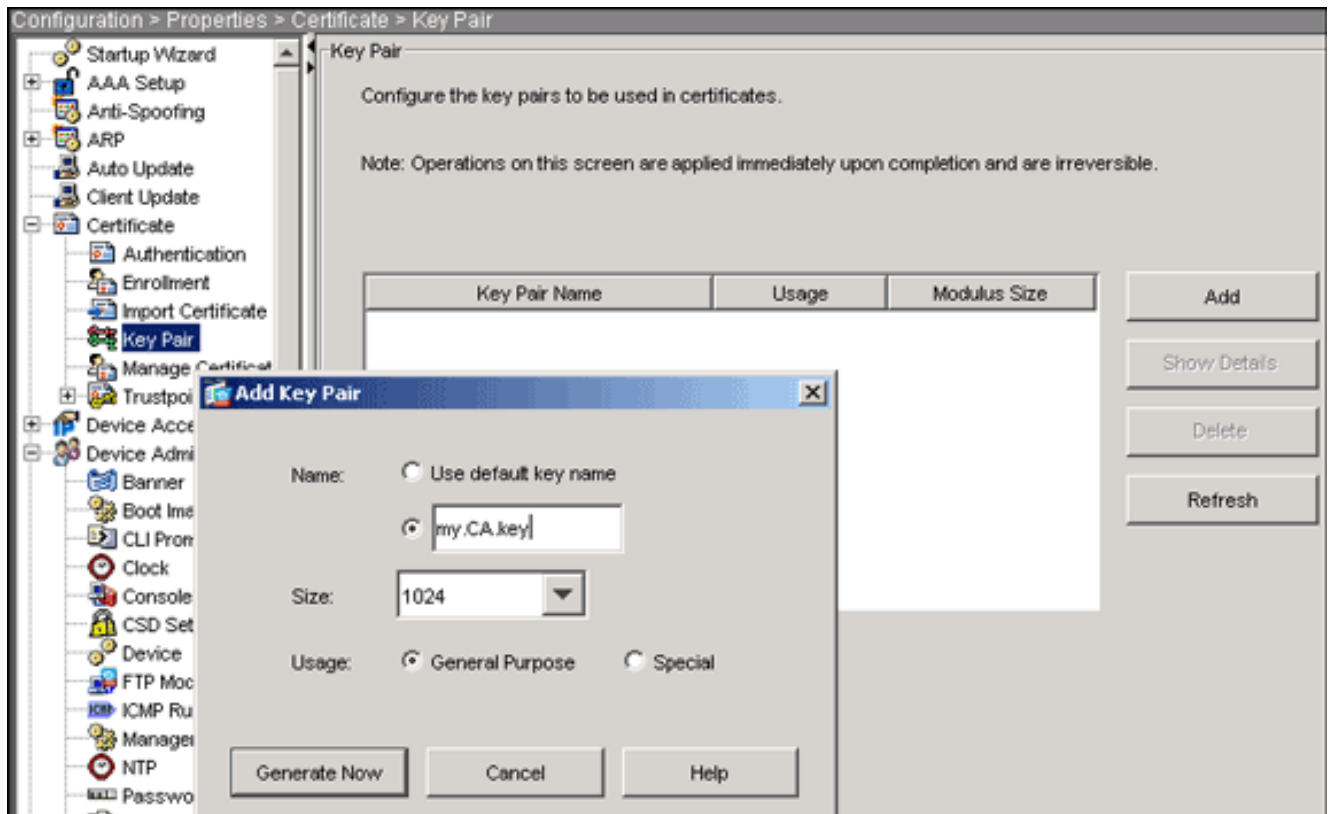
```
CiscoASA
CiscoASA#show clock 16:25:49.580 IST Fri Dec 28 2007
```

[Étape 2. Générez la paire de clés RSA](#)

La clé publique générée RSA est combinée avec les informations d'identité de l'ASA pour former une demande du certificat PKCS#10. Vous devriez distinctement identifier le nom de clé avec le point de confiance pour lequel vous créez la paire de clés.

Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez le **certificat**, et choisissez la **paire de clés**.
3. Cliquez sur **Add**.



4. Écrivez le nom de clé, choisissez la taille de module, et sélectionnez le type d'utilisation. **Remarque:** La taille recommandée de paire de clés est 1024.
5. Cliquez sur **Generate Now**. La paire de clés que vous avez créée devrait être répertoriée dans la colonne de nom de paire de clés.

Exemple de ligne de commande

CiscoASA

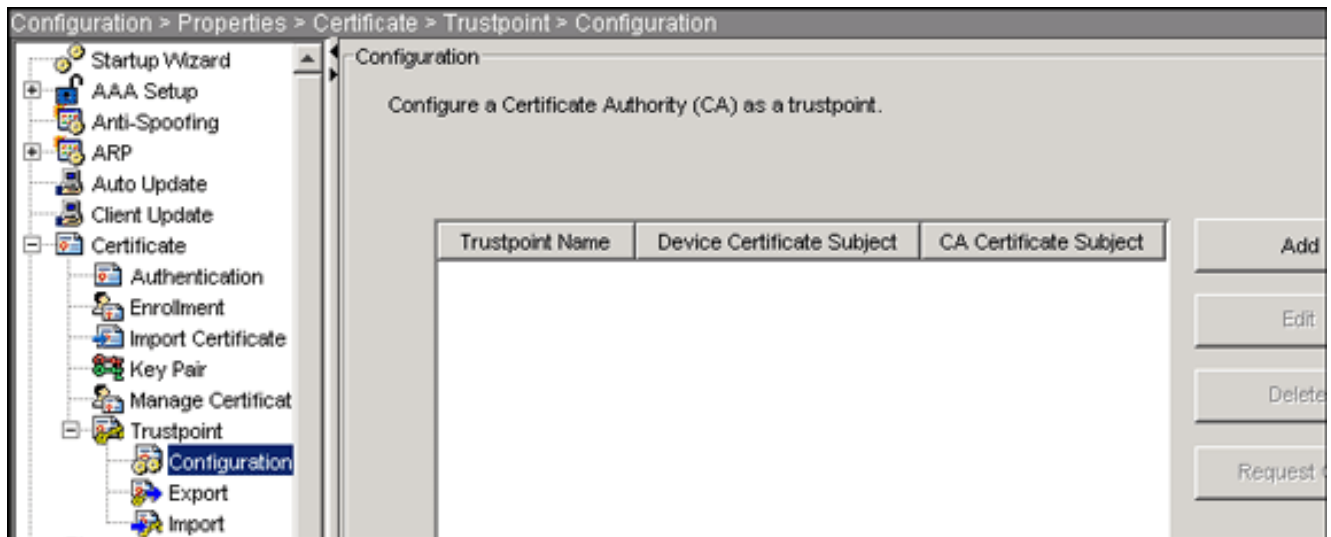
```
CiscoASA#configure terminal CiscoASA(config)#crypto key
generate rsa label my.CA.key modulus 1024 !--- Generates
1024 bit RSA key pair. "label" defines the name of the
key pair. INFO: The name for the keys will be: my.CA.key
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

Étape 3. Créez le point de confiance

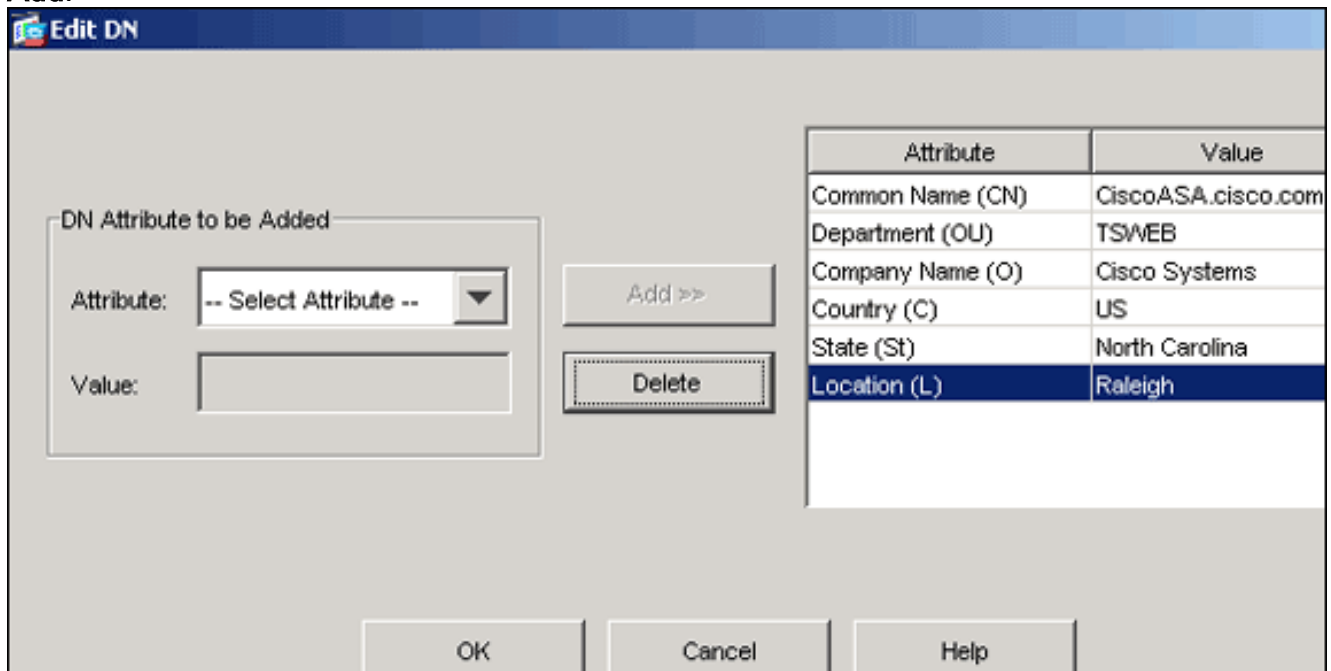
Des points de confiance sont exigés pour déclarer l'Autorité de certification (CA) que votre ASA utilisera.

Procédure ASDM

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez le **certificat**, et puis développez le **point de confiance**.
3. Choisissez la **configuration**, et puis cliquez sur **Add**.



4. Configurez ces valeurs : **Nom de point de confiance** : Le nom de point de confiance devrait être approprié à l'utilisation destinée. (Cet exemple utilise CA1.) **Paire de clés** : Sélectionnez la paire de clés générée dans l'[étape 2](#). (my.CA.key)
5. Assurez que l'Inscription manuelle est sélectionnée.
6. **Paramètres de certificat de clic**. La boîte de dialogue de paramètres de certificat apparaît.
7. Cliquez sur Edit, et configurez les attributs répertoriés dans cette table : Pour configurer ces valeurs, choisissez une valeur dans la liste déroulante Attribute, entrez la valeur, puis cliquez sur **Add**.



8. Une fois que les valeurs appropriées ont été ajoutées, cliquez sur **OK**.
9. Dans la boîte de dialogue de paramètres de certificat, écrivez le FQDN dans le domaine FQDN de spécifier. Cette valeur devrait être le même FQDN que vous avez utilisé pour le

Certificate Parameters

Enter the values for the parameters that are to be included in the certificate.

Subject DN:

Subject Alternative Name (FQDN)

Use FQDN of the device

Specify FQDN

Use none

E-mail:

IP Address:

Include device serial number

nom commun (NC).

10. Cliquez sur **OK**.

11. Vérifiez la paire de clés correcte est sélectionné, et cliquez sur la case d'option d'**Inscription manuelle d'utilisation**.

12. Cliquez sur **OK**, puis sur **Apply**.

Add Trustpoint Configuration

Trustpoint Name:

Generate a self-signed certificate on enrollment
 If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Enrollment Settings | Revocation Check | CRL Retrieval Policy | CRL Retrieval Method | OCSP

Key Pair: Show Details New Key Pair...

Challenge Password: Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint

Enrollment Mode

Use manual enrollment

Use automatic enrollment

Enrollment URL: http://

Retry Period: minutes

Retry Count: (Use 0 to indicate unlimited retries)

Certificate Parameter

OK Cancel Help

Exemple de ligne de commande

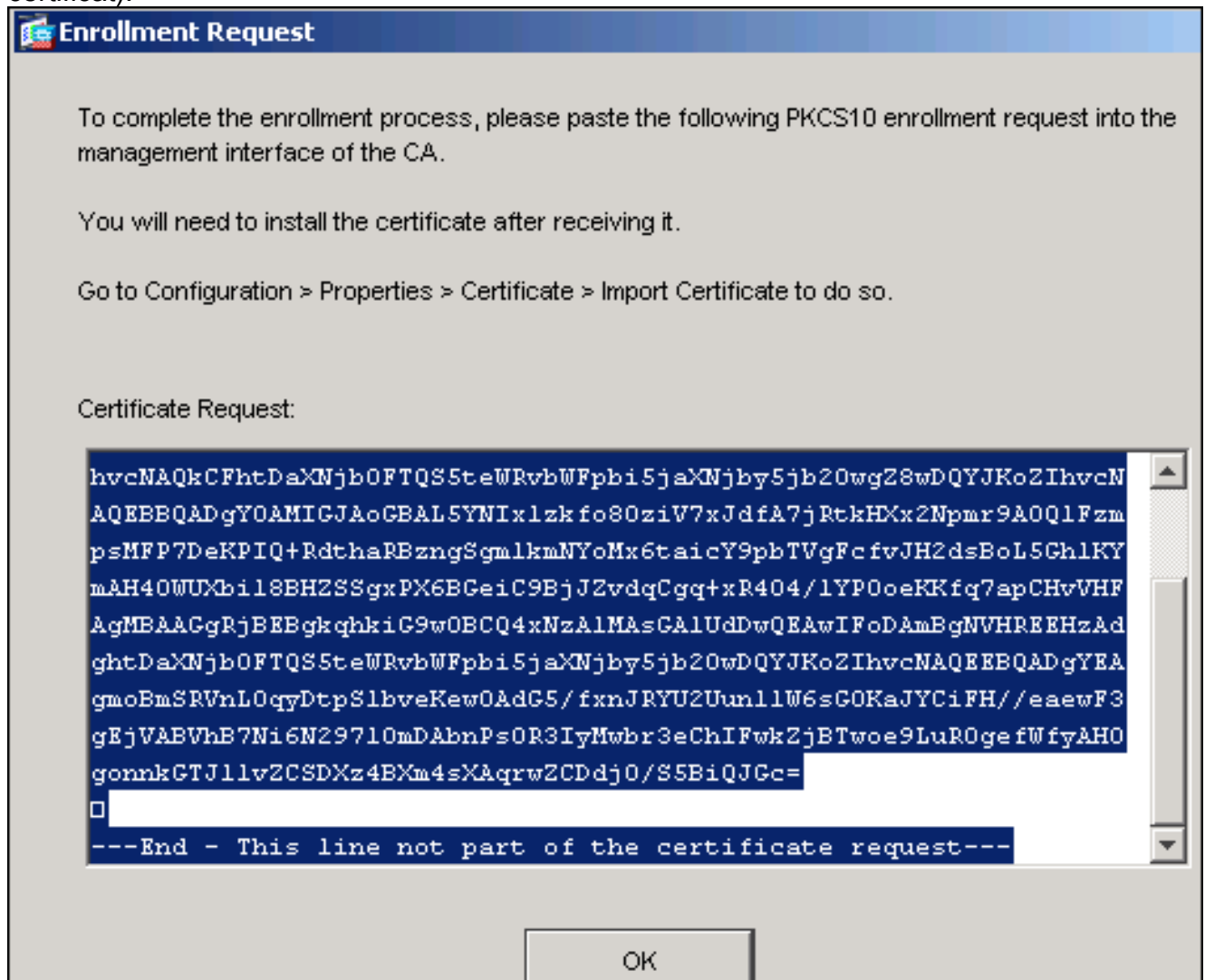
```

CiscoASA
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=wevpn.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
  
```

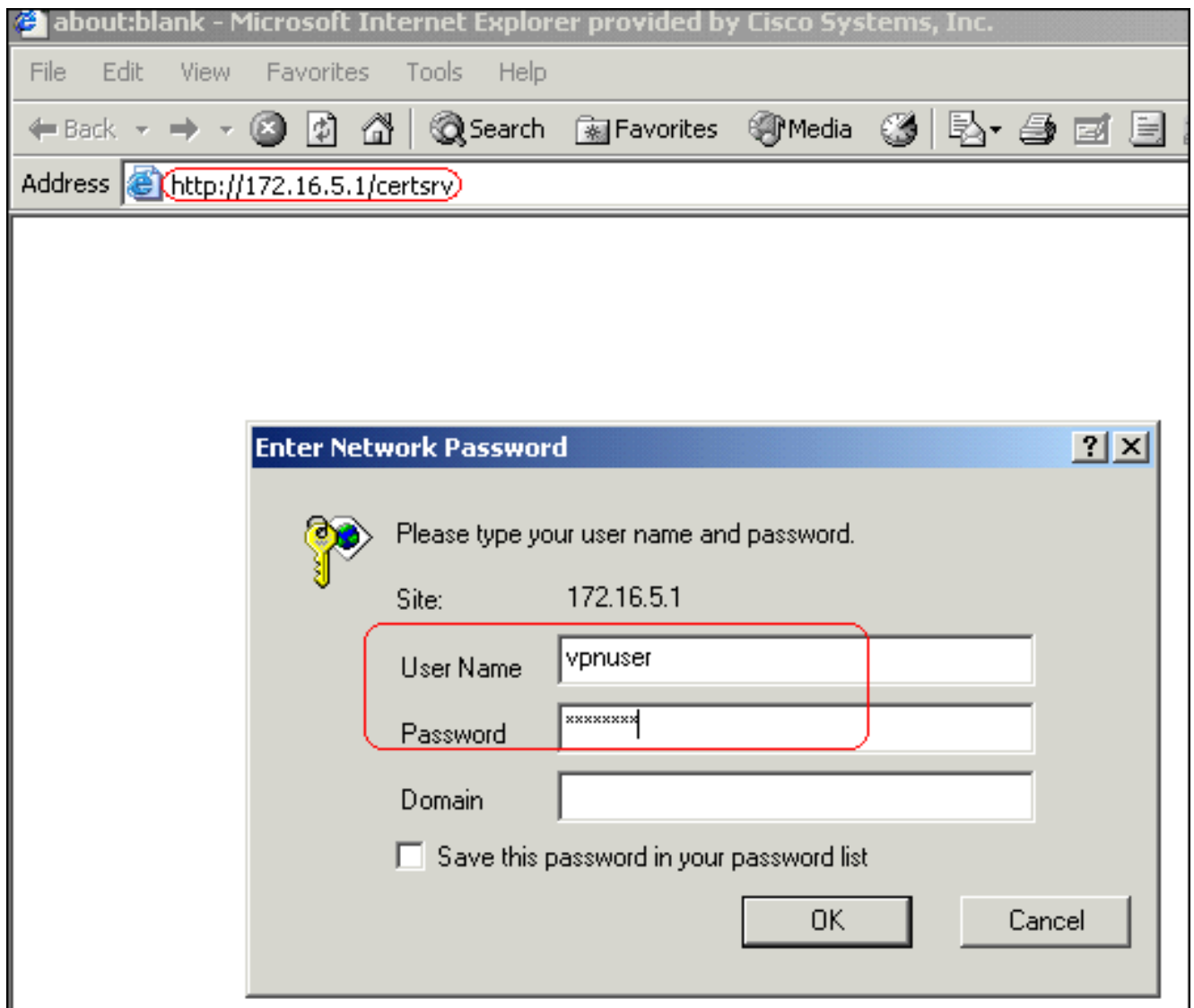
Étape 4. Générez l'inscription de certificat

Procédure ASDM

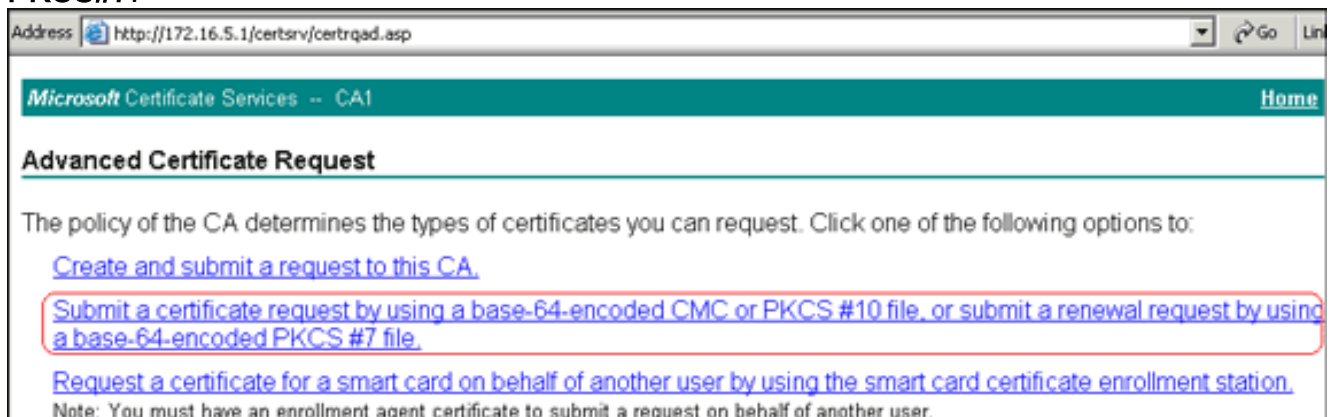
1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez le **certificat**, et choisissez l'**inscription**.
3. Vérifiez le point de confiance créé dans l'[étape 3](#) est sélectionné, et le clic **s'inscrivent**. Une boîte de dialogue apparaît qui répertorie la demande d'inscription de certificat (également désignée sous le nom d'une demande de signature de certificat).



4. Copiez la demande de l'inscription PKCS#10 sur un fichier texte, et puis soumettez le CSR enregistré à votre constructeur de tiers (tel que Microsoft CA) suivant les indications de cette procédure :Ouvrez une session au serveur 172.16.5.1 CA avec les credantials d'utilisateur fournis au serveur de vpn.



Remarque: Veillez-vous pour faire expliquer à un utilisateur l'ASA (serveur de vpn) avec le serveur CA. La demande de clic un **certificat** > a avancé la demande de certificat, et puis la sélectionne soumettent une demande de certificat à l'aide d'un fichier CMC ou PKCS#10 base-64-encoded ou soumettent une demande de renouvellement à l'aide d'un fichier base-64-encoded PKCS#7.



Copiez et collez les informations encodées dans le champ texte **enregistré de demande**, et cliquez sur

Submit a Certificate Request or Renewal Request

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

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBKjCCAQIBAgIBADANBgkqhkiG9w0BAQQFAAO
4BfcXd2OLCbXAoP5L1KbPaEeaCkfN/Pp5mATAsG8
D6MEG6cu7Bxj/K1Z6MxafUvCHrOPYWVU1wgRJGh+
t8Ux9emhFHpGHnQ/MpSfUOdQ==
-----END CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

Certificate Template:

IPSEC

Additional Attributes:

Attributes:

Submit >

Submit.


Cliquez sur la case d'option **Codé en base 64**, puis sur **Télécharger le**

Microsoft Certificate Services -- CA1

Certificate Issued

The certificate you requested was issued to you.

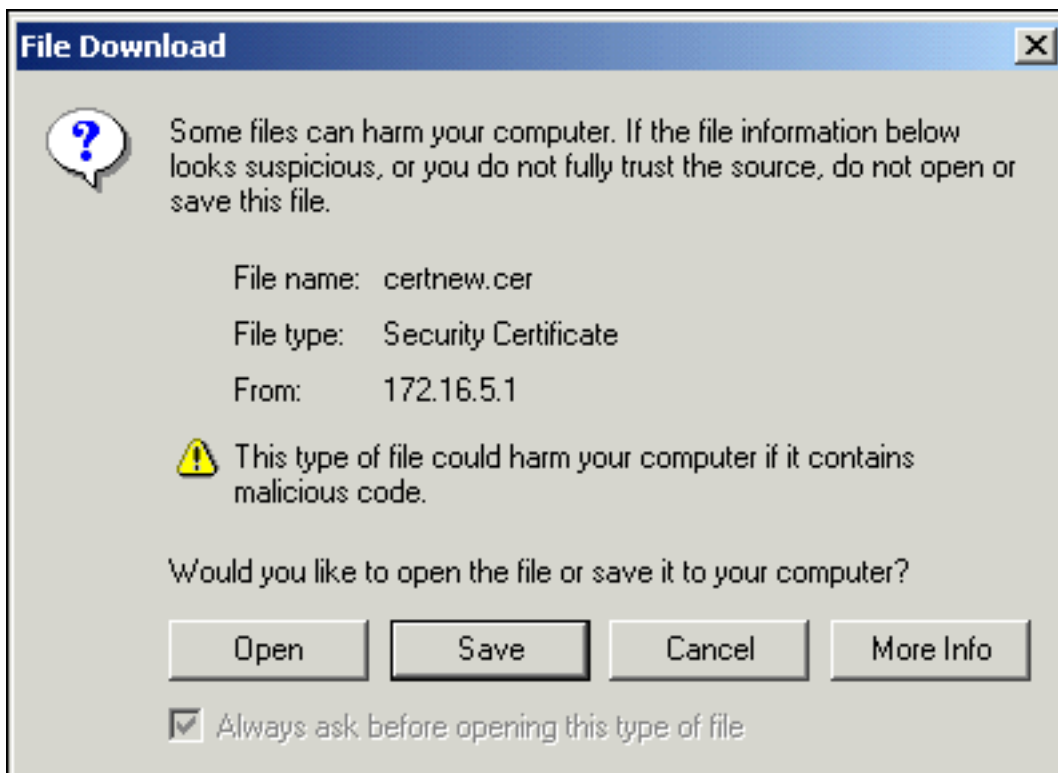
DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

certificat.

Quand la

case de dialob de téléchargement de fichier apparaît, sauvegardez-la avec le nom **cert_client_id.cer**, qui est le certificat d'identité à installer sur



'ASA.

Exemple de ligne de commande

```

CiscoASA
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:
MIICHjCCAYcCAQAwgAxEADA0BgNVBACTBlJhbGVpZ2gxZmZzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczEO
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRip9cyQp/983pm5PfDD6/ho0nTktx0i+lcEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMS4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUAA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKUlARc783w4BMO51ulIEhHgRqAxrTbQn0B7JPI
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)#
```

Étape 5. Authentifiez le point de confiance

Une fois que vous recevez le certificat d'identité du constructeur de tiers, vous pouvez poursuivre cette étape.

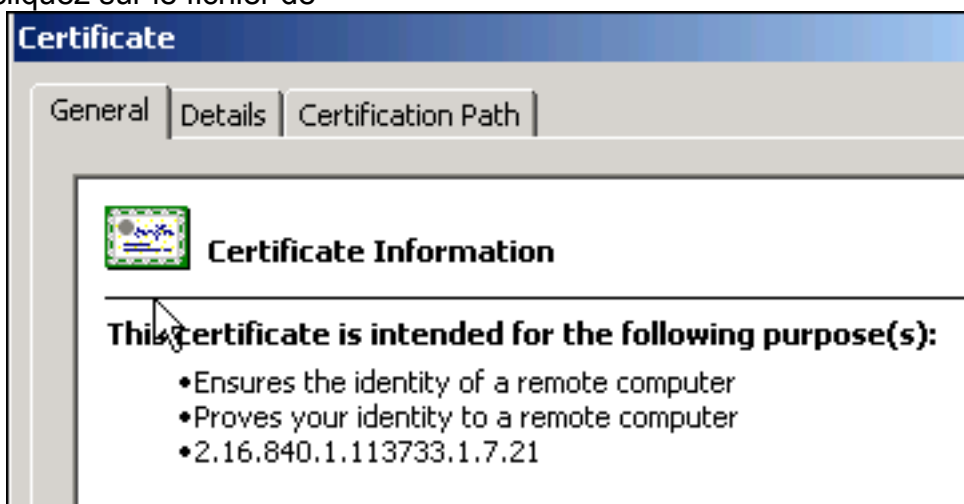
Procédure ASDM

1. Enregistrez le certificat d'identité sur votre ordinateur local.
2. Si vous étiez fourni un certificat base64-encodé qui n'a pas été livré comme fichier, vous devez copier le message base64, et le collez dans un fichier texte.
3. Renommez le fichier avec une extension de .cer. **Remarque:** Une fois le fichier est renommé avec l'extension de .cer, l'icône de fichier devrait afficher comme certificat comme



affiché.

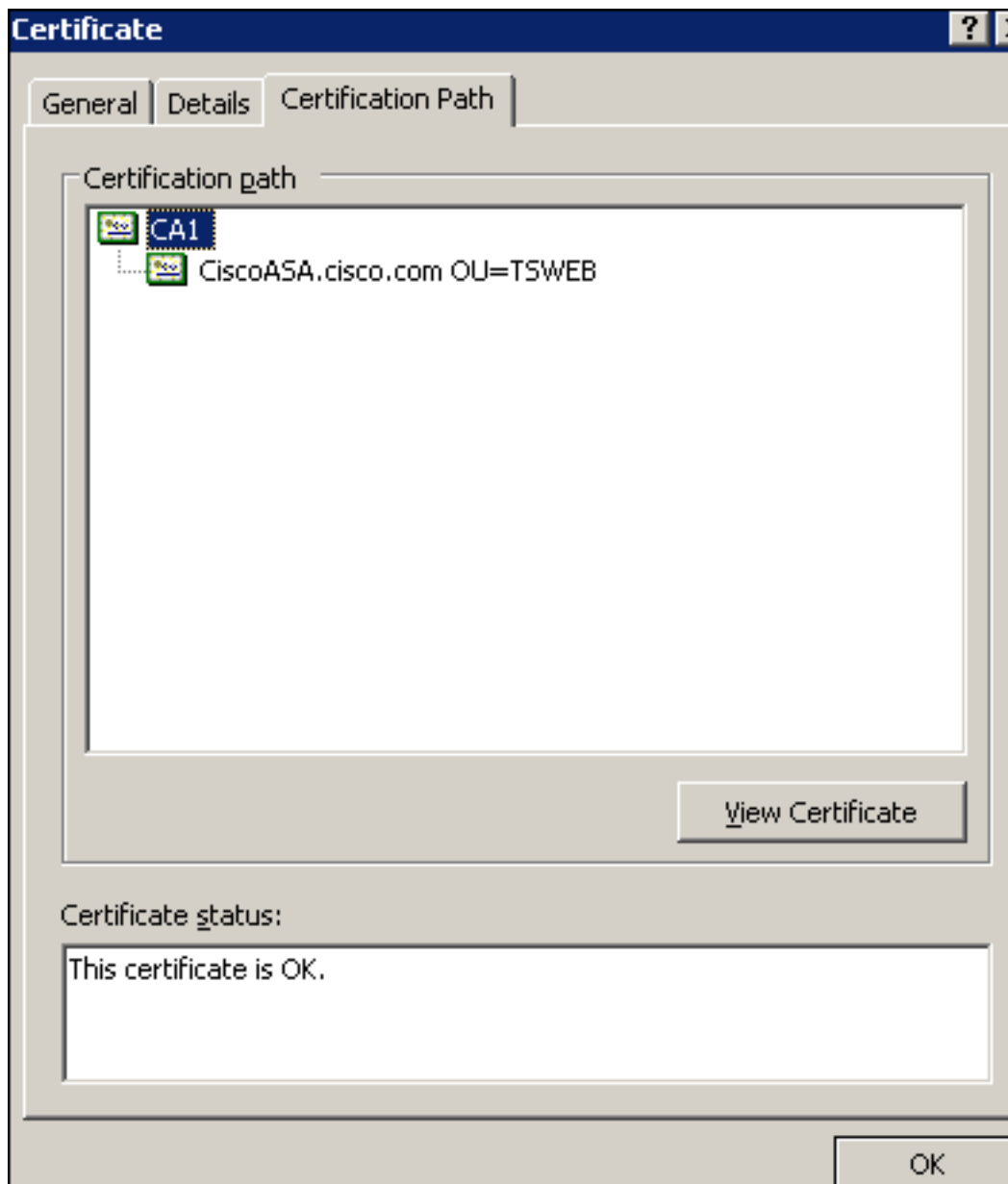
4. Double-cliquez sur le fichier de



certificat.

Remarque: Si « Windows n'a pas assez d'informations pour vérifier ce certificat » le message apparaît dans l'onglet Général, vous devez obtenir la racine CA de constructeur de tiers ou le certificat de CA intermédiaire avant que vous continuiez cette procédure. Contactez votre constructeur de tiers ou administrateur CA afin d'obtenir la racine émettante CA ou le certificat de CA intermédiaire.

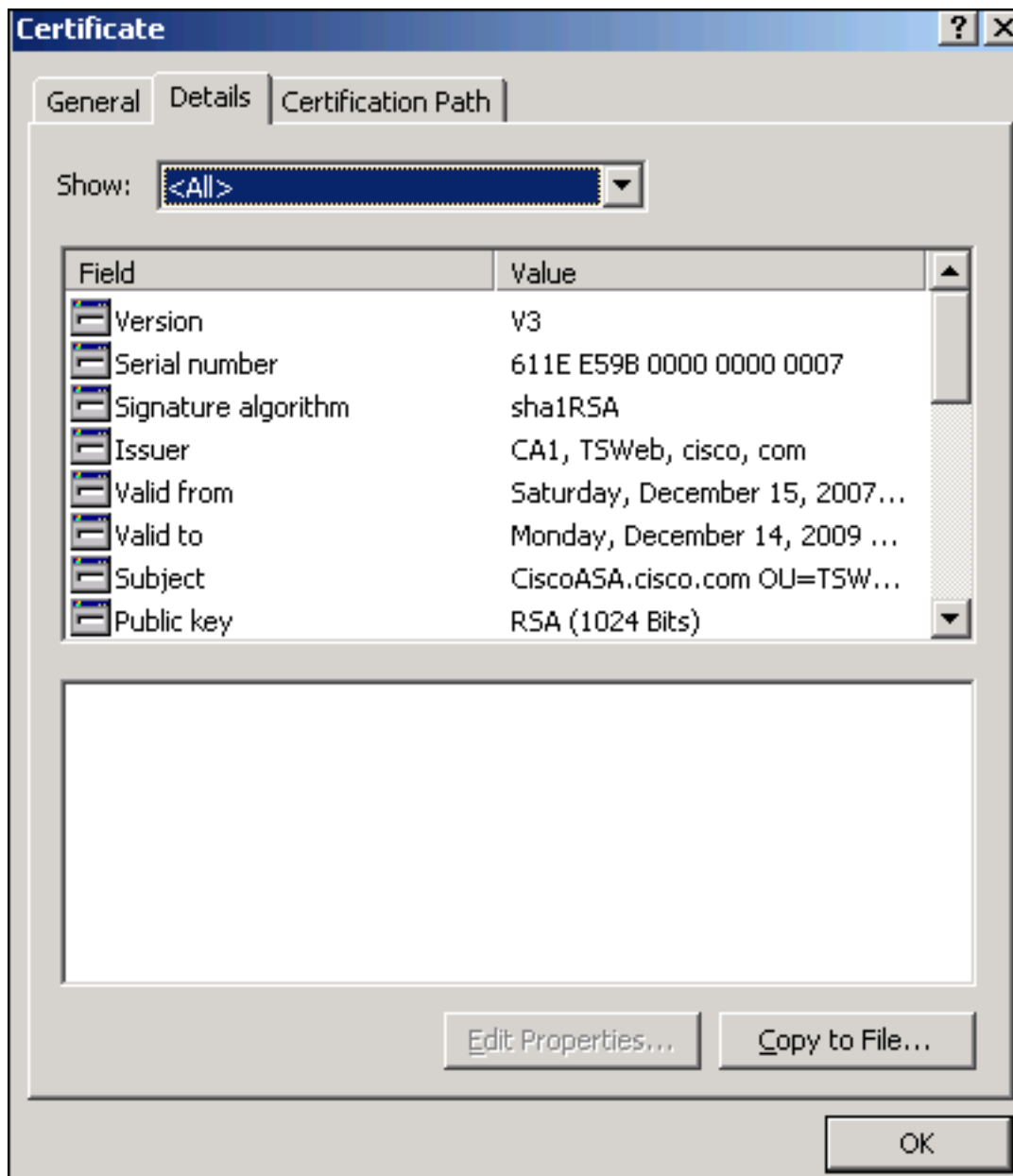
5. Cliquez sur l'onglet de **chemin de certificat**
6. Cliquez sur le certificat de CA situé au-dessus de votre certificat d'identité délivré, et cliquez sur le **certificat de**



vue. Les

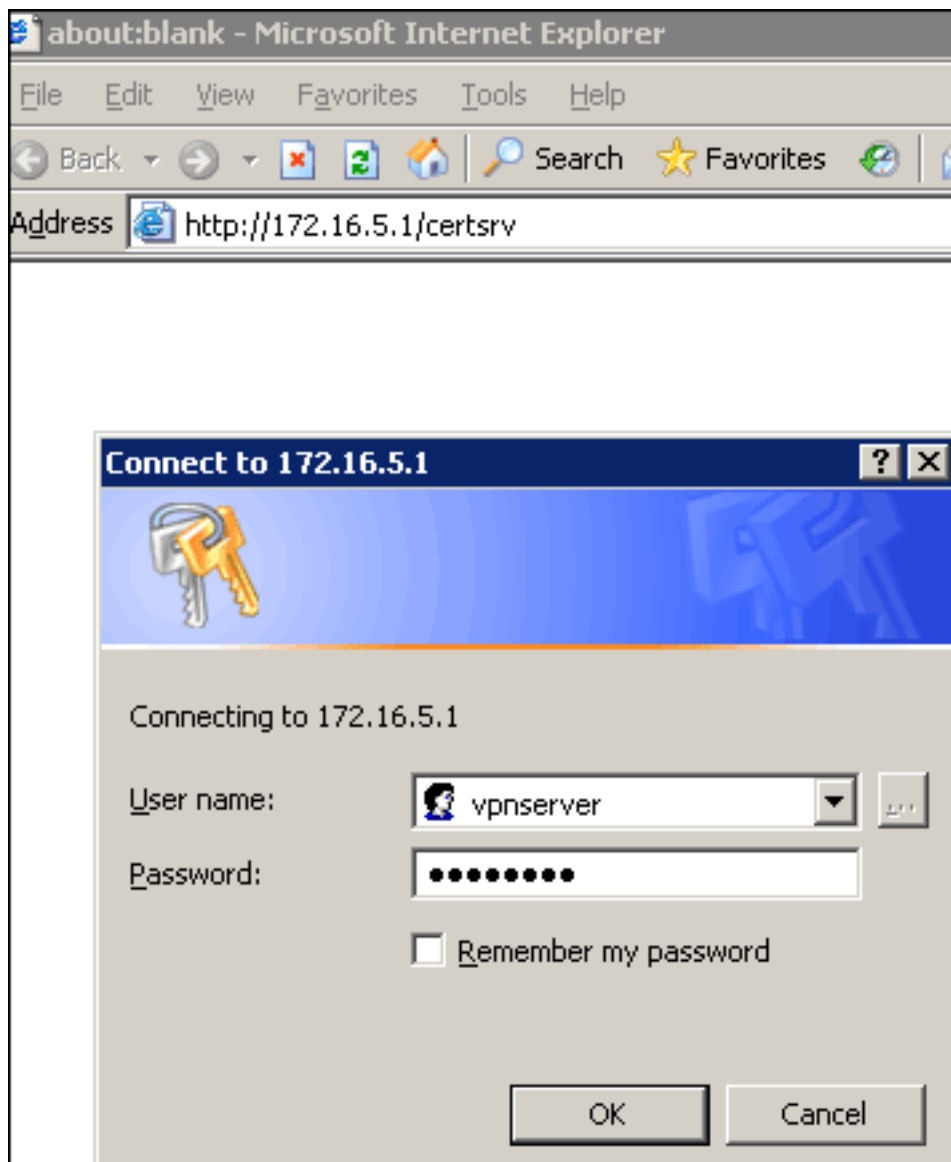
informations détaillées au sujet du certificat d'authentification apparaissent.

7. Cliquez sur **Details** afin d'en savoir plus sur le certificat



d'identité.

8. Avant que vous installiez le certificat d'identité, le certificat de CA doit être téléchargé du serveur CA et être installé dans l'ASA. Terminez-vous ces étapes afin de télécharger le certificat de CA du serveur CA nommé CA1 :Ouvrez une session au serveur 172.16.5.1 CA avec des credantials d'utilisateur fournis au serveur de



vpn.

Cliquez sur

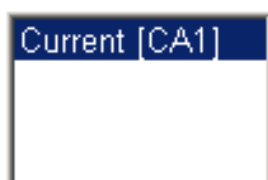
Download un **certificat de CA, une chaîne de certificat ou un CRL**, et puis sélectionnez la case d'option de la **base 64** afin de spécifier la méthode de codage. Cliquez sur le **certificat de CA de téléchargement**.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
 Base 64

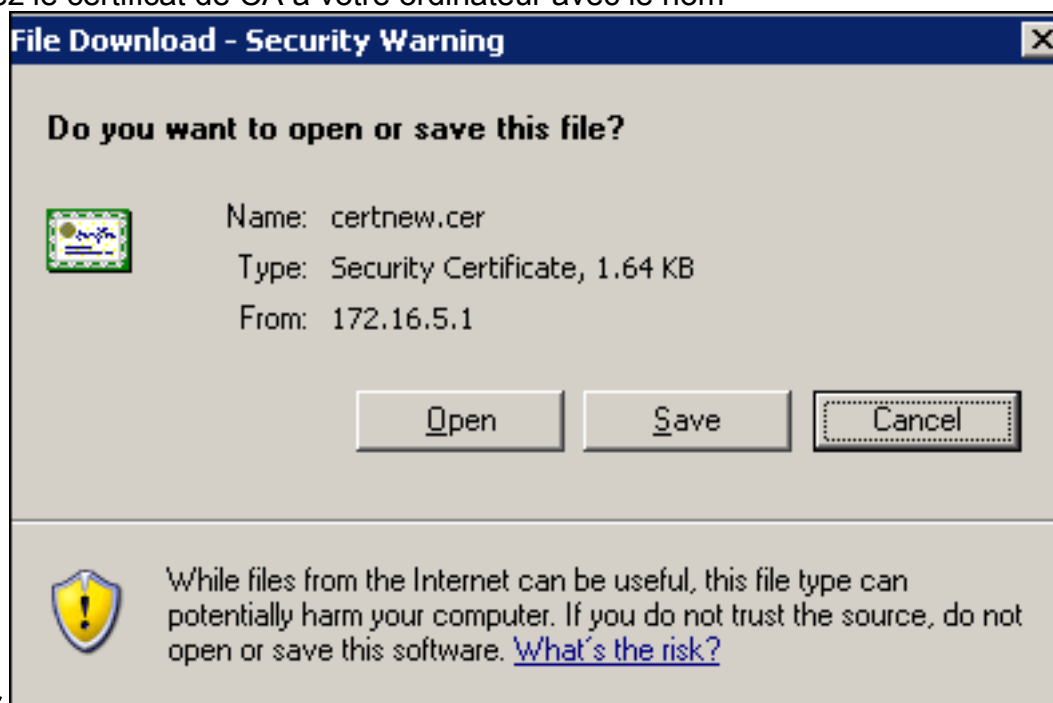
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

Sauvegardez le certificat de CA à votre ordinateur avec le nom



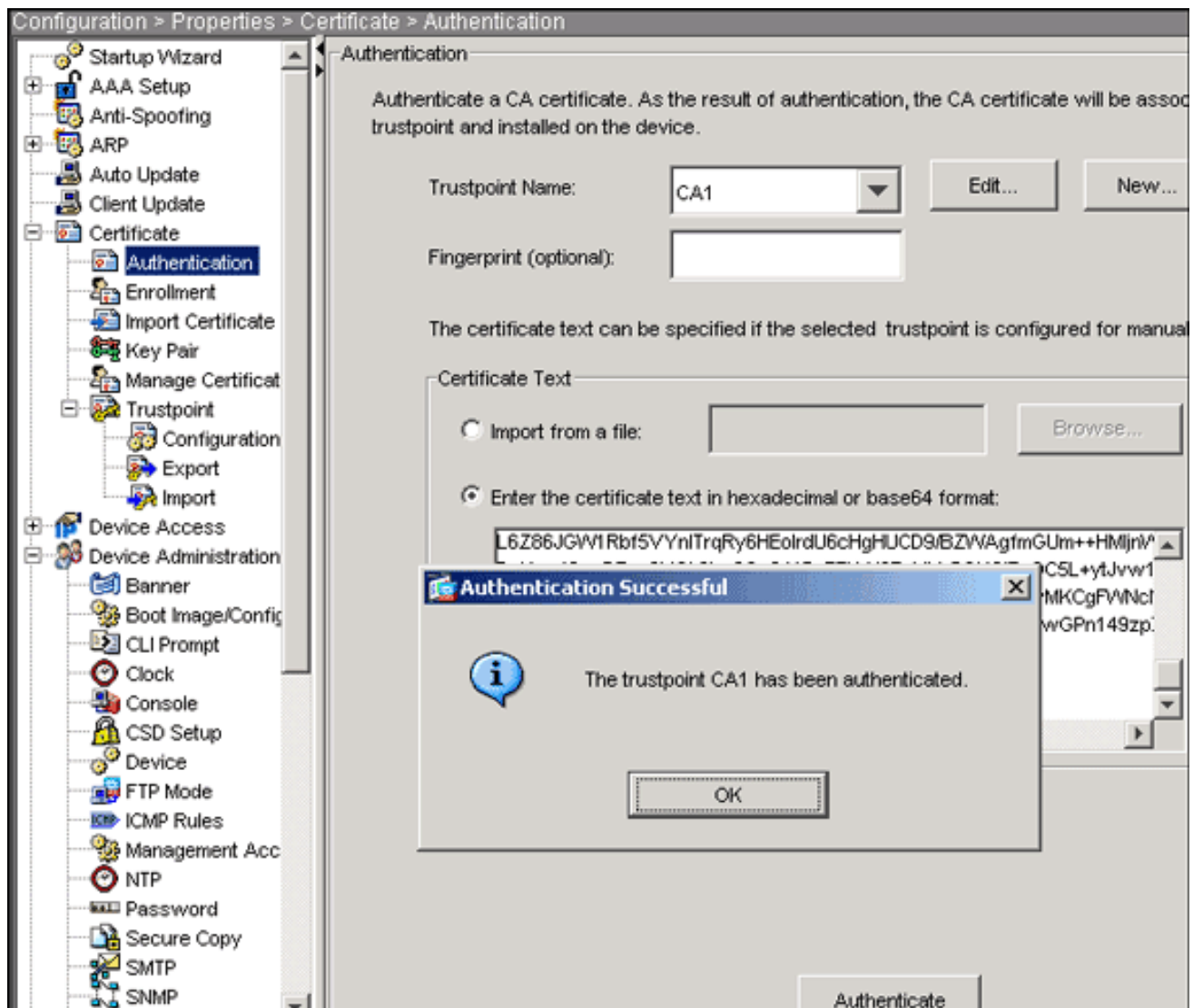
certnew.cer.

9. Naviguez jusqu'à l'emplacement où vous avez enregistré le certificat d'autorité de certification.
10. Ouvrez le fichier avec un éditeur de texte, tel que le Bloc-notes. (Cliquez avec le bouton droit le fichier, et choisissez **envoient à > Notepad.**)
11. Le message base64-encoded devrait ressembler au certificat dans cette image

:

```
certnew.cer - Notepad
File Edit Format Help
-----BEGIN CERTIFICATE-----
MIIEntCCA4wgAwIBAgIQcJnxmUdk4JxGudqAowt0nDANBgkqhkiG9w0BAQUFADBR
MRMwEQYKCZImiZPyLGQBGRYDY29tMRUwEwYKCZImiZPyLGQBGRYFY2IzY28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dIYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIXNDA2MDE0
Ml0XDTEyMTIXNDA2MTAxNVowUTETMBEGCgmsJomT8ixkARKWA2NvbTEVMBMGCgms
JomT8ixkARKwBWNpc2NvMRUwEwYKCZImiZPyLGQBGRYFVFNXZWIXDDAKBgnVBAMT
A0NBMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAAOqP7seuvvyiLmA9
BSGZMz3sctR9TCMwOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd4TNgntjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vweMijcqnwdoq+
Kx+swaenCjslrxeuaHpIBTuaNOckueBUBjxgpJUNPAk1G8YwBfaTV4M7kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQXRvwhdbMivwqYBXWkh4uc04xxQmr//Sct1tdwQcvk2V
UBwCsptw7C1akTqfm5XK/d//z2euuxrHYysQCfoFyk1vE6/qlo+fQessz+Tldhxx
wPXRO18CAwEAAaOCaw8wggFrMBMGCSSGAQQBggjCUAgQHgQAQwBBMASGA1UddwQE
AwIBhjAPBgnVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRDL3myfNQJ
pAPlwDCCAQMGA1UdHwSB+zCB+DCB9aCB8qCB74aBtwxkYXA6Ly8vQ049Q0ExLENO
PVRTLvcyszmtQUNTLENOPUNEUCxDTj1QdwJsawMlMjBLZXklMjBTZXJ2awNlcYxD
Tj1TZXJ2awNlcYxDTj1Db25mawd1cmF0aw9uLERDPVRTV2viLERDPwnpc2NvLERD
Pwnvbt9jZXJ0awZpY2F0ZVJldm9jYXRpb25maxN0P2Jhc2U/b2JqZWNOQ2xhc3M9
Y1JMRG1zdHJpYnV0aw9uUG9pbnsGNwH0dHA6Ly90cy13MmszLWwFjcy50c3dlYi5j
aXNjby5jb20vQ2vydEVucm9sbc9DQTEuY3JsMBAGCSsGAQQBggjCVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAavFpAsyESItqa+7sii/5L+KUV34/DoE4MibXJekr
L6Z86JGw1Rbf5VynlTrqRy6HEo1rdU6cHgHUCD9/BZWagfmGUM++HMLjnw8liyIF
DcnwxlQxsDT+n9Yok6bnG6uof4SgETNrN8EyyVrSGK0lE+OC5L+ytJvw19Gzh1ze
lOVUFPA+PT47dmAR6Uo2V2ZDW5KGAVLU8GsrFd8wZDPBVMKCGFwNcNItcufu0x1b
LXXc68DKoZY09pPq877uTaou8cLtuipPomeOyzgJ0N+xaZx2EwGPN149zpxv5tqt
9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+p85at
-----END CERTIFICATE-----
```

12. Dans l'ASDM, la **configuration de clic**, et cliquent sur alors **Properties**.
13. Développez le **certificat**, et choisissez l'**authentification**.
14. Cliquez sur l'**entrer le texte de certificat dans la case d'option d'hexadécimal ou de format base64**.
15. Collez le certificat de CA base64-formatted de votre éditeur de texte dans la zone de texte.
16. Le clic **authentifiant**.



17. Cliquez sur OK.

Exemple de ligne de commande

CiscoASA

```

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
MRMwEQYKCZImiZPyLQGGRYDY29tMRUwEwYKCZImiZPyLQGGRYFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dlYjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIx
NDA2MDE0
M1oXDTEyMTIxNDA2MTAxNVowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCS
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQGGRYFVFNXZWIxDDAK
BgNVBAMT
A0NBMTCCASIdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbdosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaenCjs1rxuAhpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI

```

```

y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvWqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQQGHgQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBTZrb8I8jqI8RRD
L3mYfnQJ
pAP1WDCCAQMGA1UdHwsB+zCB+DCB9aCB8qCB74aBtWxkYXA6Ly8vQ049
Q0ExLENO
PVRTLVcysZmtQUNTLENOPUNEUCxDTj1QdWJsaWMLmjBLZXk1mjBTZXJ2
aWN1cyxD
Tj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPVRTV2ViLERDPWNp
c2NvLERD
PWNvbT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNO
Q2xhc3M9
Y1JMRGlzdHJpYnV0aW9uUG9pbnsGNWh0dHA6Ly90cy13MmszLWFjcy50
c3dlYi5j
aXNjby5jb20vQ2VydeVucm9sbC9DQTEuY3JsMBAGCSsGAQQBgjcVAQQD
AgEAMA0G
CSqGSIB3DQEBBQUAA4IBAQAavFpAsyESItqA+7sii/5L+KUV34/DoE4M
icbXJeKr
L6Z86JGw1Rbf5VYnlTrqRy6HEolrdU6cHgHUCD9/BZWAqfmGUm++Hm1j
nW8liyIF
DcNwxlQxsDT+n9YOk6bnG6uOf4SgETNrN8EyYVrSGKOLE+OC5L+ytJvw
19GZhlzE
lOVUfPA+PT47dmAR6Uo2V2zDW5KGAVLU8GsrFd8wZDPBvMKCGFWNcNI
tcfu0xlb
lXXc68DKoZY09pPq877uTaou8cLtuuiPomeOyZgJ0N+xaZx2EwGpN149
zpXv5tqt 9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dxlVD+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)#

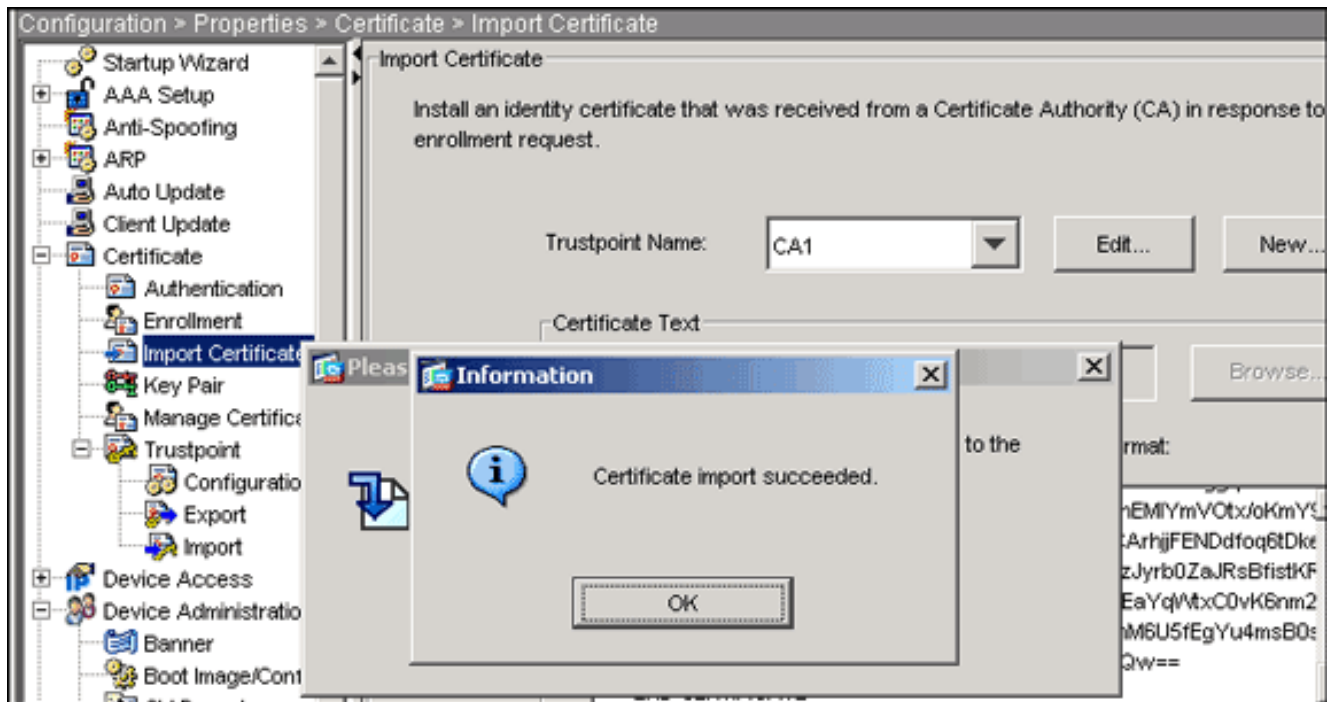
```

Étape 6. Installez le certificat

Procédure ASDM

Utilisez le certificat d'identité fourni par le constructeur de tiers pour exécuter ces étapes :

1. Cliquez sur **Configuration**, et ensuite sur **Properties**.
2. Développez le **certificat**, et puis choisissez le **certificat d'importation**.
3. Cliquez sur **l'entrer le texte de certificat dans la case d'option d'hexadécimal ou de format base64**, et collez le certificat d'identité base64 dans le champ **texte**.



4. Cliquez sur l'importation, et puis cliquez sur OK.

Exemple de ligne de commande

CiscoASA

```

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
CZImiZPyLGQBGRYDY29tMRUwEwYKZImiZPyLGQBGRYFY2l2Y28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1d1YjEMMAoGA1UEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoxDTA5
MTIxNDA4MzUzOVowdJELMAkGA1UEBhMCVVMxZjZAVBgNVBAGTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRQwEwYDVRQKEw1DaXNjbyBTeXNO
ZWl2MSQw
IgyDVQQDEXTDaXNjbyBFTQs5jaXNjby5jb20gT1U9VFNXRUlwgZ8wDQYJ
KoZlhvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2YAc1AI03NdI8UpW5JHK14C
qB9j3HpX
BmFXVF5/mNPUI5tCq4+vC+i105T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcZ3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBywFIISQ2l2
Y29BU0Eu
Y2l2Y28uY29tMB0GA1UdDgQWBBSJC3bSQzeGv4tY+MeH7KML0xCFjAF
BgnVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAP1WDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
aWMLMjBLZXk1MjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdl
cmF0aW9u

```

```
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnsG
NWh0dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjby5jb20vQ2VydeVucm9sbC9D
QTEuY3Js
MIIBHQYIKwYBBQUHAQEgEPMIIBCzCBQQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDtj1BSUESQ049UHVibGljJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjbyxEQz1j
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25B
dXR0b3Jp
dHkwXQYIKwYBBQUHMAKGUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjby5j
b20vQ2VydeVucm9sbC9UUy1lXmksZLUFDUy5UU1dlYi5jaXNjby5jb21f
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFCAZQBIAFMAZQByAHYAZQByMAWGA1Ud
EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAAwEwDQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzCWAEVRXCyBlx0NpR/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkZlGEpuBnENTohdhtz5vBjGlcROXIs8
+3Ghg8hy
YZZEM73e8EC0sEMedFb+KYpAFy3PPy418EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTFPNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnFlzCnqfcyHcETieZtS
tlnwLpsc 1L5nuPsd8MaexBc= -----END CERTIFICATE----- quit
INFO: Certificate successfully imported
CiscoASA(config)#
```

[Étape 7. Configurez l'Accès à distance VPN \(IPSec\) pour utiliser le certificat nouvellement installé](#)

Procédure ASDM

Complétez ces étapes afin de configurer le VPN d'accès à distance :

1. Choisissez la **configuration > le VPN > l'IKE > les stratégies > ajoutent** afin de créer une stratégie ISAKMP 65535 suivant les indications de cette image.

Add IKE Policy

Priority: Authentication:

Encryption: D-H Group:

Hash: Lifetime: Unlimited

2. Cliquez sur **OK**, puis sur **Apply**.
3. Choisissez la **configuration > le >Add VPN > d'IPSec > de jeux de transformations** afin de créer un jeu de transformations (*myset*) suivant les indications de cette image

Add Transform Set

Set Name:

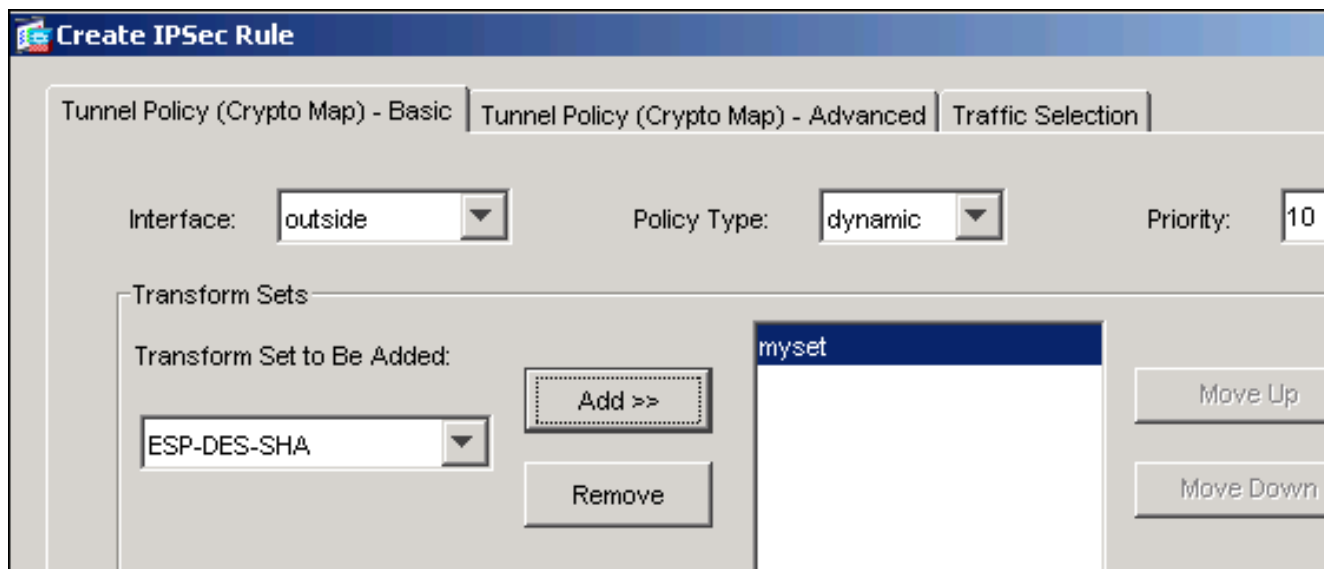
Properties

Mode: Tunnel Transport

ESP Encryption:

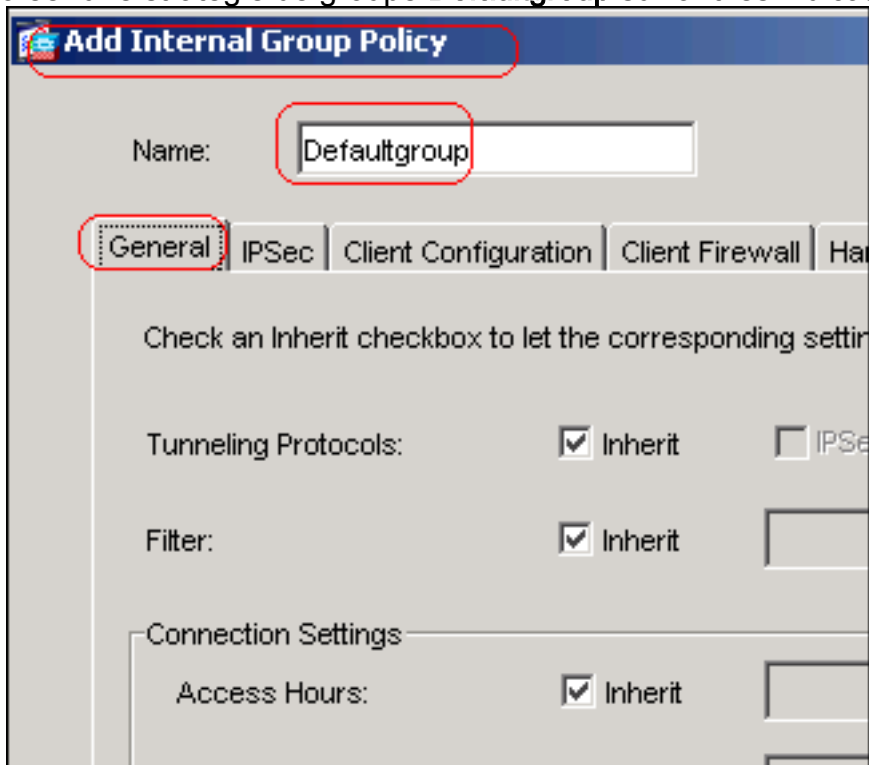
ESP Authentication:

4. Cliquez sur **OK**, et puis **appliquez**
 5. Choisissez la **configuration > le >Add VPN > d'IPSec > de règles IPSecs** afin de créer un crypto map avec la stratégie dynamique de la priorité 10 suivant les indications de cette image
- :



6. Cliquez sur OK, et puis **appliquez**

7. Choisissez le **Configuration > VPN > General > Group Policy > l'Add Internal Group Policy** afin de créer une stratégie de groupe **Defaultgroup** suivant les indications de ces



images.

The screenshot shows the 'Add Internal Group Policy' dialog box with the 'Client Configuration' tab selected. The 'Name' field contains 'Defaultgroup'. Below the tabs, there is a checkbox for 'Inherit' which is checked. Underneath, there are three sub-tabs: 'General Client Parameters', 'Cisco Client Parameters', and 'Microsoft Client Parameters'. In the 'Cisco Client Parameters' section, the 'Default Domain' field is set to 'cisco.com' and its 'Inherit' checkbox is unchecked. Red circles highlight the 'Client Configuration' tab and the 'cisco.com' text.

8. Cliquez sur OK, et puis **appliquez**

9. Choisissez la **configuration > le VPN > la gestion d'adresse IP > les groupes IP > ajoutent** afin de configurer le vpnpool de pool d'adresses pour que les utilisateurs de client vpn soient

The screenshot shows the 'Add IP Pool' dialog box. The 'Name' field contains 'vpnpool'. The 'Starting IP Address' field contains '10.5.5.10'. The 'Ending IP Address' field contains '10.5.5.20'. The 'Subnet Mask' field contains '255.255.255.0'. At the bottom, there are three buttons: 'OK', 'Cancel', and 'Help'.

assignés dynamiquement.

10. Cliquez sur OK, et puis **appliquez**

11. Choisissez la **configuration > le VPN > le général > les utilisateurs > ajoutent** afin de créer un **vpnuser de** compte utilisateur pour l'accès de client

Add User Account

Identity | VPN Policy | WebVPN

Username: vpnuser

Password: *****

Confirm Password: *****

User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

vpn.

12. Ajoutez cet utilisateur à **DefaultRAGroup**.

Add User Account

Identity | VPN Policy | WebVPN

Check an Inherit checkbox to let the corresponding setting take its value from the group

Group Policy: Inherit

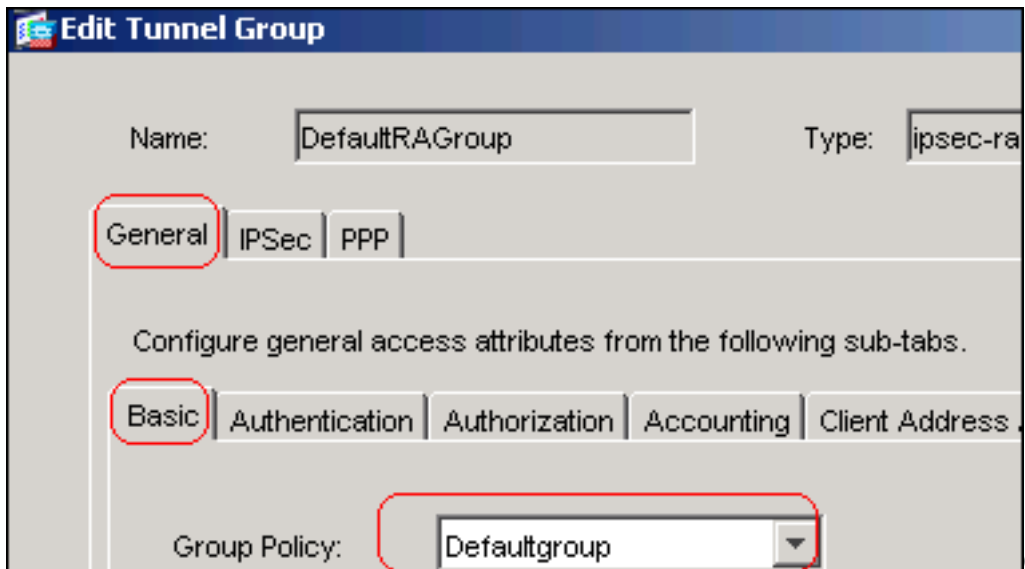
Tunneling Protocols: Inherit IPsec WebVPN

Filter: Inherit

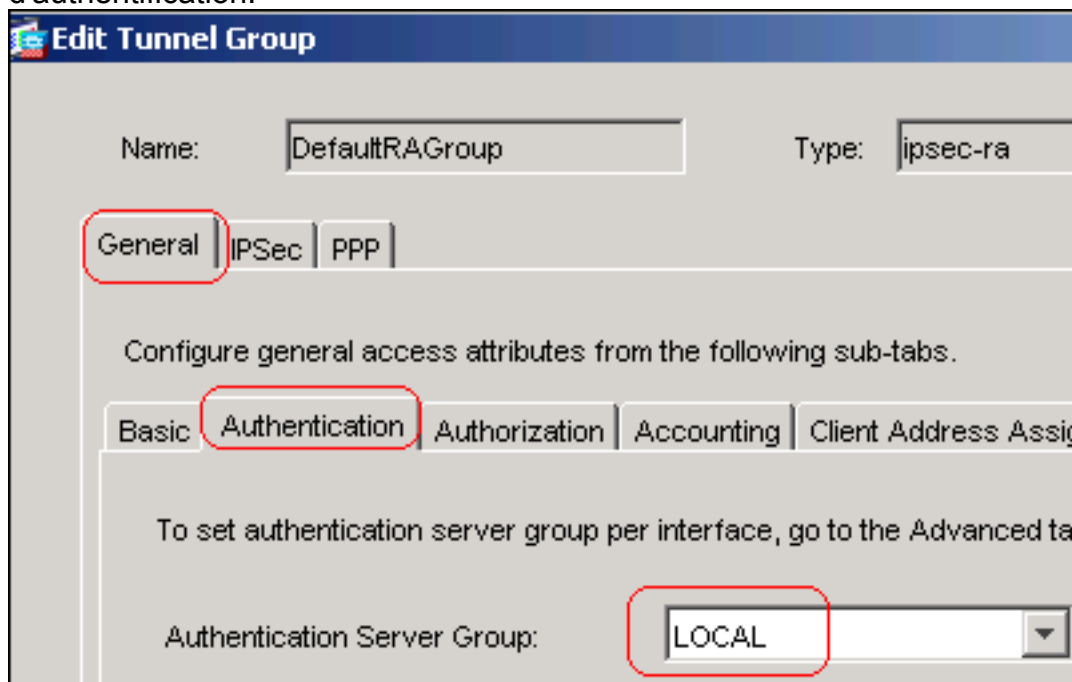
Tunnel Group Lock: Inherit DefaultRAGroup

Store Password on Client System: Inherit Yes No

13. Cliquez sur OK, et puis **appliquez**
14. Éditez le DefaultRAGroup comme décrit dans cette procédure :Choisissez la **configuration > le VPN > le groupe de général > de tunnel > éditent**.Choisissez **Defaultgroup** de la liste déroulante de stratégie de



groupe. Choisissez les **GENS DU PAYS** de la liste déroulante de groupe de serveurs d'authentification.



Choisissez le **vpnpool** de la liste déroulante d'affectation d'adresse du

Edit Tunnel Group

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | **Client Address Assignment**

To specify whether to use DHCP or address pools for address assignment > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab

Available Pools	Assigned
<input type="text"/>	<input type="text" value="vpnpool"/>

client.

15. Cliquez sur OK, et puis appliquez.

Exemple de ligne de commande

```

CiscoASA
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

```

Résumé de configuration ASA

CiscoASA

```

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
15301306 0a099226 8993f22c 64011916 05636973 636f3115
3013060a 09922689 93f22c64 01191605 54535765 62310c30
0a060355 04031303 43413130 1e170d30 37313232 37313430
3033365a 170d3038 31323236 31343030 33365a30 67311330
11060a09 92268993 f22c6401 19160363 6f6d3115 3013060a
09922689 93f22c64 01191605 63697363 6f311530 13060a09
92268993 f22c6401 19160554 53576562 310e300c 06035504
03130555 73657273 31123010 06035504 03130976 706e7365
72766572 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 0001a382
03313082 032d300b 0603551d 0f040403 02052030 34060355
1d11042d 302ba029 060a2b06 01040182 37140203 a01b0c19
76706e73 65727665 72405453 5765622e 63697363 6f2e636f
6d301d06 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
25323053 65727669 6365732c 434e3d53 65727669 6365732c
434e3d43 6f6e6669 67757261 74696f6e 2c44433d 54535765
622c4443 3d636973 636f2c44 433d636f 6d3f6365 72746966
69636174 65526576 6f636174 696f6e4c 6973743f 62617365
3f6f626a 65637443 6c617373 3d63524c 44697374 72696275
74696f6e 506f696e 74863568 7474703a 2f2f7473 2d77326b
332d6163 732e7473 7765622e 63697363 6f2e636f 6d2f4365
7274456e 726f6c6c 2f434131 2e63726c 3082011d 06082b06
01050507 01010482 010f3082 010b3081 a906082b 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
01050507 30028651 68747470 3a2f2f74 732d7732 6b332d61
63732e74 73776562 2e636973 636f2e63 6f6d2f43 65727445
6e726f6c 6c2f5453 2d57324b 332d4143 532e5453 5765622e
63697363 6f2e636f 6d5f4341 312e6372 74301506 092b0601
04018237 14020408 1e060045 00460053 300c0603 551d1301
01ff0402 30003015 0603551d 25040e30 0c060a2b 06010401
82370a03 04304406 092a8648 86f70d01 090f0437 3035300e
06082a86 4886f70d 03020202 0080300e 06082a86 4886f70d
03040202 00803007 06052b0e 03020730 0a06082a 864886f7
```

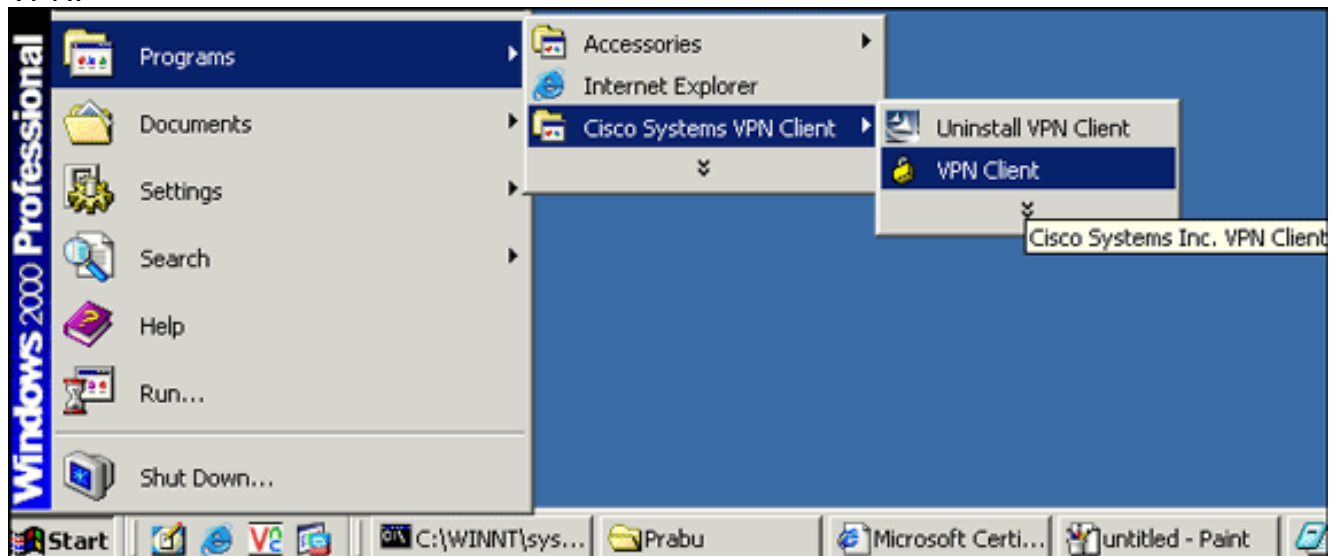
0d030730 0d06092a 864886f7 0d010105 05000382 010100bf
99b9daf2 e24f1bd6 ce8271eb 908fad3 772df610 0e78b198
f945f379 5d23a120 7c38ae5d 8f91b3ff 3da5d139 46d8fb6e
20d9a704 b6aa4113 24605ea9 4882d441 09f128ab 4c51a427
fa101189 b6533eef adc28e73 fcfed3f1 f4e64981 0976b8a1
2355c358 a22af8bb e5194b42 69a7c2f6 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
05545357 6562310c 300a0603 55040313 03434131 30820122
300d0609 2a864886 f70d0101 01050003 82010f00 3082010a
02820101 00ea8fee c7ae56fc a22e603d 0521b333 3dec0ad4
7d4c2316 3bleea33 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
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 03020186 300f0603
551d1301 01ff0405 30030101 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
06010401 82371501 04030201 00300d06 092a8648 86f70d01
01050500 03820101 001abc5a 40b32112 22da80fb bb228bfe
4bf8a515 df8fc3a0 4e0c89c6 d725e2ab 2fa67ce8 9196d516
dfe55627 953aea47 2e871289 6b754e9c 1e01d408 3f7f0595
8081f986 526fbc1c 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
bl699c76 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#
```

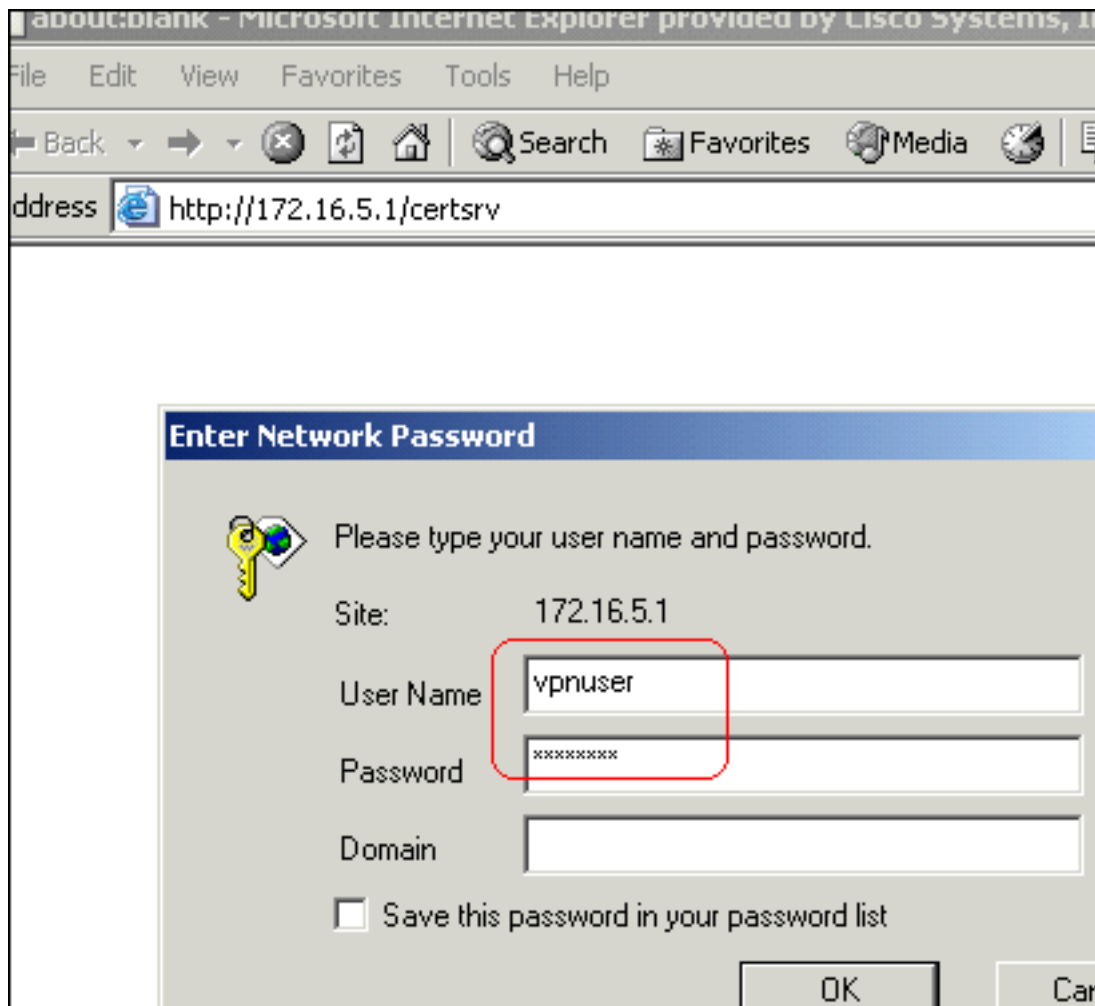
Configuration du client VPN

Terminez-vous ces étapes afin de configurer le client vpn :

1. Sélectionnez le **début > les programmes > le client vpn de Cisco Systems > le client vpn** afin de lancer le logiciel de client VPN.



2. Terminez-vous ces étapes afin de télécharger le certificat de CA du serveur CA nommé **CA1** et l'installer dans le Client VPN Cisco : Ouvrez une session au serveur 172.16.5.1 CA avec les credantial d'utilisateur fournis au



vpnuser.

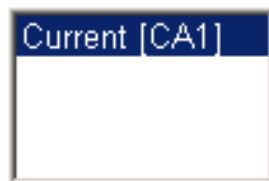
Remarque: Veuillez-vous pour faire expliquer à un utilisateur l'utilisateur de client vpn avec le serveur CA. Cliquez sur Download un **certificat de CA**, une **chaîne de certificat** ou un **CRL**, et puis sélectionnez la case d'option de la **base 64** afin de spécifier la méthode de codage. Cliquez sur le **certificat de CA de téléchargement**.

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA cert](#)

To download a CA certificate, certificate chain, or CRL, select the certificate

CA certificate:



Encoding method:

- DER
 Base 64

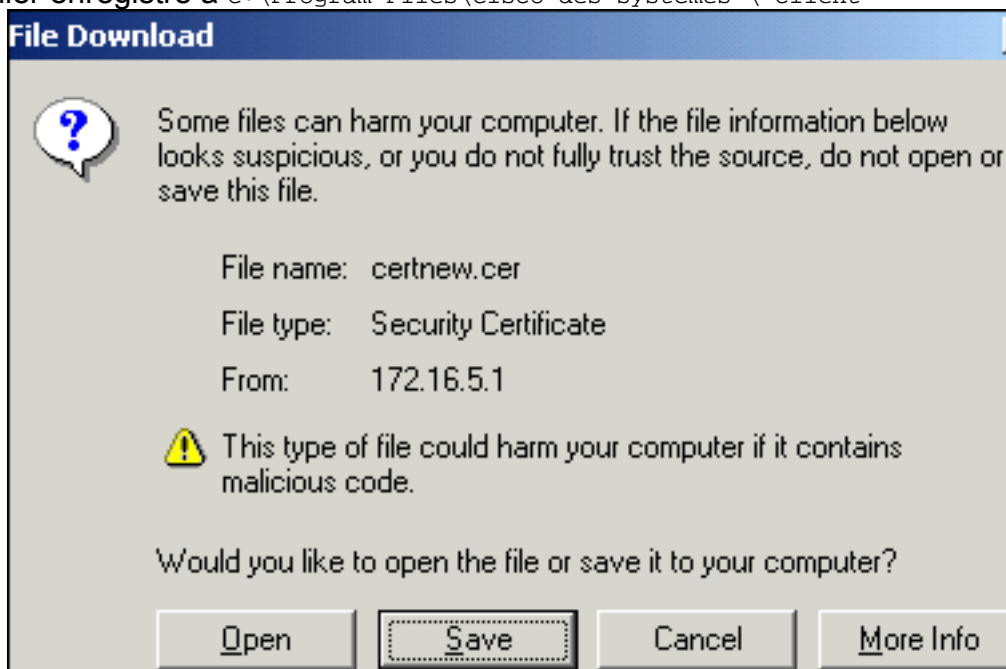
[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

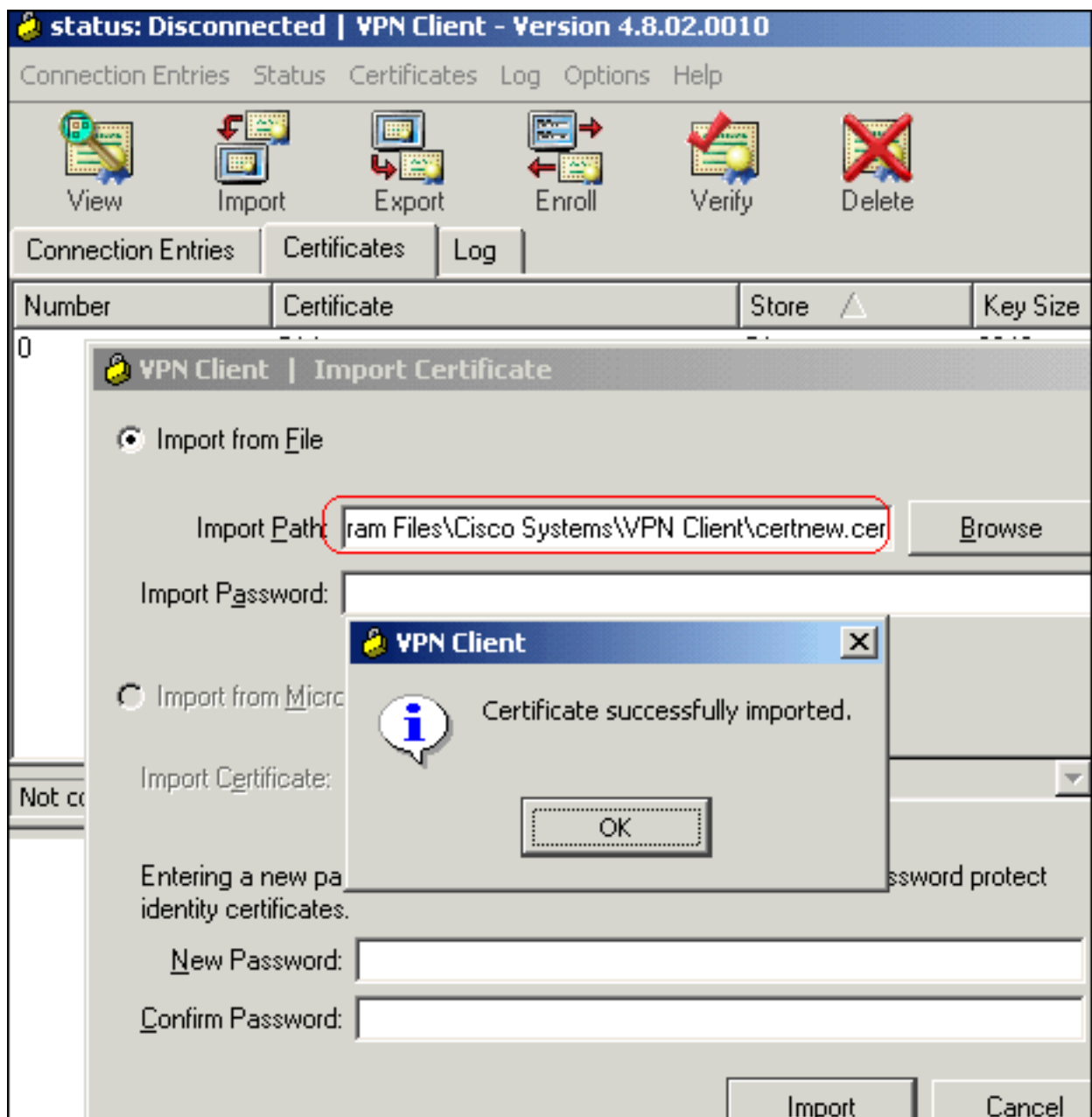
Sauvegardez le certificat de CA à votre ordinateur avec le nom **certnew.cer**. Par défaut, le fichier enregistre à C:\Program Files\Cisco des systèmes \ client



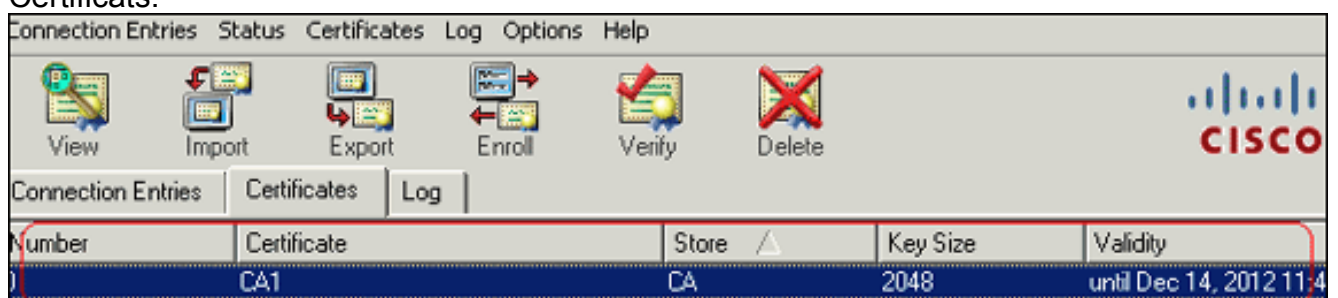
vpn.

Dans le client

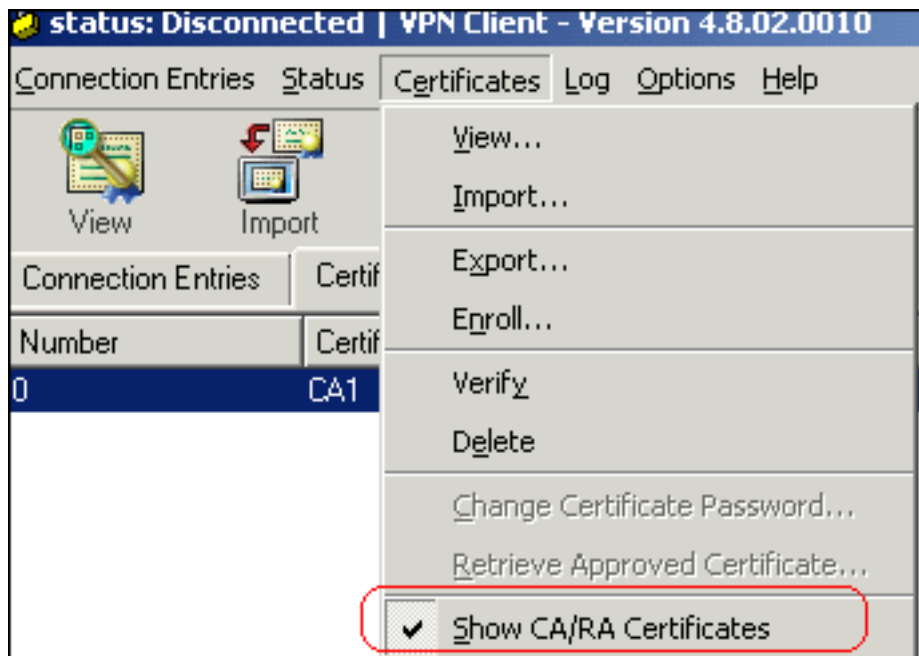
vpn, cliquez sur l'onglet de **Certificats**, et puis choisissez l'**importation**. Cliquez sur l'**importation en provenance de la** case d'option de **fichier**, et puis cliquez sur **parcourez** afin d'importer le certificat de CA des systèmes de C:\Program Files\Cisco d'emplacement de mémoire \ client vpn. Cliquez sur **Import**. Une boîte de dialogue est évident qu'énonce que le certificat a été avec succès importé.



Les Certificats CA CA1 apparaissent dans l'onglet de Certificats.



Remarque: Assurez-vous que l'option de **Certificats de l'exposition CA/RA** est sélectionnée ; autrement, les Certificats CA n'apparaîtront pas dans la fenêtre de



certificat.

3. Terminez-vous ces étapes afin de télécharger le certificat d'identité et l'installer dans le client vpn : Dans le serveur d'autorité de certification CA1, choisissez **Demander un certificat > demande de certificat avancée > Créer et soumettre une demande de requête auprès de cette Autorité de certification** afin de s'inscrire pour le certificat d'identité. Cliquez sur **Submit**.

Certificate Template:

User ▼

Key Options:

Create new key set Use existing key set

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

Key Usage: Exchange

Key Size: 1024 Min: 384 Max: 16384 (common key sizes: [512](#) [1024](#) [2048](#) [4096](#) [8192](#) [16384](#))

Automatic key container name User specified key container name

Mark keys as exportable

Export keys to file

Enable strong private key protection

Store certificate in the local computer certificate store

Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an administrator to generate or use a key in the local machine store.

Additional Options:

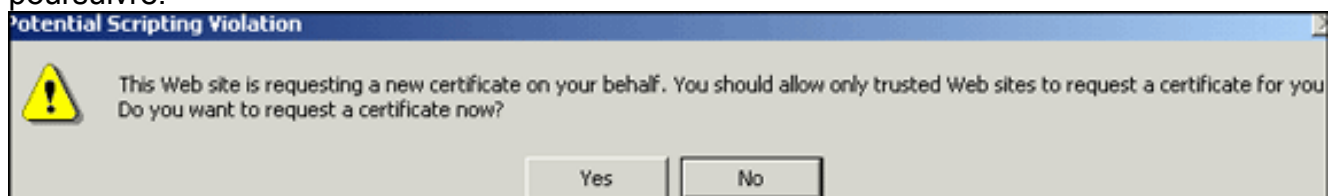
Request Format: CMC PKCS10

Hash Algorithm: MD5 ▼

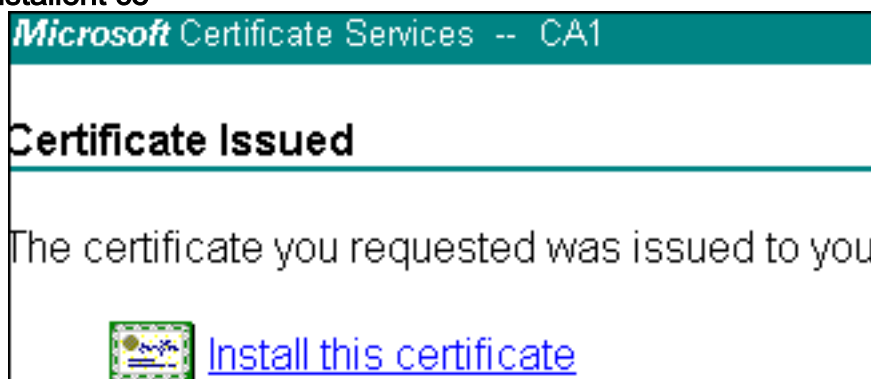
Only used to sign request.

Save request to a file

Cliquez sur **oui** pour poursuivre.



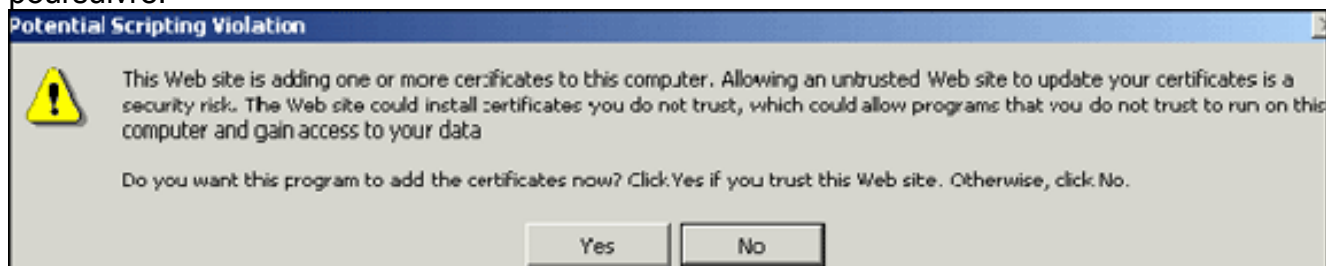
Le clic installent ce



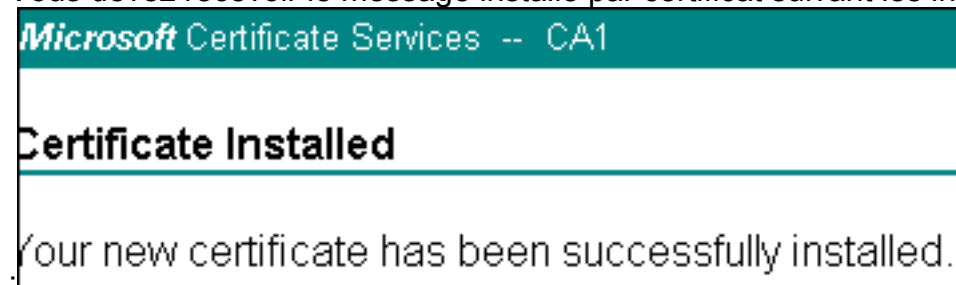
certificat.

Cliquez sur **oui** pour

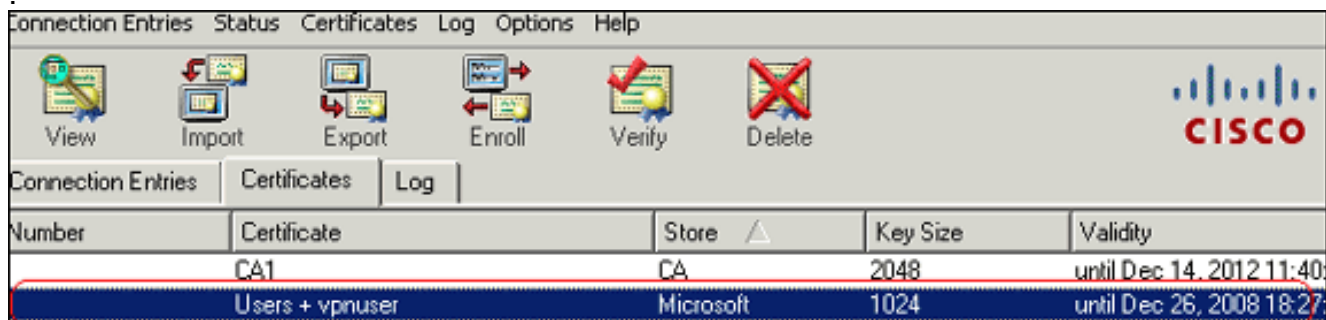
poursuivre.



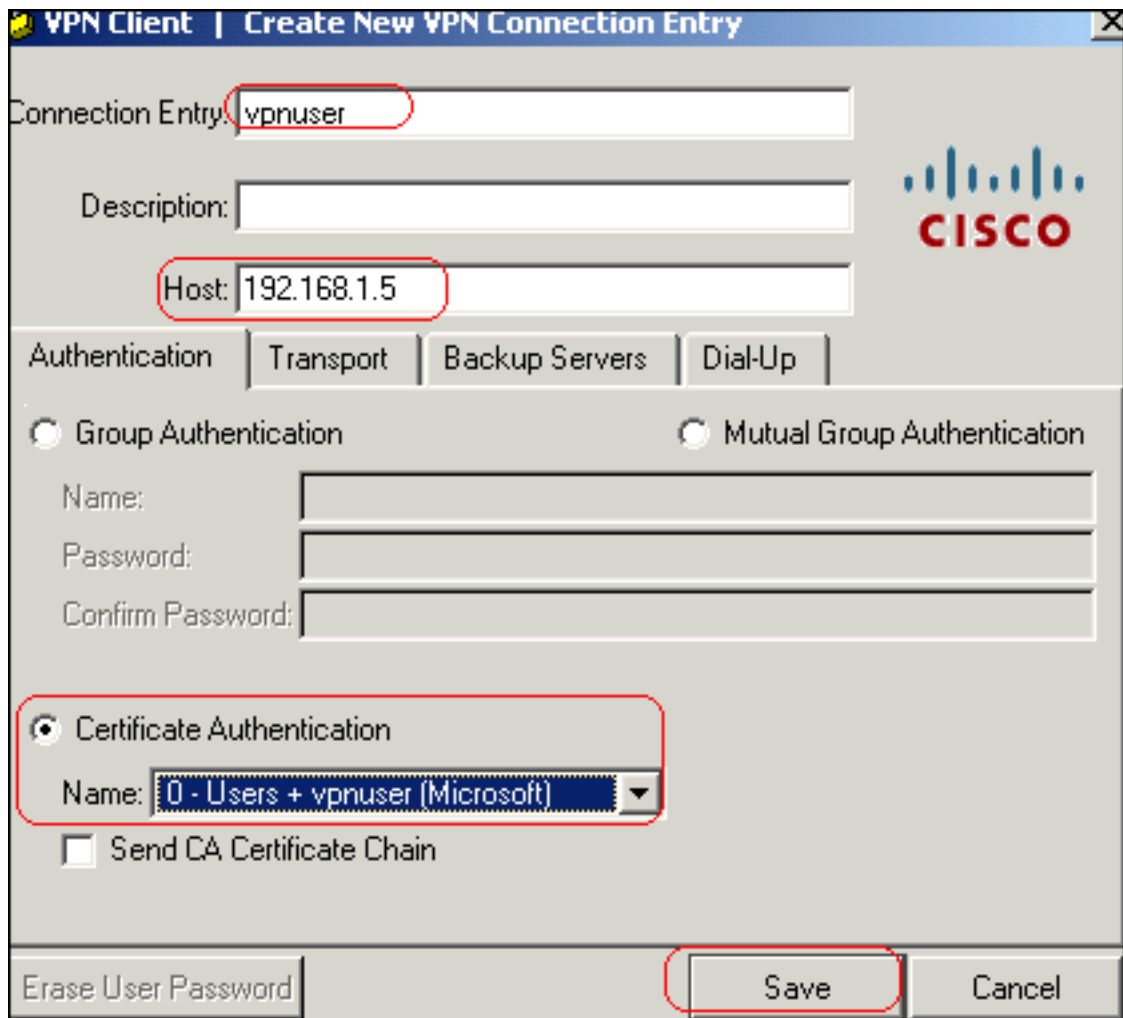
Vous devez recevoir le message installé par certificat suivant les indications de cette image



Quittez et puis relancez le client vpn afin de permettre au certificat d'identité installé pour apparaître dans l'onglet de Certificats du client vpn suivant les indications de cette image

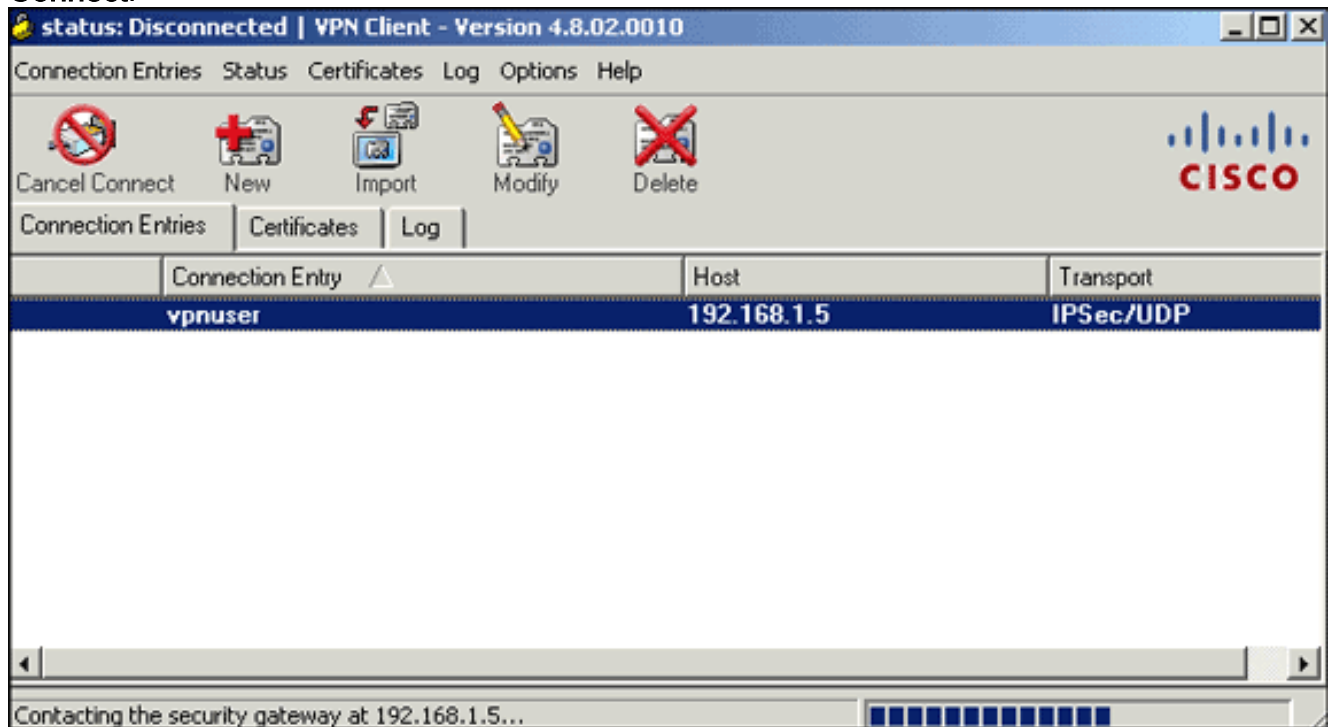


- Terminez-vous ces étapes afin de créer une entrée de connexion (*vpnuser*) : Cliquez sur l'onglet d'entrées de connexion, et puis cliquez sur New. Entrez l'adresse IP du partenaire distant (routable) dans le champ Host. Sélectionnez la case d'option d'**authentification de certificat**, et choisissez le certificat d'identité de la liste déroulante. Cliquez sur

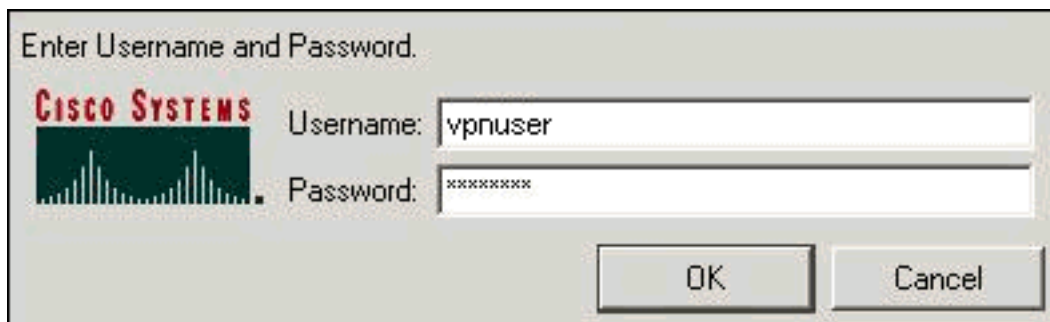


Save.

5. Cliquez sur Connect.



6. Une fois incité, écrivez les informations de nom d'utilisateur et de mot de passe pour le Xauth, et cliquez sur OK afin de se connecter au réseau



distant.

7. Le client vpn se connecte à l'ASA suivant les indications de cette image



Vérifiez

Sur l'ASA vous pouvez employer plusieurs commandes show à la ligne de commande afin de vérifier l'état d'un certificat.

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- **crypto ca trustpoint d'exposition** — Les affichages ont configuré des points de confiance. CiscoASA#`show crypto ca trustpoints` Trustpoint CA1: Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com Serial Number: 7099f1994764e09c4651da80a16b749c Certificate configured.
- **affichez le crypto certificat Ca** — Affiche tous les Certificats installés sur le système. 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: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.crl 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: [1] ldap:///CN=CA1,CN=TS-W2K3-ACS,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuratio n,DC=TSWeb,DC=cisco,DC=com?certificateRevocationList?base?objectClass= cRLDistributionPoint [2] http://ts-w2k3-ac.s.tsweb.cisco.com/CertEnroll/CA1.crl 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** — Les affichages ont caché les listes des révocations de certificat (CRL).
- **show crypto key mypubkey rsa** — Affiche toutes les cryptos paires de clés générées. 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** — Affiche l'IKE les 1 informations de tunnel. 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 1 IKE Peer: 10.1.1.5 Type : user Role : responder Rekey : no State : MM_ACTIVE
- **show crypto ipsec sa** — Dislays les informations de tunnel d'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

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

[Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Voici quelques erreurs possibles que vous pourriez rencontrer :

- **ERREUR : Failed to parse or verify imported certificate**Cette erreur peut se produire quand vous installez le certificat d'identité et que vous n'avez pas le certificat d'autorité de certification racine ou intermédiaire correct authentifié avec le point de confiance associé. Vous devez supprimer et réauthentifier avec le certificat d'autorité de certification racine ou intermédiaire correct. Contactez votre constructeur de tiers afin de vérifier que vous avez reçu le certificat de CA correct.
- **Certificate does not contain general purpose public key**Cette erreur peut se produire quand vous essayez d'installer votre certificat d'identité sur le point de confiance incorrect. Vous essayez d'installer un certificat d'identité non valide ou la paire de clés associée au point de confiance ne correspond pas à la clé publique contenue dans le certificat d'identité. Employez la commande de **trustpointname de show crypto ca certificat** afin de vous vérifier a installé votre certificat d'identité sur le point de confiance correct. Recherchez la ligne énonçant des **points de confiance associés**. si le point de confiance incorrect est répertorié, utilisez les procédures décrites dans ce document afin de supprimer et de réinstaller le point de confiance approprié. Vérifiez également que la paire de clés n'a pas changé depuis que la CSR a été générée.
- **ERREUR : ASA/PIX. Sev=Warning/3 IKE/0xE300081 Invalid remote certificate id:**Vous pourriez recevoir cette erreur dans le client vpn si un problème se pose avec les Certificats pendant l'authentification. Afin de résoudre ce problème, utilisez la **commande auto de crypto isakmp identity** dans la configuration ASA/PIX.

[Informations connexes](#)

- [Page d'assistance pour Serveur de sécurité adaptatif Cisco](#)
- [Cisco VPN Client Support Page](#)
- [Dispositifs de sécurité de la gamme Cisco PIX 500](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Notices de champs relatives aux produits de sécurité \(y compris PIX\)](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)