ASA/PIX 8.x e autenticação IPSec do cliente VPN usando Certificados digitais com exemplo de configuração de Microsoft CA

Índice

Introdução

Este documento descreve como instalar manualmente um certificado digital do fornecedor de terceira parte no dispositivo do Cisco Security (ASA/PIX) 8.x assim como em clientes VPN a fim autenticar os ipsec peer com o server de Microsoft Certificate Authority (CA).

Pré-requisitos

Requisitos

Este documento exige que você tem o acesso a um Certificate Authority para o certificado de registro. Terceira parte que apoiada vendedores de CA é Baltimore, Cisco, confiam, iPlanet/Netscape, Microsoft, RSA, e Verisign.

Este documento supõe que não há nenhuma configuração de VPN PRE-existente no ASA/PIX.

Nota: Este documento usa um server de Microsoft Windows 2003 como o server de CA para a encenação.

Nota: Refira configurar CA no Windows Server para obter informações completas sobre de como configurar um server de Windows 2003 como CA.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5510 que executa a versão de software 8.0(2) e a versão 6.0(2) ASDM
- Cliente VPN que executa a versão de software 4.x e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

A configuração ASA pode igualmente ser usada com o Cisco 500 Series PIX que executa a versão de software 8.x.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

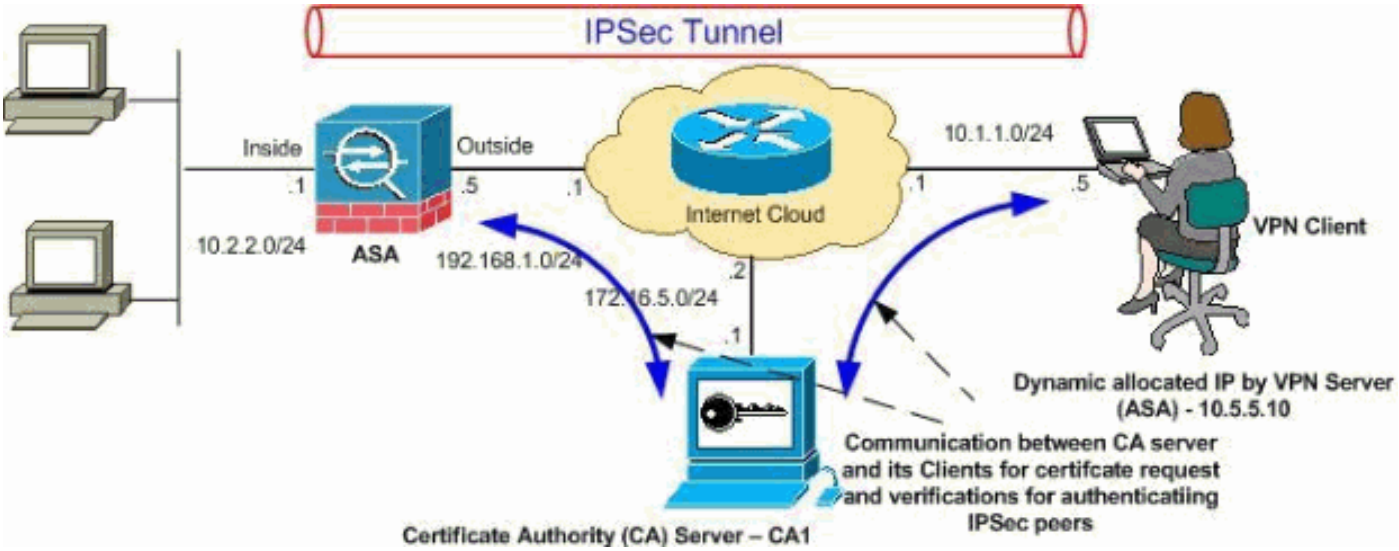
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

- Configuração ASA
- Sumário de configuração ASA
- Configuração de cliente de VPN

Configuração ASA

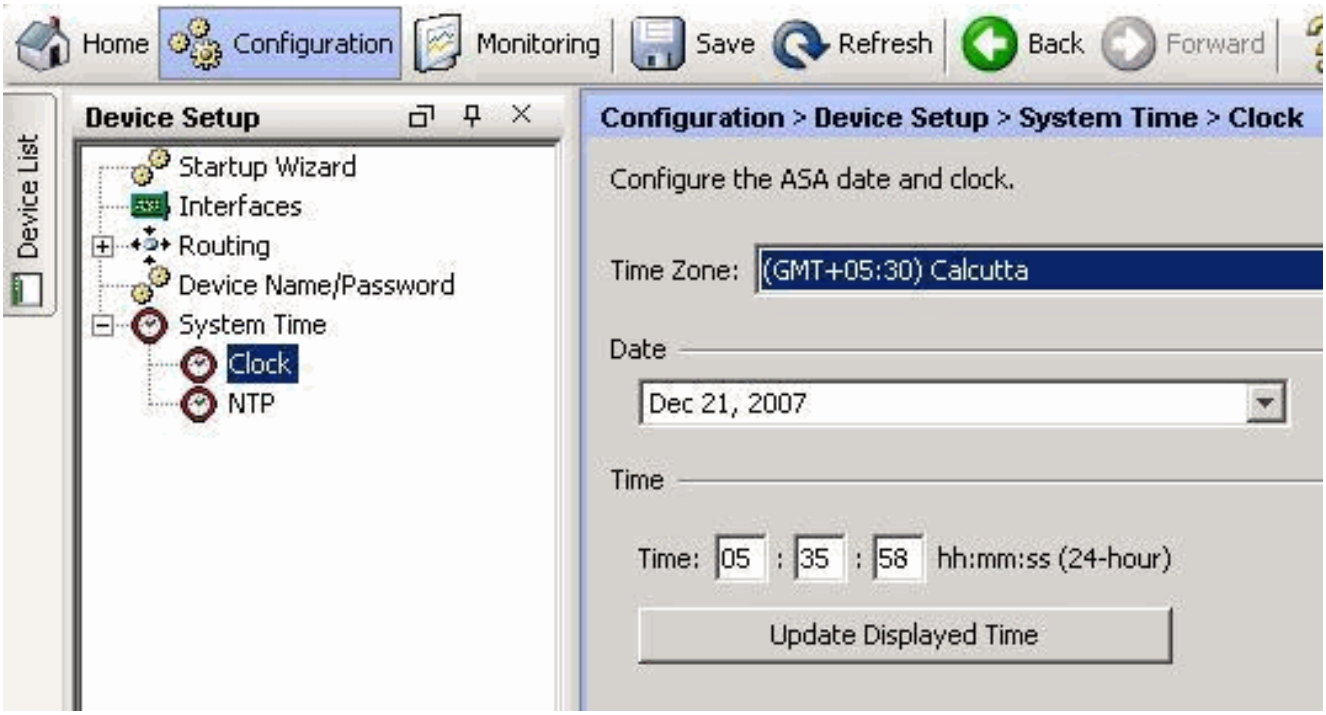
A fim instalar um certificado digital do fornecedor de terceira parte no ASA, termine estas etapas:

- Etapa 1. Verifique que a data, o tempo, e os valores da zona de hora (fuso horário) são exatos
- Etapa 2. Gerencia uma solicitação de assinatura de certificado
- Etapa 3. Autentique o ponto confiável
- Etapa 4. Instale o certificado
- Etapa 5. Configurar o acesso remoto VPN (IPsec) para usar o certificado recentemente instalado

Etapa 1. Verifique que a data, o tempo, e os valores da zona de hora (fuso horário) são exatos

Procedimento ASDM

1. Clique a **configuração**, e clique então a **instalação de dispositivo**.
2. Expanda o **tempo de sistema**, e escolha o **pulso de disparo**.
3. Verifique que a informação alistada é exata.Os valores para a data, o tempo, e a zona de hora (fuso horário) devem ser exatos para que a validação certificada apropriada ocorra.



Exemplo da linha de comando

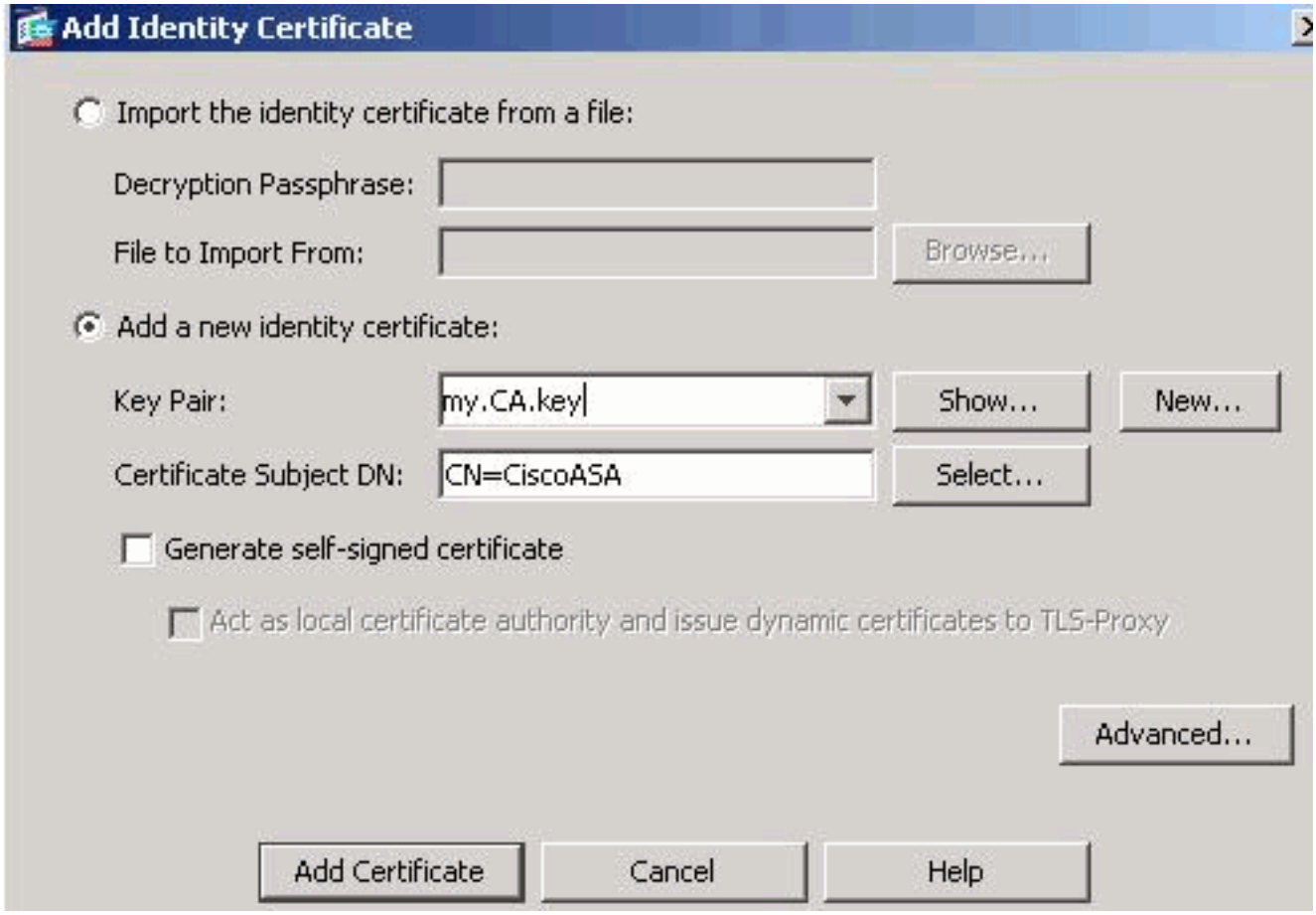
CiscoASA
`CiscoASA#show clock` `05:37:37.904 UTC Fri Dec 21 2007`

Etapa 2. Gerencia uma solicitação de assinatura de certificado

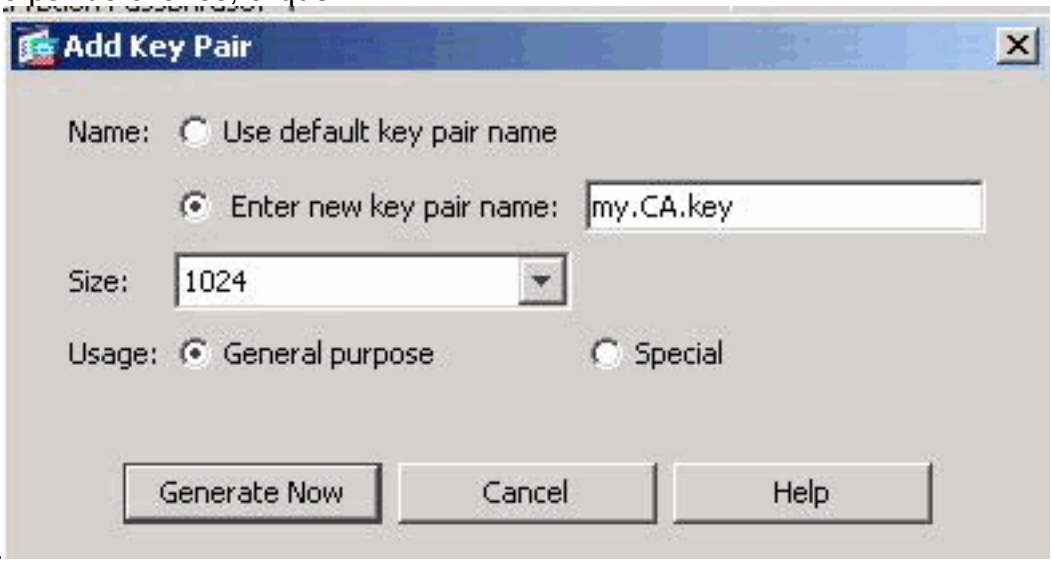
Uma solicitação de assinatura de certificado (CSR) é exigida para que a terceira parte CA para emitir um certificado de identidade. O CSR contém a corda do nome destacado (DN) do seu ASA junto com a chave pública gerada do ASA. O ASA usa a chave privada gerada para assinar digitalmente o CSR.

Procedimento ASDM

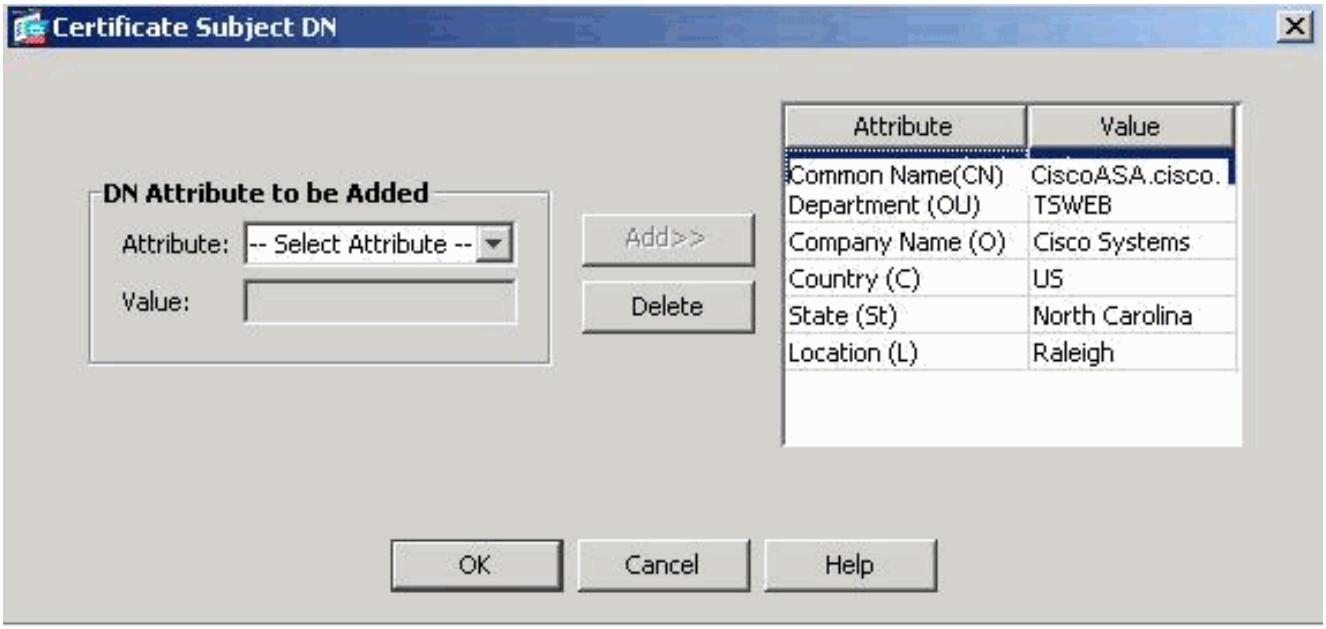
1. **A configuração do** clique, e clica então o **Gerenciamento de dispositivos**.
2. Expanda o **gerenciamento certificado**, e escolha **certificados de identidade**.
3. Clique em
   Add.



4. Clique **adicionar um** botão de rádio **novo do certificado de identidade**.
5. Para o par de chaves, clique **novo**.

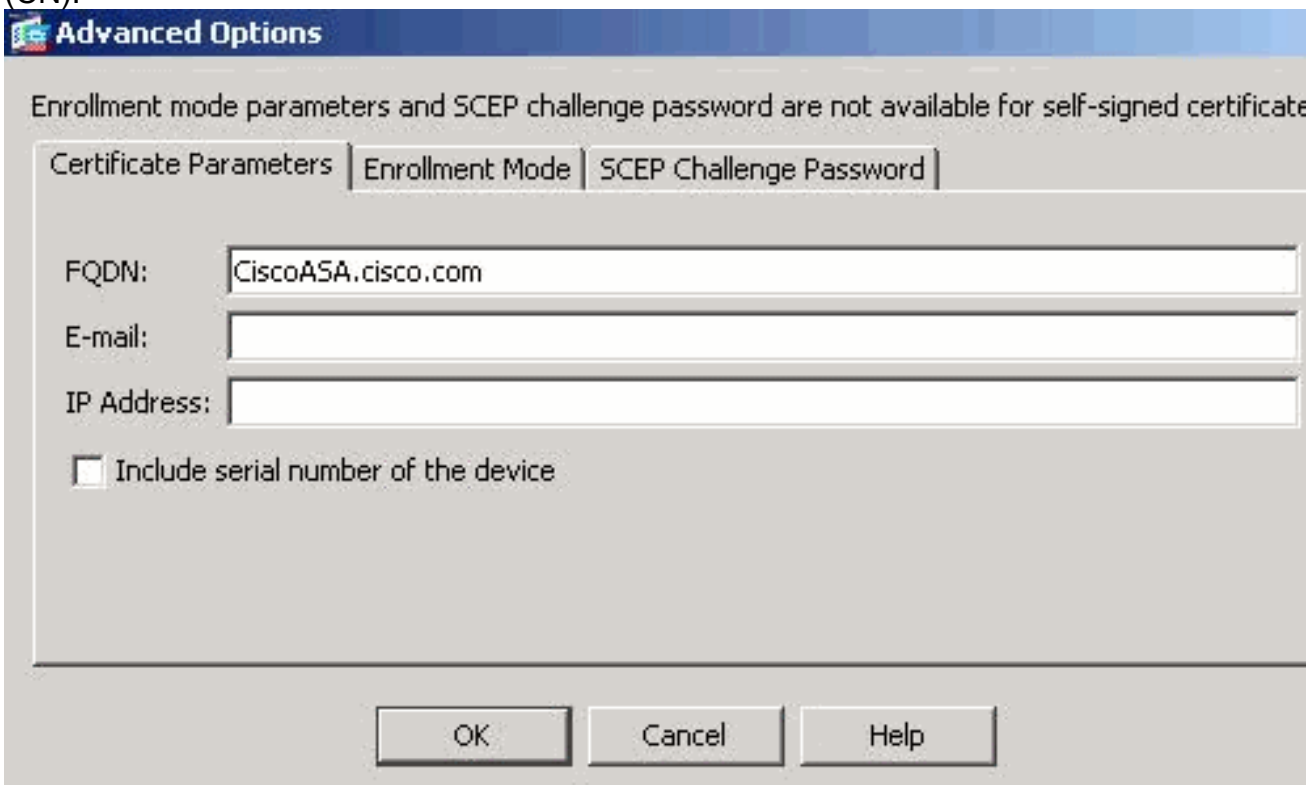


6. Clique o botão de rádio **novo do nome do par de chaves da entrada**. Você deve distintamente identificar o nome do par de chaves para finalidades do reconhecimento.
7. O clique **gerencie agora**.O par de chaves deve agora ser criado.
8. A fim definir o assunto DN do certificado, o clique **seleto**, e configurar os atributos alistados nesta tabela:A fim configurar estes valores, para escolher um valor da lista de drop-down do atributo, para incorporar o valor, e o clique **adicionar**.

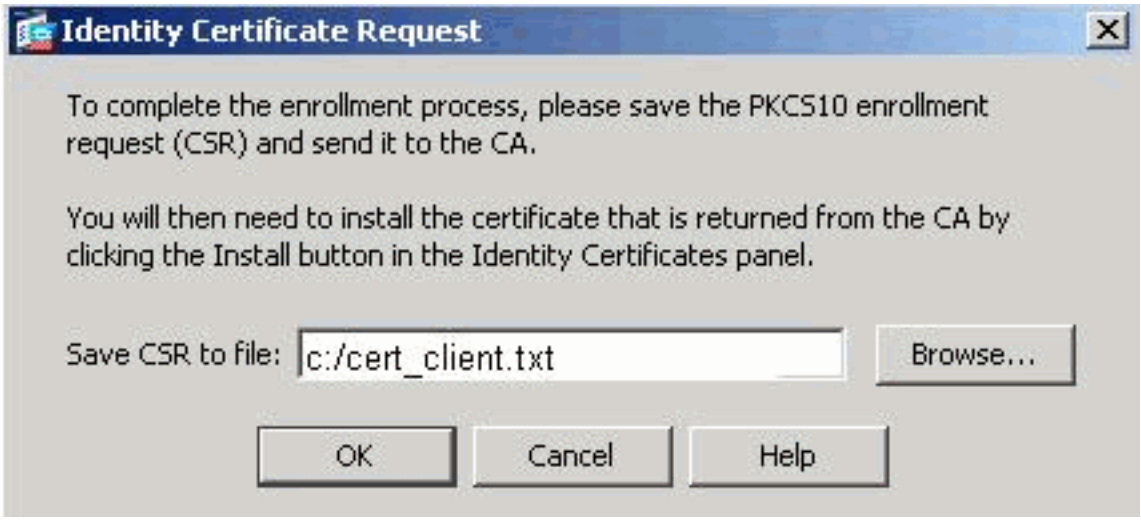


Nota: Alguns fornecedores de terceira parte exigem atributos particulares ser incluídos antes que um certificado de identidade esteja emitido. Se você é incerto dos atributos requerido, verifique com seu vendedor para ver se há detalhes.

9. Uma vez que os valores apropriados são adicionados, clique a **APROVAÇÃO**.A caixa de diálogo do certificado de identidade adicionar aparece com o campo do assunto DN do certificado povoado.
10. Clique **avançado**.
11. No campo FQDN, incorpore o FQDN a ser usado para alcançar o dispositivo do Internet.Este valor deve ser o mesmo FQDN que você se usou para o Common Name (CN).

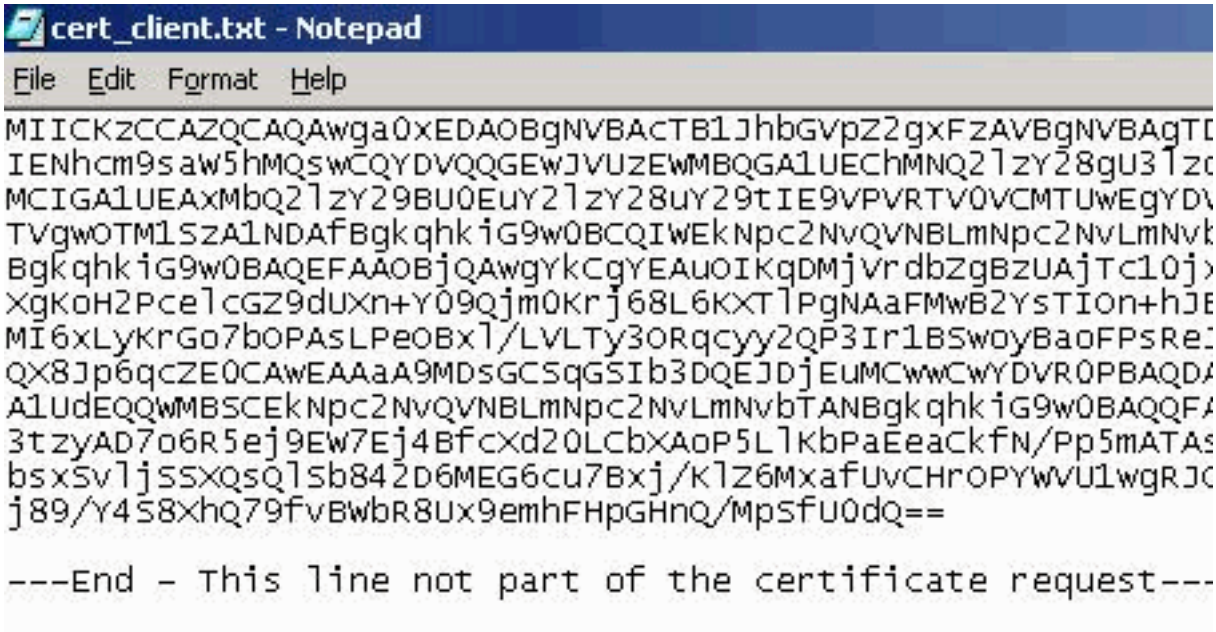


12. Clique a **APROVAÇÃO**, e clique-a então **adicionam o certificado**.Você é alertado salvar o CSR a um arquivo em sua máquina

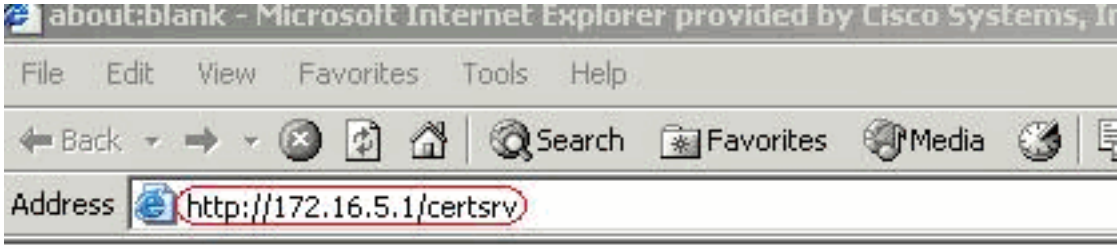


local.

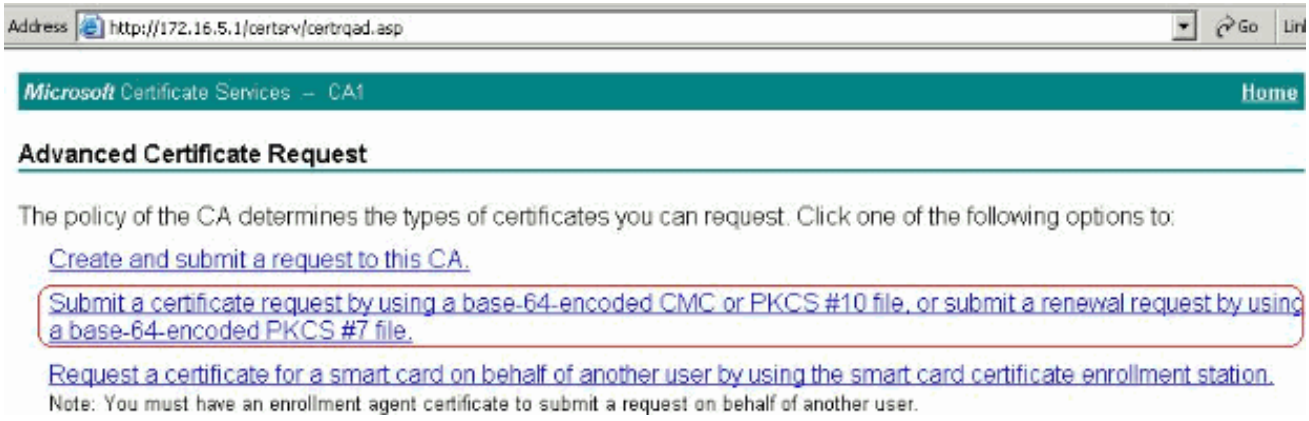
13. Clique **consultam**, escolhem um lugar em que para salvar o CSR, e para salvar o arquivo com a extensão de .txt.**Nota:** Quando você salvar o arquivo com uma extensão de .txt, você pode abrir o arquivo com um editor de texto (tal como o bloco de notas) e ver o pedido PKCS#10.



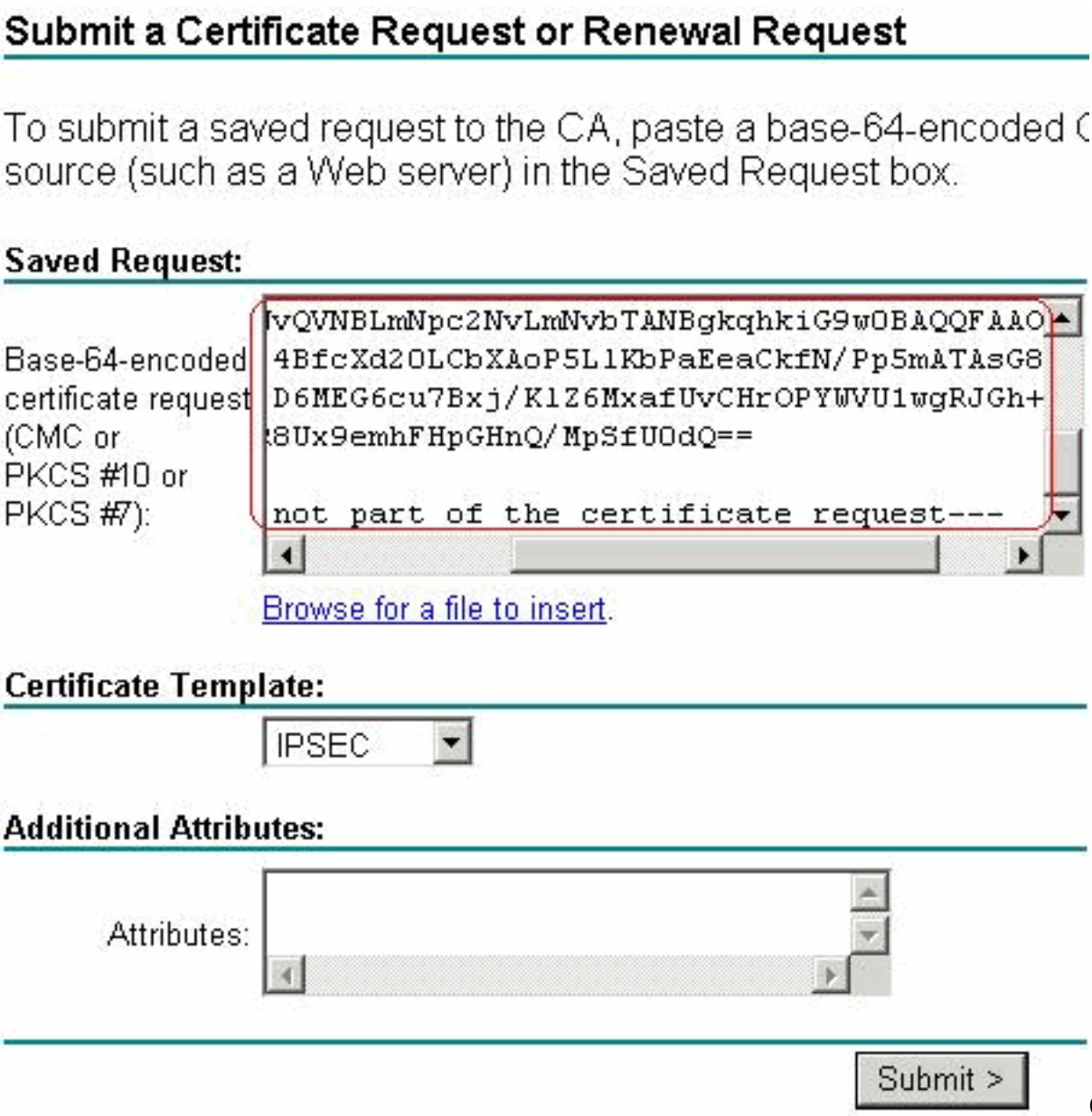
14. Submeta o CSR salvar a seu fornecedor de terceira parte tal como Microsoft CA, como mostrado.Execute o início de uma sessão da Web no server 172.16.5.1 de CA com a ajuda das credenciais do usuário fornecidas para o



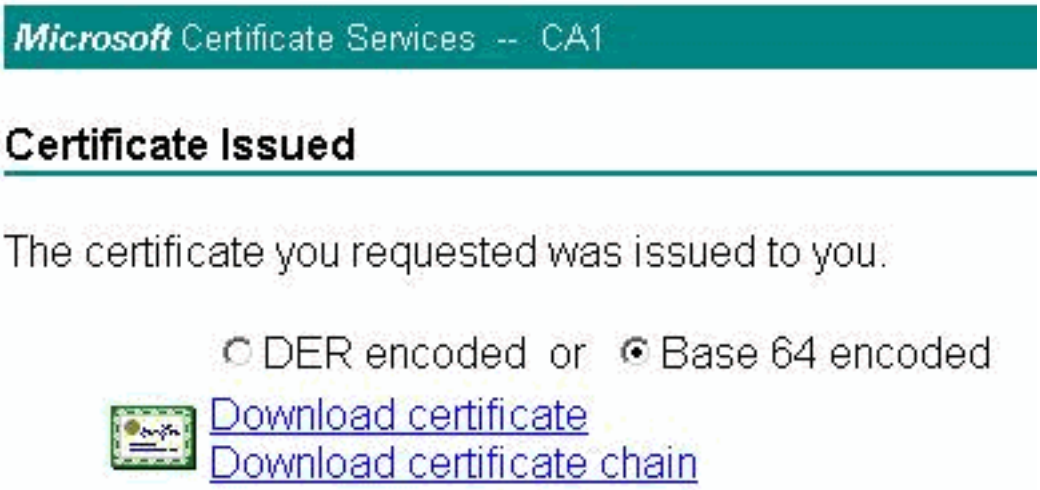
vpnserver. **N**
ota: Certifique-se de que você manda um usuário esclarecer o ASA (server do vpn) com o server de CA.Clique o **pedido um certificado > avançou o pedido do certificado** a fim selecionar **submetem um pedido do certificado usando um arquivo CMC ou PKCS#10 base-64-encoded ou submetem uma requisição de renovação usando um arquivo base-64-encoded**
PKCS#7.



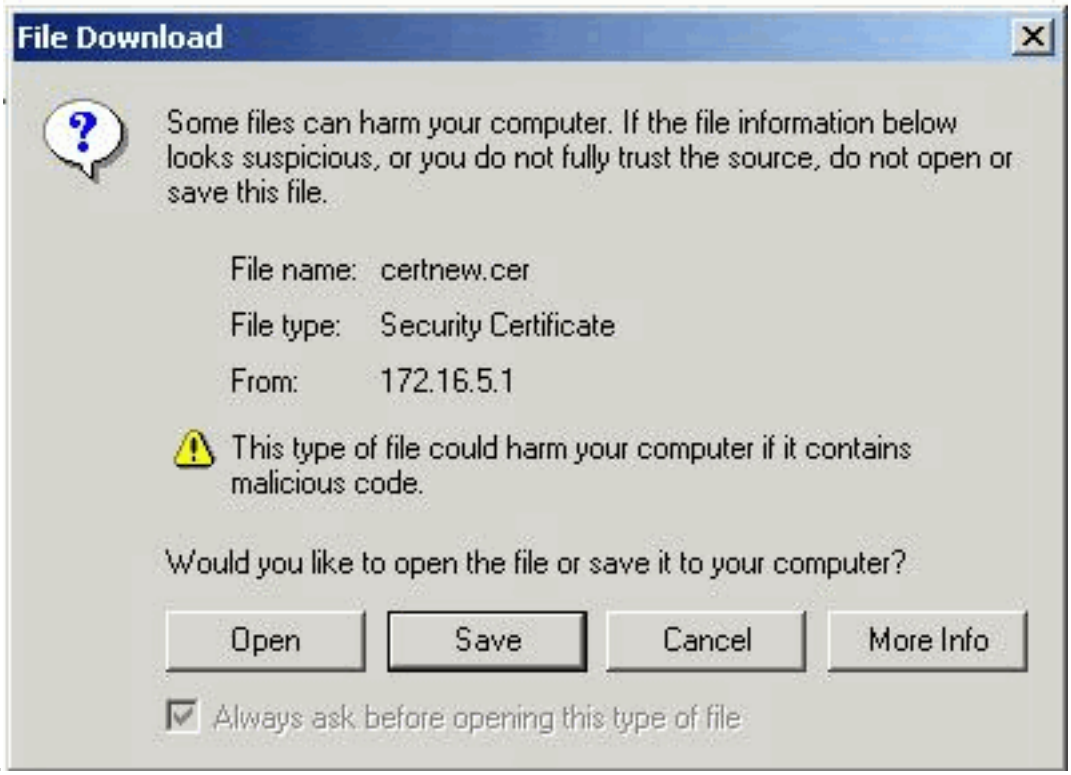
A cópia e cola a informação codificada na caixa da **solicitação salva**, e clica-a então **submete-**



se. Cli que o botão de rádio **codificado Base64**, e clique o **certificado da**



transferência. O indicador da transferência do arquivo aparece. Salvar o com o nome de **cert_client_id.cer**, que é o certificado de identidade a ser instalado no



ASA.

Exemplo da linha de comando

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)#**crypto ca trustpoint CA1** ciscoasa(config-ca-trustpoint)# subject-name CN=CiscoASA.cisco.com,OU=TSWEB, O=Cisco Systems,C=US,St=North Carolina,L=Raleigh *!--- Defines x.500 distinguished name. Use the attributes defined in table as a guide.* CiscoASA(config-ca-trustpoint)#**keypair my.CA.key** *!--- Specifies key pair generated in Step 3* CiscoASA(config-ca-trustpoint)#**fqdn CiscoASA.cisco.com** *!--- Specifies the FQDN (DNS:) to be used as the subject alternative name* CiscoASA(config-ca-trustpoint)#**enrollment terminal** *!--- Specifies manual enrollment.* CiscoASA(config-ca-trustpoint)#**exit** CiscoASA(config)#**crypto ca enroll CA1** *!--- Initiates certificate signing request. This is the request to be !--- submitted via Web or Email to the third 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]: **y** *!--- 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 third party CA.* Certificate Request follows: MIICKzCCAZQCAQAwga0xEDAOBgNVBAcTB1JhbGVpZ2gxFzAVBgNVBAgTDk5vcnRo

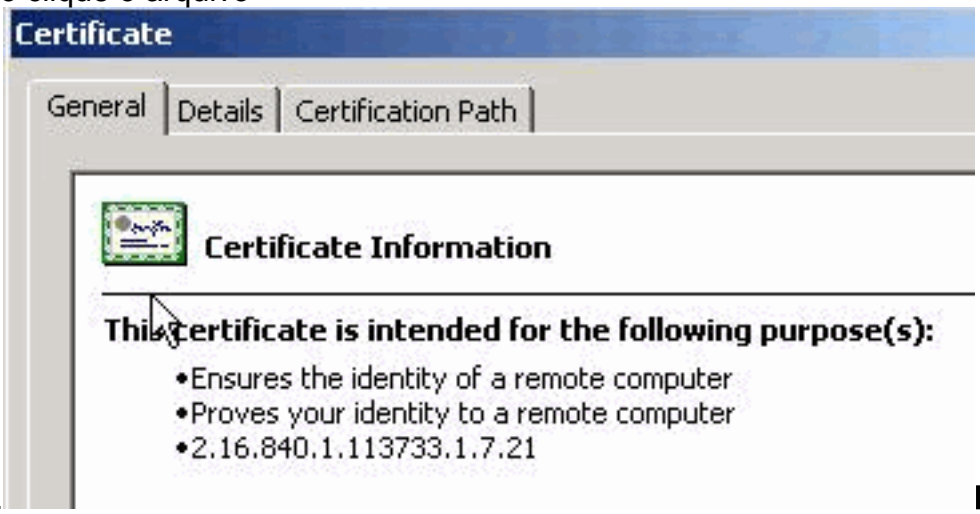
```
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lz
dGVtczEk
MCIGA1UEAxMbQ2lzY29BU0EuY2lzY28uY29tIE9VPVRTV0VCMTUwEgYD
VQQFEwtK
TVgwOTM1SzA1NDAfBgkqhkiG9w0BCQIWEkNpc2NvQVNBLmNpc2NvLmNv
bTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAuOIKqDMjVrdbZgBzUAjTc10j
xSlbkkcr
XgKoH2PcelcGZ9dUXn+Y09Qjm0Krj68L6KXTlPgNAaFMwB2YsTIOn+hJ
BVq5Sxjv
MI6xLyKrGo7bOPAsLPeOBxl/LVLTy3ORqcyy2QP3Ir1BSwoyBaoFPsRe
JGSAYG+O
QX8Jp6qcZE0CAwEAAaA9MDsGCSqGSIb3DQEJDjEuMCwwCwYDVR0PBAQD
AgWgMB0G
A1UdEQQWMBSCEkNpc2NvQVNBLmNpc2NvLmNvbTANBgkqhkiG9w0BAQQF
AAOBgQBM
3tzyAD7o6R5ej9EW7Ej4BfcXd20LCbXAoP5LlKbPaEeaCkfN/Pp5mATA
sG832TBm
bsxSvljSSXQsQlSb842D6MEG6cu7Bxj/KlZ6MxafUvCHrOPYWVU1wgRJ
Gh+ndCZK j89/Y4S8XhQ79fvBWbR8Ux9emhFHpGHnQ/MpSfU0dQ== --
-End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]: n
CiscoASA(config)#
```

Etapa 3. Autentique o ponto confiável

Uma vez que você recebe o certificado de identidade do fornecedor de terceira parte, você pode continuar com esta etapa.

Procedimento ASDM

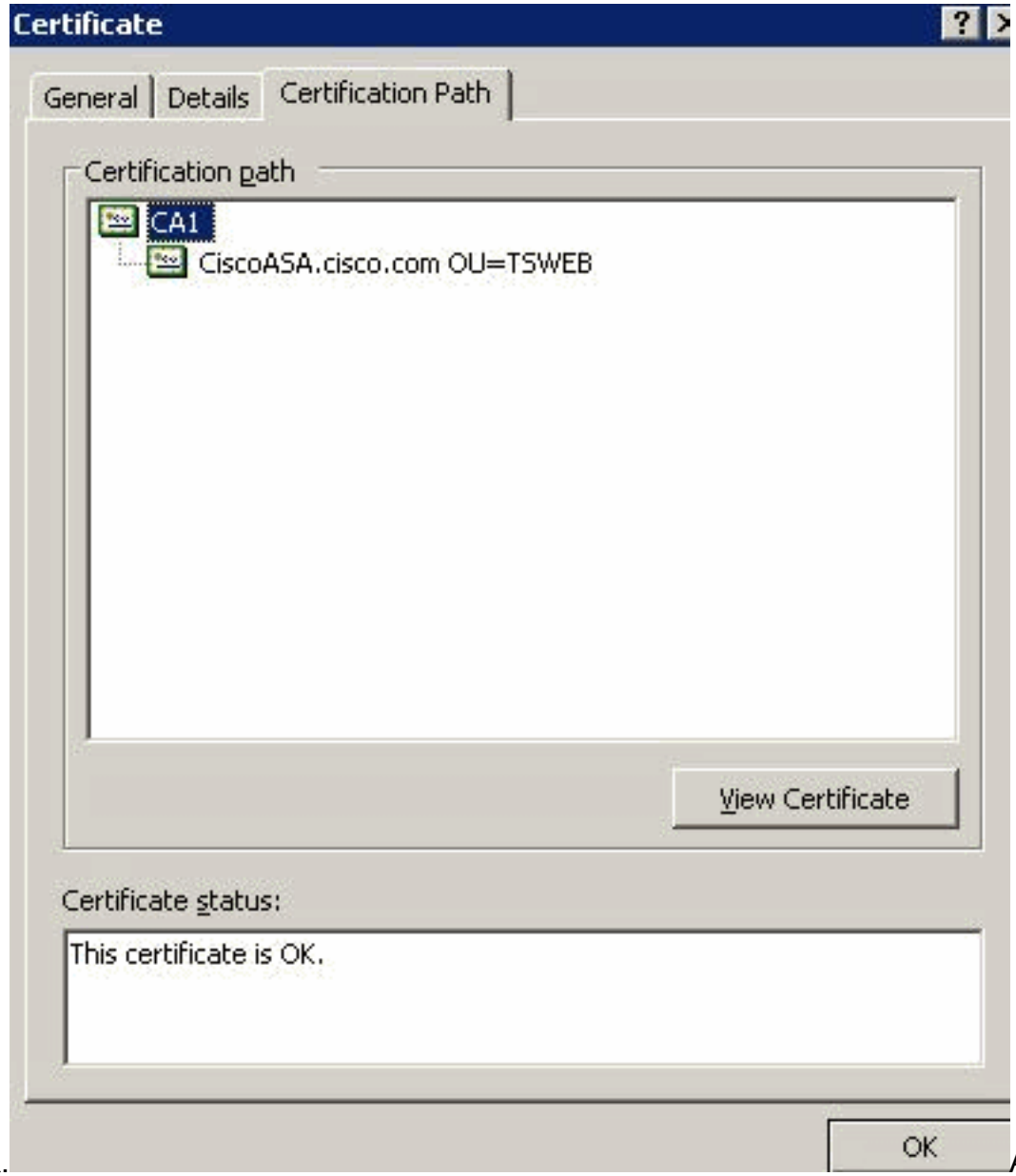
1. Salvar o certificado de identidade a seu computador local.
2. Se seu foram fornecidos um certificado base64-encoded que não venha como um arquivo, você deve copiar a mensagem base64 e colá-la em um arquivo de texto.
3. Rebatize o arquivo com uma extensão de .cer**Nota:** O arquivo é rebatizado uma vez com a extensão de .cer, os indicadores do ícone do arquivo como um certificado, como mostrado. 

4. Fazer duplo clique o arquivo certificado. 

Nota: Se `Windows não tem bastante informação a verificar que esta` mensagem do `certificado` aparece

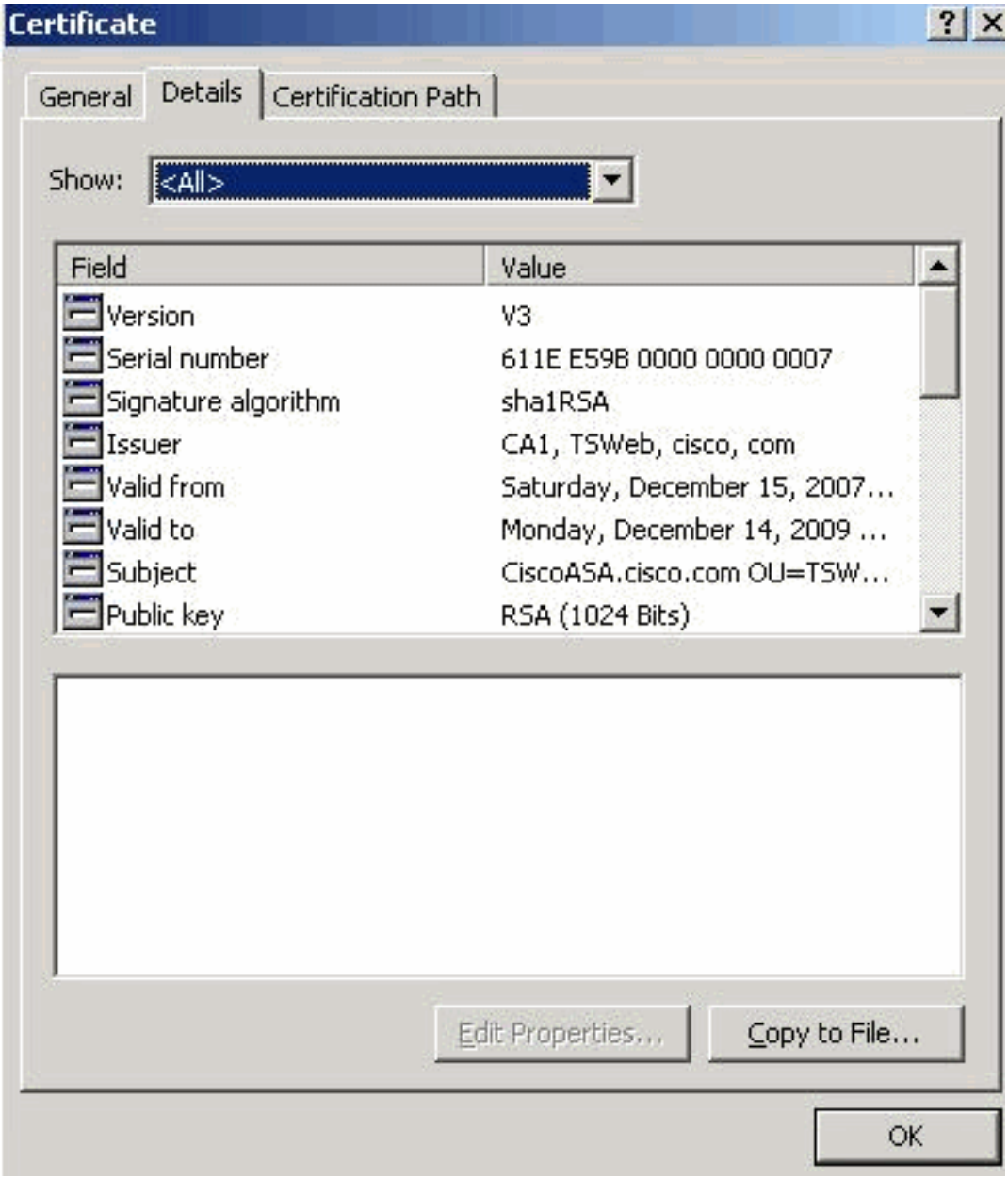
no tab geral, você deve obter a CA raiz do fornecedor de terceira parte ou o certificado de CA intermediário antes que você continue com este procedimento. Contacte seu fornecedor de terceira parte ou administrador de CA a fim obter a CA raiz de emissão ou o certificado de CA intermediário.

5. Clique a aba do **trajeto do certificado**.
6. Clique o certificado de CA associado com seu certificado de identidade emitido, e clique o **certificado da**



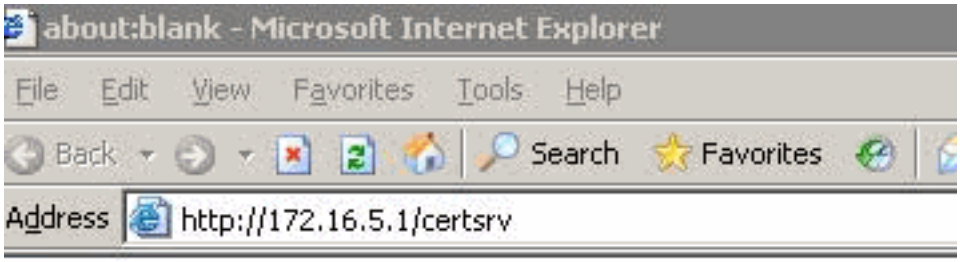
vista. A informação detalhada sobre o certificado de CA aparece.

7. Clique **detalhes** a fim conhecer mais informação sobre o certificado de



identidade.

8. Antes que você instale o certificado de identidade, o certificado de CA deve ser transferido do server de CA e ser instalado no ASA, como mostrado.Termine estas etapas a fim transferir o certificado de CA do server de CA nomeado **CA1**.Execute o início de uma sessão da Web no server 172.16.5.1 de CA com a ajuda das credenciais fornecidas ao servidor de

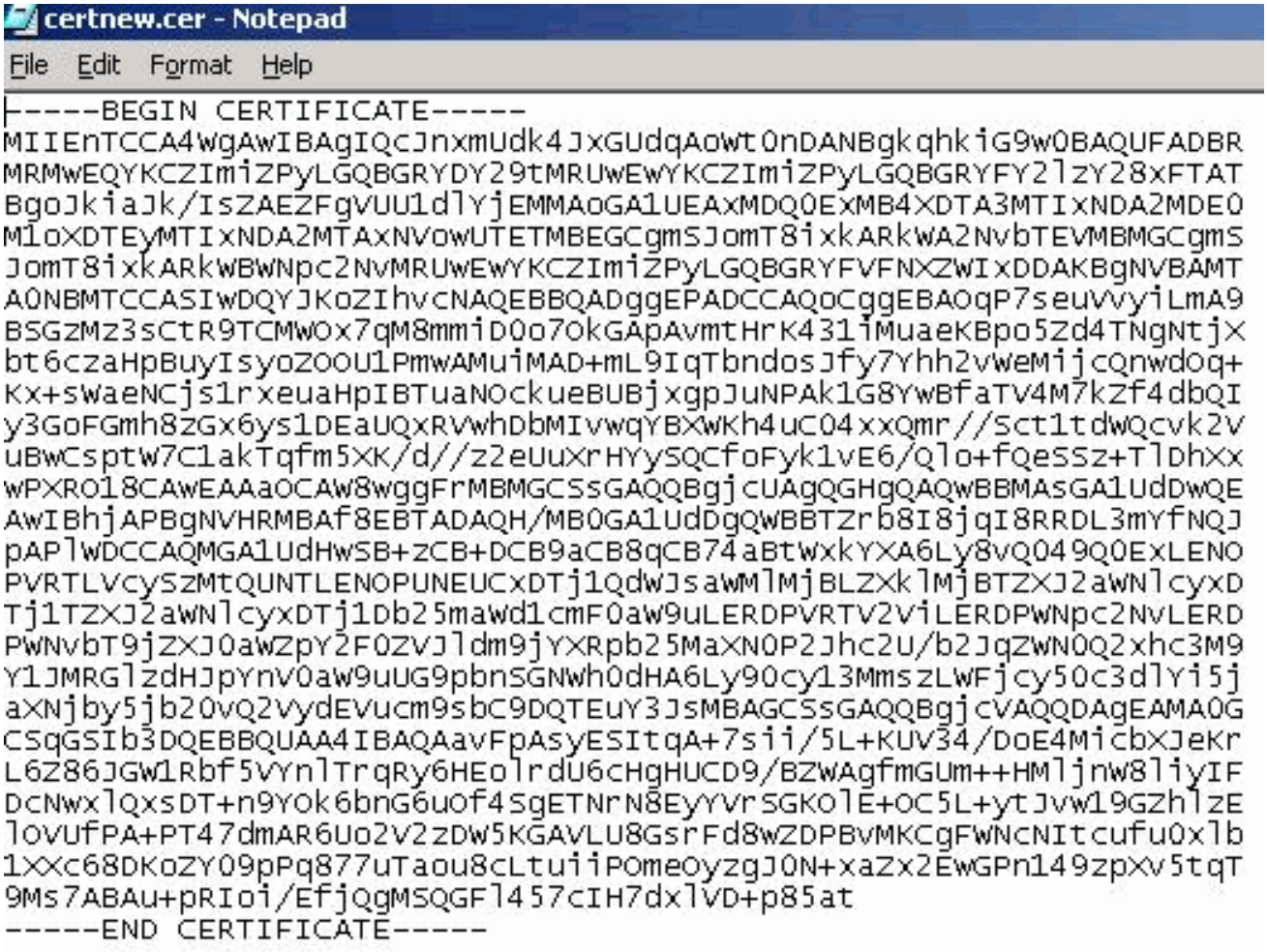


VPN. Clique a **transferência um certificado de CA, um certificate chain ou um CRL** a fim abrir o indicador, como mostrado. Clique o botão de rádio de **Base64** como o método de codificação, e clique o **certificado de CA da transferência**.

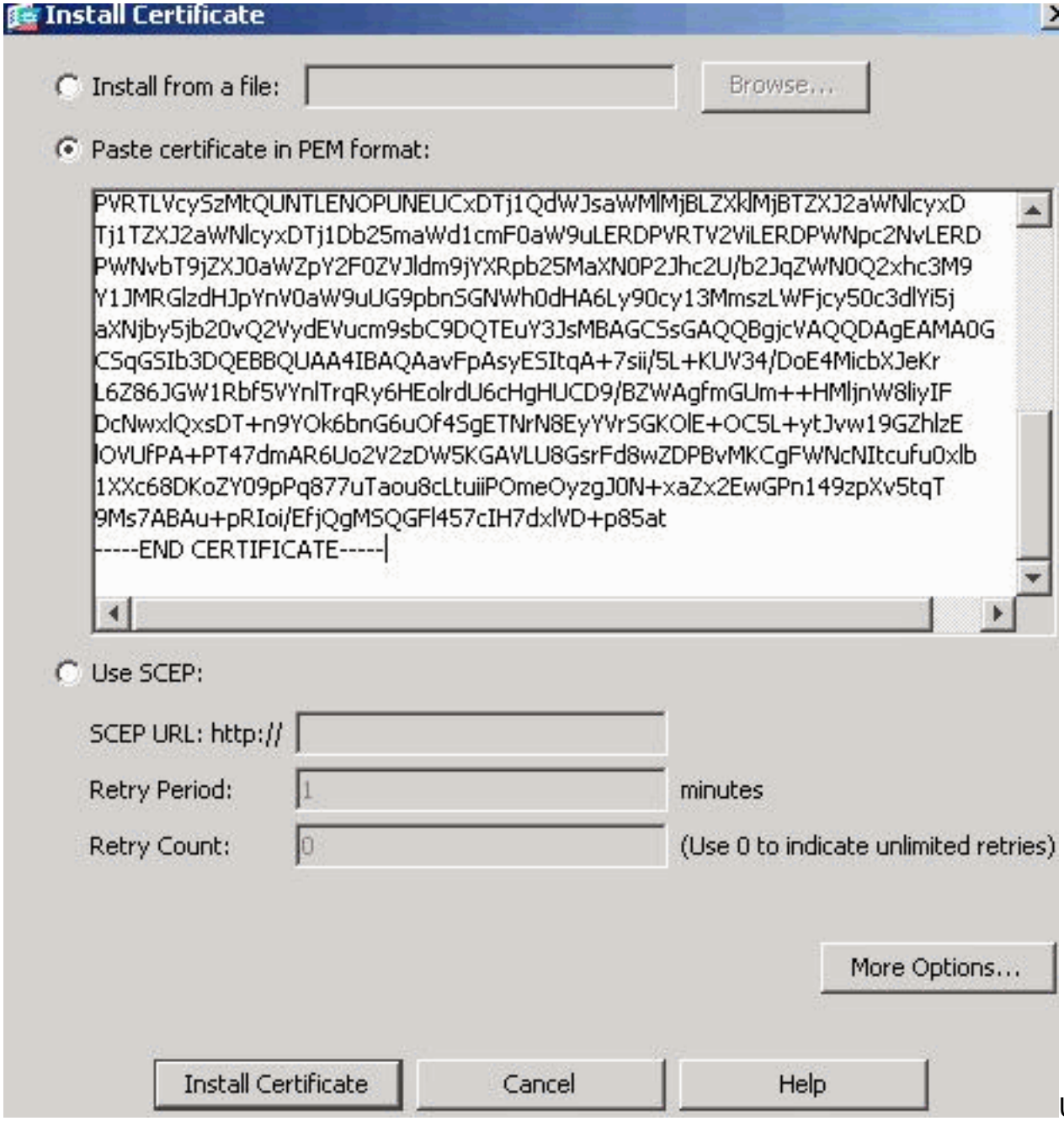
Salvar o certificado de CA com o nome de **certnew.cer em** seu

computador.

9. Consulte ao lugar onde você salvar o certificado de CA.
10. Abra o arquivo com um editor de texto, tal como o bloco de notas. Clicar com o botão direito o arquivo, e escolha-o **enviam a > bloco de notas**.
11. A mensagem base64-encoded similar ao certificado nesta imagem aparece:



12. Dentro do ASDM, a **configuração do** clique, e clica então o **Gerenciamento de dispositivos**.
13. Expanda o **gerenciamento certificado**, e escolha **certificados de CA**.
14. Clique em Add.
15. Clique o **certificado da pasta no** botão de rádio do **formato PEM**, e cole o certificado de CA base64 fornecido pelo fornecedor de terceira parte no campo de texto.
16. O clique **instala o certificado**.



Uma caixa de diálogo aparece que confirme a instalação seja bem sucedida.

Exemplo da linha de comando

CiscoASA
CiscoASA(config)#**crypto ca authenticate CA1** *!--- Initiates the prompt for paste-in of base64 CA intermediate certificate. ! This should be provided by the third party vendor.* 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**

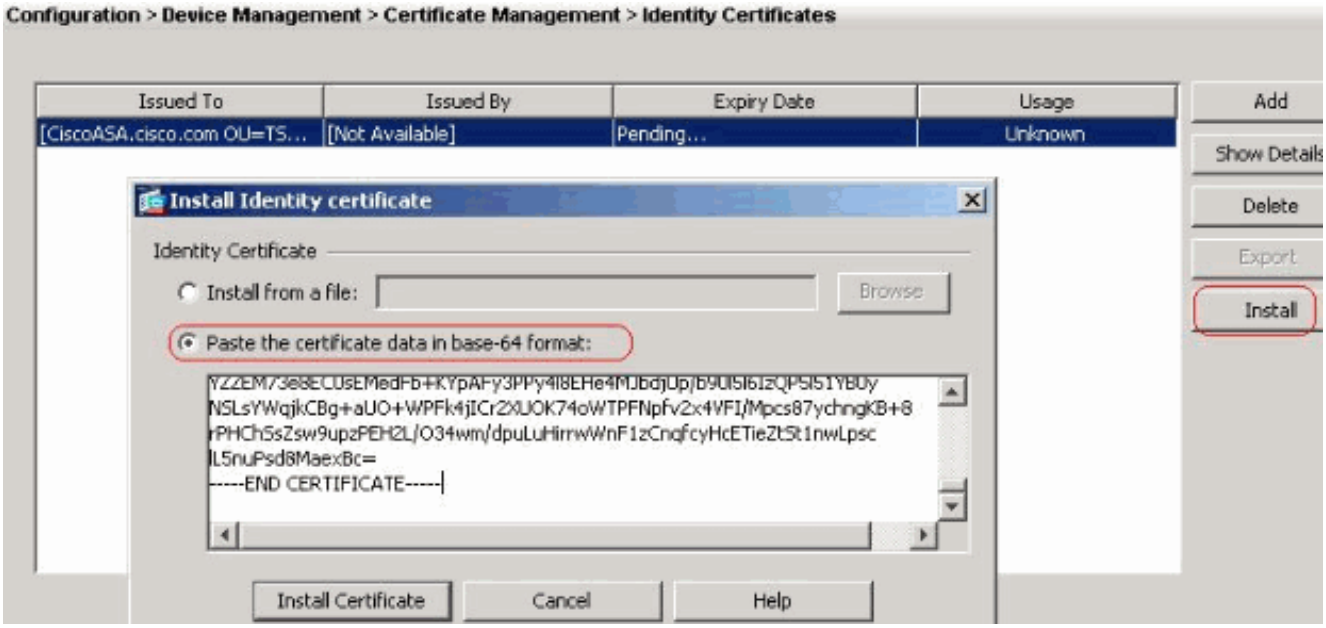
```
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGApAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZOOU1PmwAMuiMAD+mL9IqTbndosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjs1rxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKh4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQCfoFyk1vE6/Qlo+fQeSS
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)#
```

Etapa 4. Instale o certificado

Procedimento ASDM

Use o certificado de identidade fornecido pelo fornecedor de terceira parte a fim terminar estas etapas:

1. Clique a **configuração**, e clique então o **Gerenciamento de dispositivos**.
2. Expanda o **gerenciamento certificado**, e escolha então **certificados de identidade**.
3. Selecione o certificado de identidade que você criou em etapa 2.**Nota:** A data de expiração indica pendente.
4. O clique
   instala.



Clique a **pasta os dados do certificado no** botão de rádio do **formato base-64**, e cole o certificado de identidade fornecido pelo fornecedor de terceira parte no campo de texto.

5. O clique **instala o certificado**. 

Uma caixa de diálogo aparece a fim confirmar a importação é bem sucedida.

Exemplo da linha de comando

CiscoASA

```
CiscoASA(config)#crypto ca import CA1 certificate !---
Initiates prompt to paste the base64 identity !---
certificate provided by the third 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 third 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
```

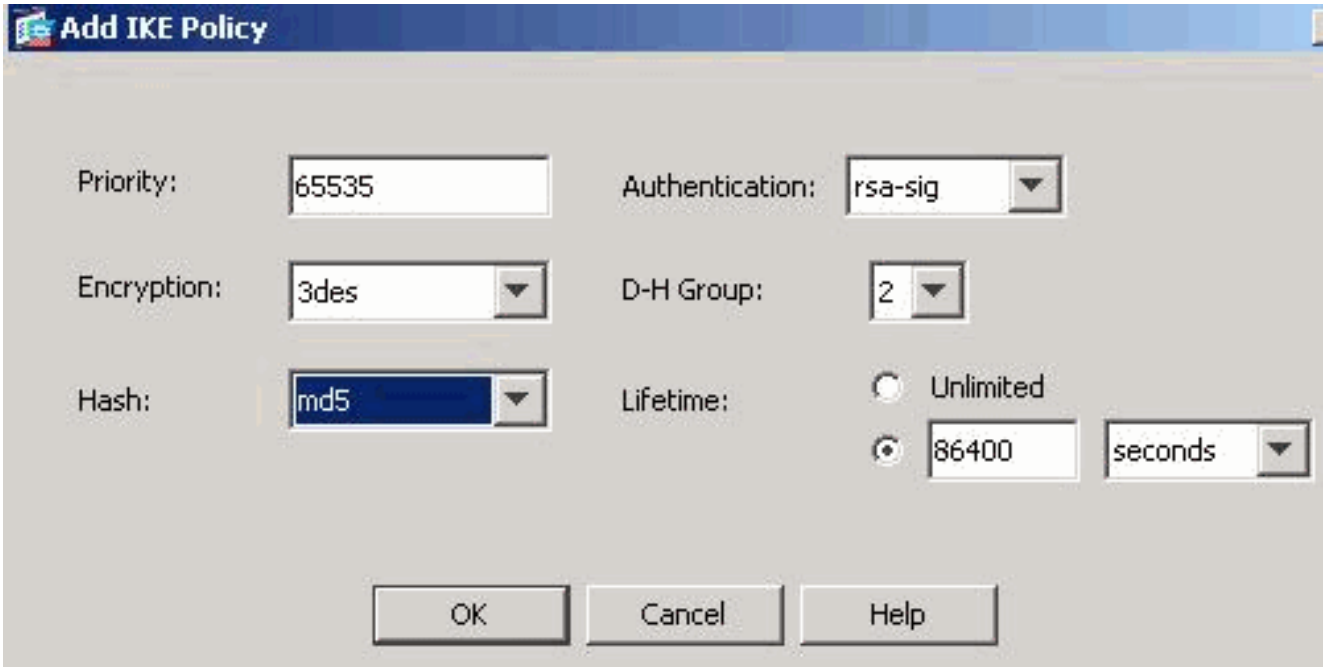
```
2zjwLCz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBYwFIISQ2lz
Y29BU0Eu
Y2lzY28uY29tMB0GA1UdDgQWBBQsJC3bSQzeGv4tY+MeH7KMl0xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfNQJpAPlWDCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
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/b90l5l6IzQP
5l51YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
t1nwLpsc lL5nuPsd8MaexBc= -----END CERTIFICATE----- quit
INFO: Certificate successfully imported
CiscoASA(config)#
```

Etapa 5. Configurar o acesso remoto VPN (IPsec) para usar o certificado recentemente instalado

Procedimento ASDM

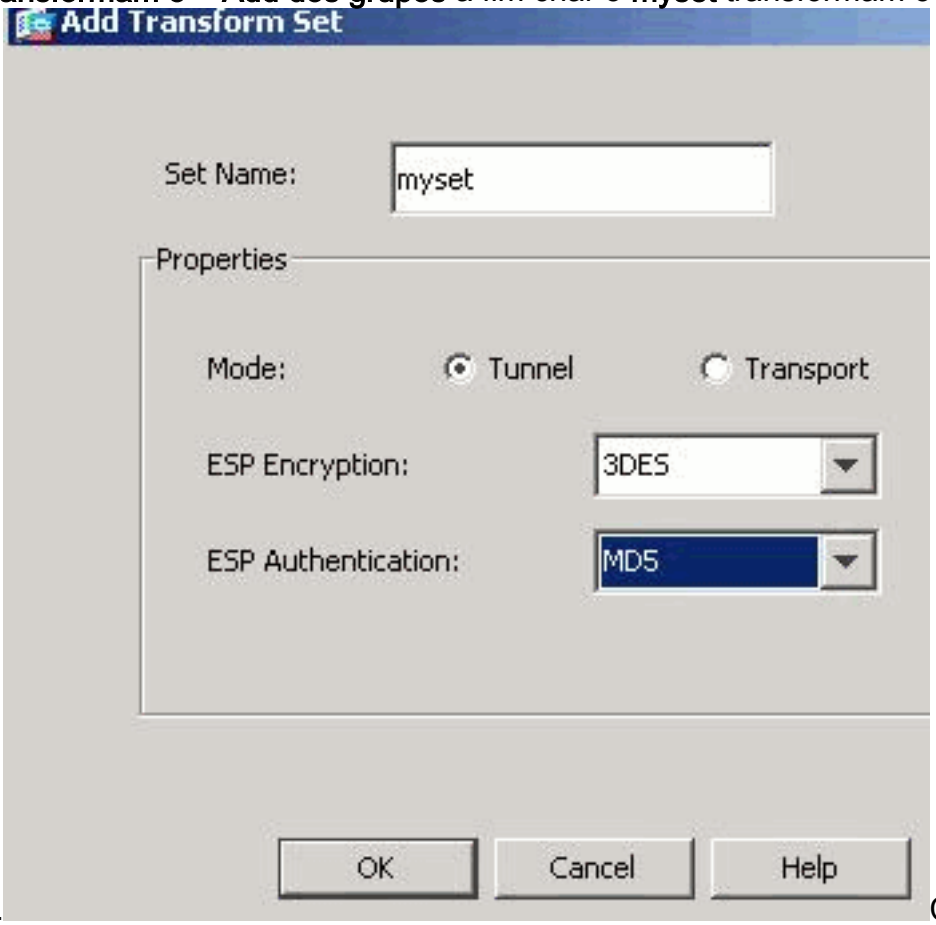
Termine estas etapas a fim configurar o acesso remoto VPN:

1. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > das políticas de IKE** a fim criar uma política de ISAKMP 65535, como mostrado.



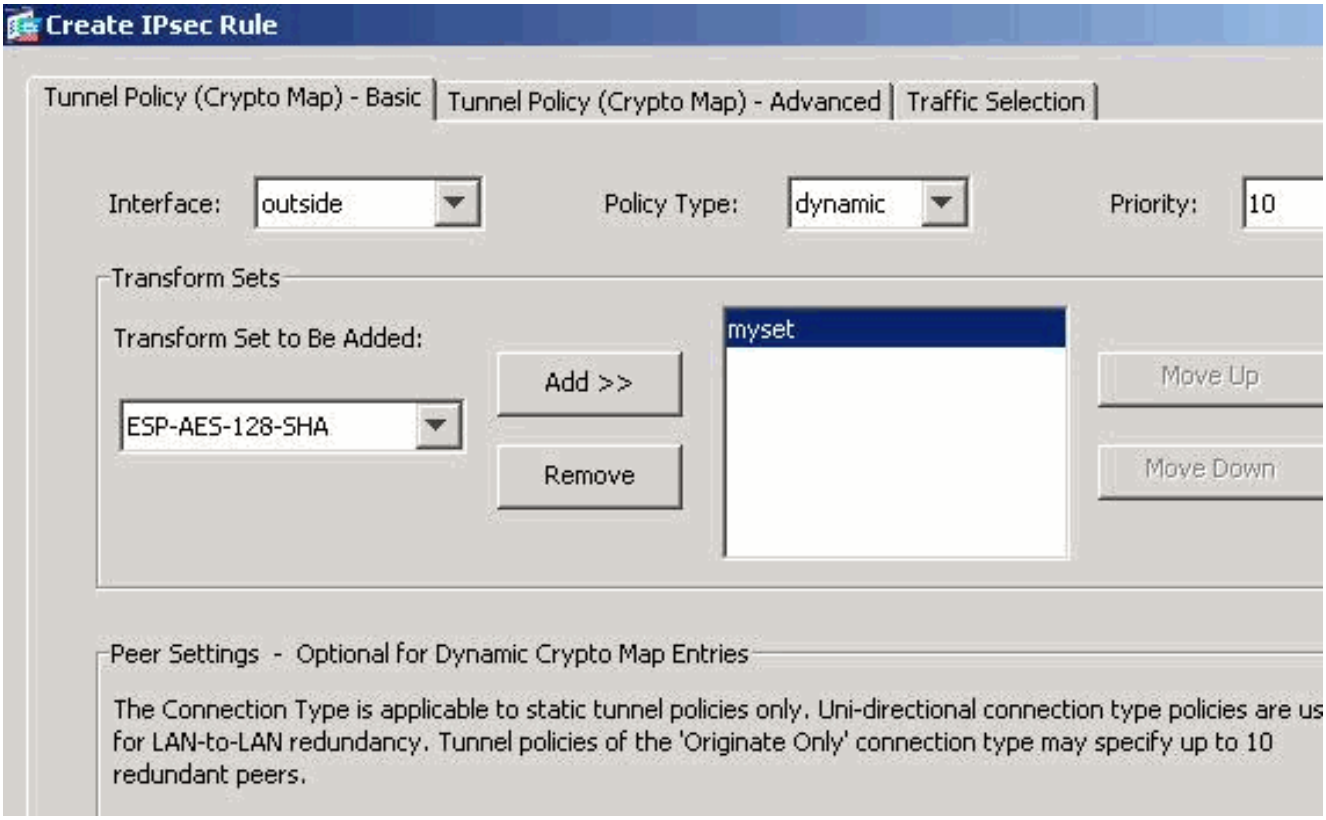
Clique a **APROVAÇÃO** e **aplique-a**.

2. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > IPsec > IPsec transformam o > Add dos grupos** a fim criar o **myset** transformam o grupo, como mostrado.



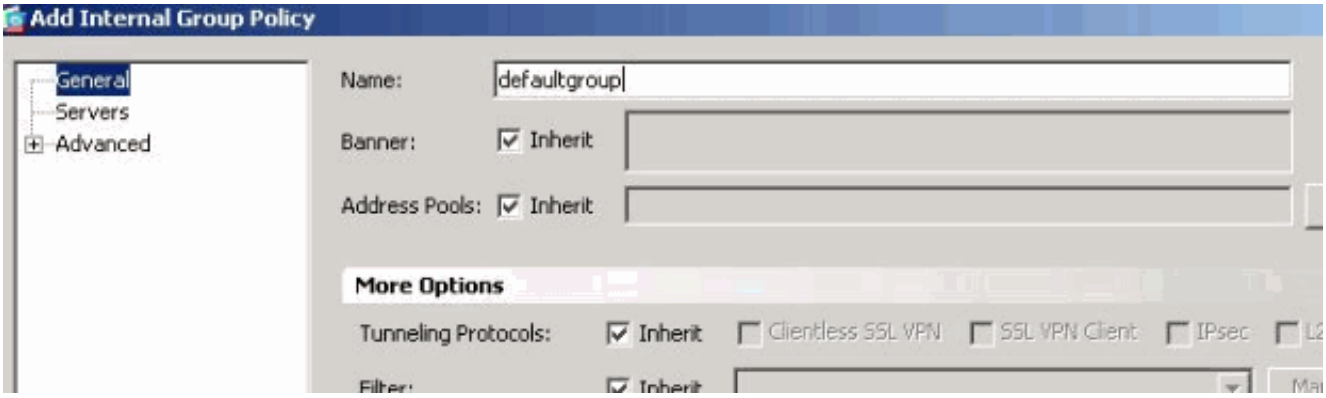
Clique a **APROVAÇÃO** e **aplique-a**.

3. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add do IPsec > dos crypto map** a fim criar um crypto map com a política dinâmica da prioridade 10, como
mostrado.



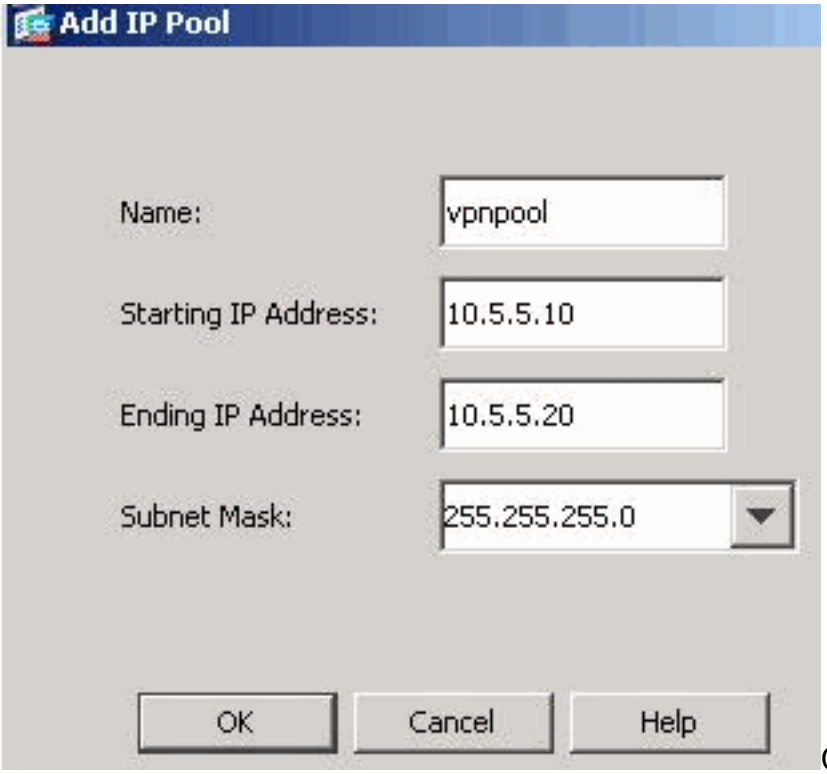
Clique a **APROVAÇÃO** e **aplique-a**.**Nota:** O ASA 8.0 não apoia SHA 2. Os clientes de IPSec que usam Certificados com uma mistura 256 não são apoiados igualmente.

4. Escolha a **configuração > o acesso do acesso remoto VPN > da rede (cliente) > avançou > > Add das políticas do grupo** a fim criar uma política do grupo de **Defaultgroup**, como mostrado.



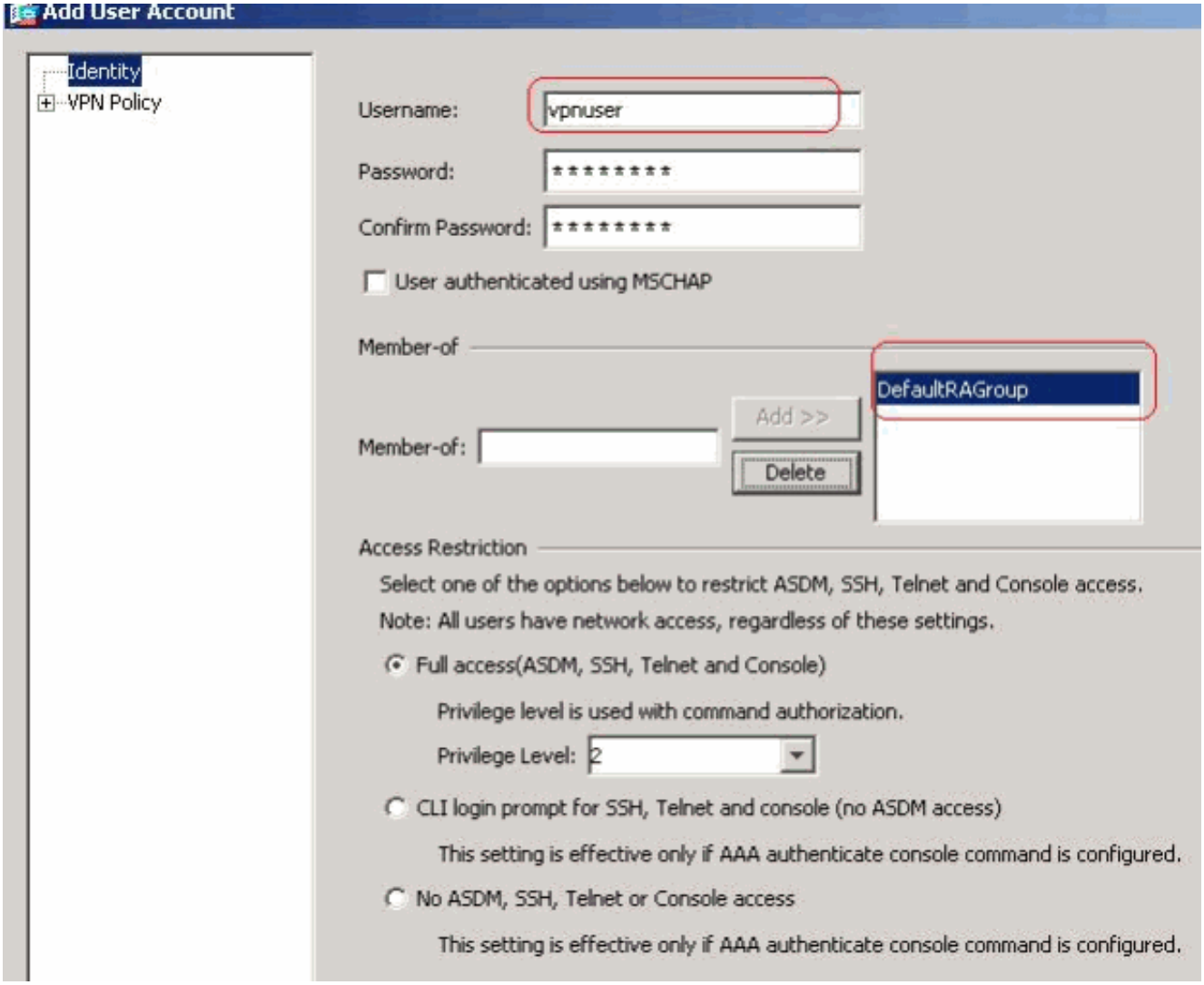
Clique a **APROVAÇÃO** e **aplique-a**.

5. Escolha a **configuração > o acesso remoto VPN > do acesso > da atribuição de endereço > dos conjuntos de endereços da rede (cliente) > Add** a fim configurar o conjunto de endereços do **vpnpool** para que os usuários de cliente VPN sejam atribuídos

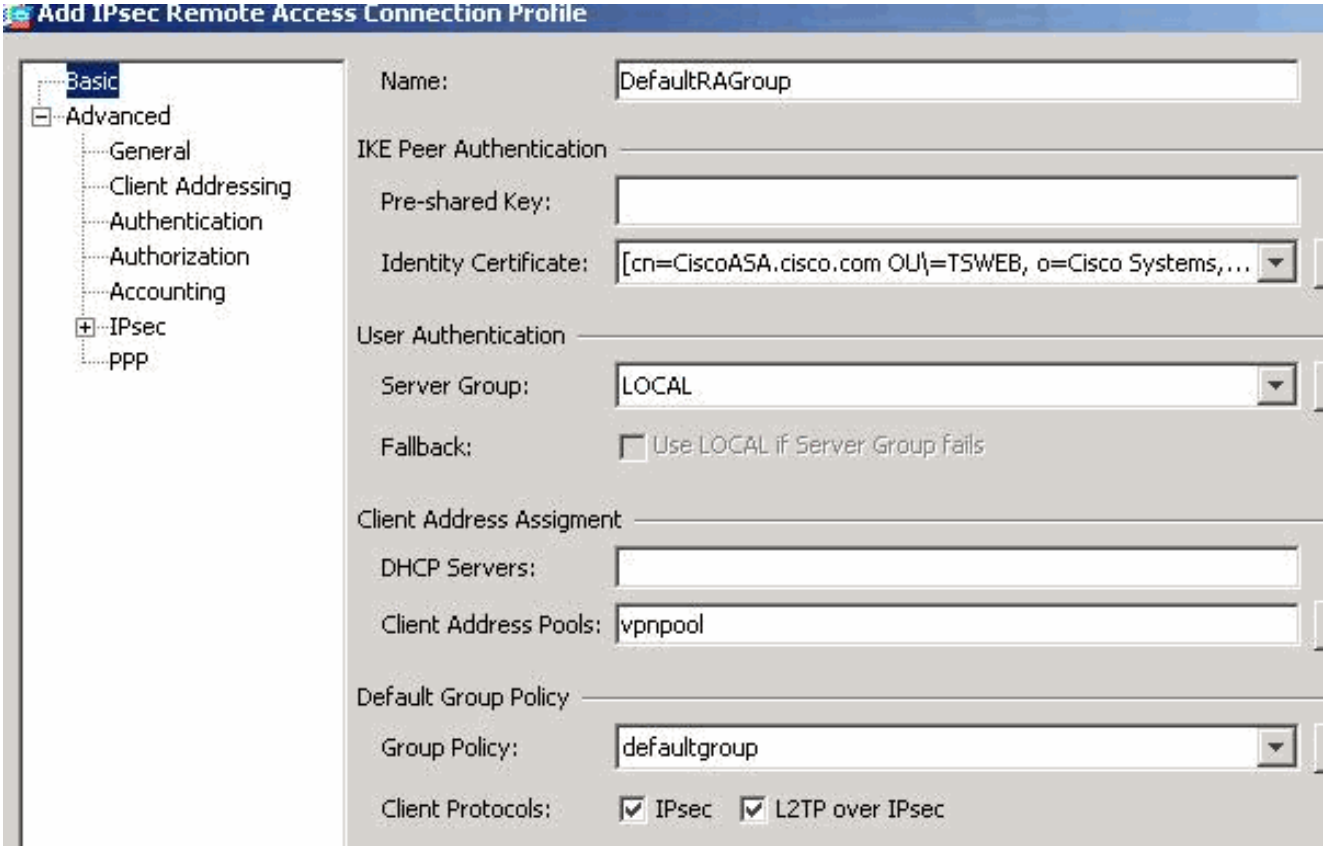


dinamicamente. Clique a **APROVAÇÃO** e **aplique-a**.

6. Escolha a **configuração > o acesso remoto VPN > o AAA Setup > > Add dos usuários locais** a fim criar o usuário do **vpnuser** esclarecem o acesso de cliente VPN. Também, faça a este usuário um membro de **DefaultRAGroup**.



7. Escolha a **configuração > o acesso remoto VPN > do acesso > da conexão IPSec da rede (cliente) perfis > editam** a fim editar o **DefaultRAGroup**, como mostrado.Escolha o **certificado de identidade** apropriado da gota para baixo para o campo da autenticação de peer IKE.Escolha o grupo de servidor como o **LOCAL** para o campo da autenticação de usuário.Escolha o **vpnpool** como o pool do endereço de cliente para o campo da atribuição de endereço de cliente.Escolha o **defaultgroup** como a política do grupo para o campo da política do grupo
padrão.



Clique a **APROVAÇÃO** e **aplique-a**.

Exemplo da linha de comando

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 dynmap 10 set
transform-set myset CiscoASA(config)#crypto map mymap 10
ipsec-isakmp dynamic dynmap CiscoASA(config)#crypto map
mymap 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
Cisco123 CiscoASA(config)#username vpnuser attributes
CiscoASA(config-username)#memberof DefaultRAGroup
CiscoASA(config-username)#exit !--- Create a user
account "vpnuser" and added to !--- "DefaultGroup"
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
```

Sumário de configuração ASA

CiscoASA

```
CiscoASA#show running-config
: Saved
:
ASA Version 8.0(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
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
no failover
icmp unreachable rate-limit 1 burst-size 1
```

```
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list 100
route DMZ 0.0.0.0 0.0.0.0 10.77.241.129 1
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
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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 DMZ
http 0.0.0.0 0.0.0.0 outside
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 dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap 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=Rale
 serial-number
 keypair my.CA.key
 crl configure
crypto ca certificate chain CA1
 certificate 611ee59b000000000007
    308205a7 3082048f a0030201 02020a61 1ee59b00
00000000 07300d06 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
    37313231 35303833 3533395a 170d3039 31323134
30383335 33395a30 76310b30
    09060355 04061302 55533117 30150603 55040813
0e4e6f72 74682043 61726f6c
    696e6131 10300e06 03550407 13075261 6c656967
68311630 14060355 040a130d
    43697363 6f205379 7374656d 73312430 22060355
0403131b 43697363 6f415341
    2e636973 636f2e63 6f6d204f 553d5453 57454230
819f300d 06092a86 4886f70d
    01010105 0003818d 00308189 02818100 b8e20aa8
332356b7 5b660073 5008d373
    5d23c529 5b92472b 5e02a81f 63dc7a57 0667d754
5e7f98d3 d4239b42 ab8faf0b
    e8a5d394 f80d01a1 4cc01d98 b1320e9f e849055a
b94b18ef 308eb12f 22ab1a8e
    db38f02c 2cf78e07 197f2d52 d3cb7391 a9ccb2d9
03f722bd 414b0a32 05aa053e
    c45e2464 80606f8e 417f09a7 aa9c644d 02030100
```

```
01a38202 de308202 da300b06
    03551d0f 04040302 05a0301d 0603551d 11041630
14821243 6973636f 4153412e
    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 74302106
092b0601 04018237 14020414
    1e120057 00650062 00530065 00720076 00650072
300c0603 551d1301 01ff0402
    30003013 0603551d 25040c30 0a06082b 06010505
07030130 0d06092a 864886f7
    0d010105 05000382 0101008a 82680f46 fbc87edc
84bc45f5 401b3716 0045515c
    2c81971d 0da51fe3 96870627 b41b4319 23284b30
5eafcedb 10c1ef05 d0686a61
    cd1ab877 100b965d 499088e1 7de418fb b5529199
46129b81 9c4353a2 1761b61c
    f9bc18c6 95c44e5c 8b3cfb71 a183c872 61964433
bddef040 b4b0431e 7456fe29
    8a40172d cf3f2e25 f041dee0 c25b7635 29fdbf74
97997a23 340fe65e 75601d32
    3522ec61 6aa39020 60f9a50e f963c593 88c80abd
9750e2bb e285933c 53697efd
    b1e15148 fcca5cb3 cef27219 e0281fbc acf1c285
2b19b30f 6ea733c4 1f62ff3b
    7e309bf7 69b8bb87 8abaf05a 7175cc29 ea7dcc87
7044e279 9b52b759 f02e9b1c
    94be67b8 fb1df0c6 9ec417
```

```
  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 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
    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
```

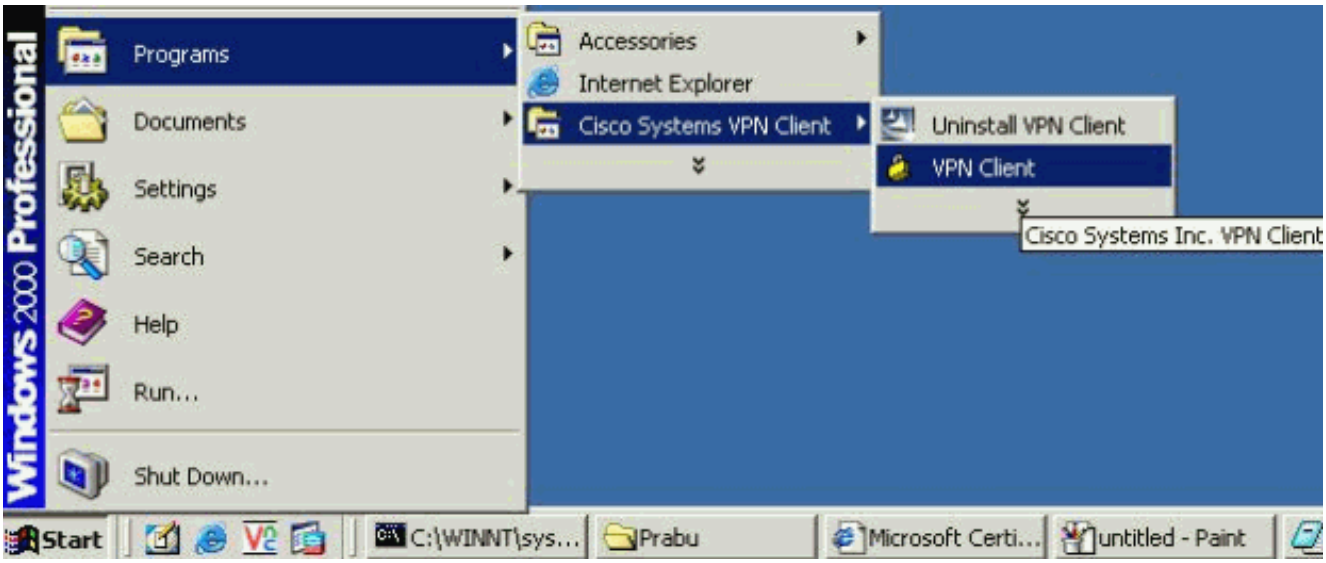
```
    8081f986 526fbe1c c9639d6f 258b2205 0dc370c6
5431b034 fe9fd60e 93a6e71b
    ab8e7f84 a011336b 37c13261 5ad218a3 a513e382
e4bfb2b4 9bf0d7d1 99865cc4
    94e5547c f03e3d3e 3b766011 e94a3657 6cc35b92
860152d4 f06b2b15 df306433
    c1bcc282 80558d70 d22d72e7 eed3195b d575dceb
c0caa196 34f693ea f3beee4d
    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
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
!
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
group-policy defaultgroup internal
group-policy defaultgroup attributes
 default-domain value cisco.com
username vpnuser password TXttW.eFqbHusJQM encrypted
username vpnuser attributes
 memberof DefaultRAGroup
tunnel-group DefaultRAGroup general-attributes
 address-pool vpnpool
tunnel-group DefaultRAGroup ipsec-attributes
 trust-point CA1
prompt hostname context
Cryptochecksum:dd6f2e3390bf5238815391c13e42cd21
```

```
: end
CiscoASA#
```

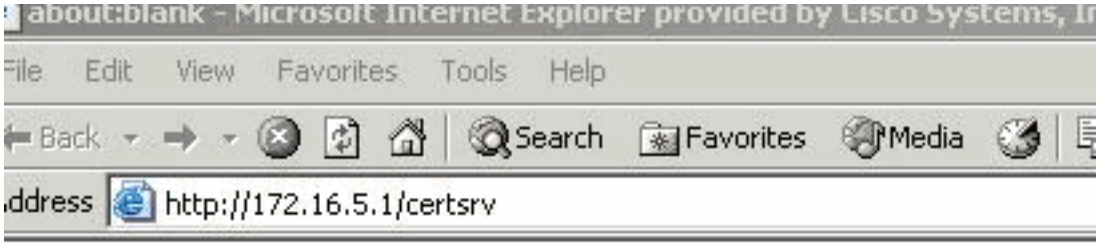
Configuração de cliente de VPN

Termine estas etapas a fim configurar o cliente VPN.

1. Escolha o **Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN** a fim lançar o software do cliente
   VPN.

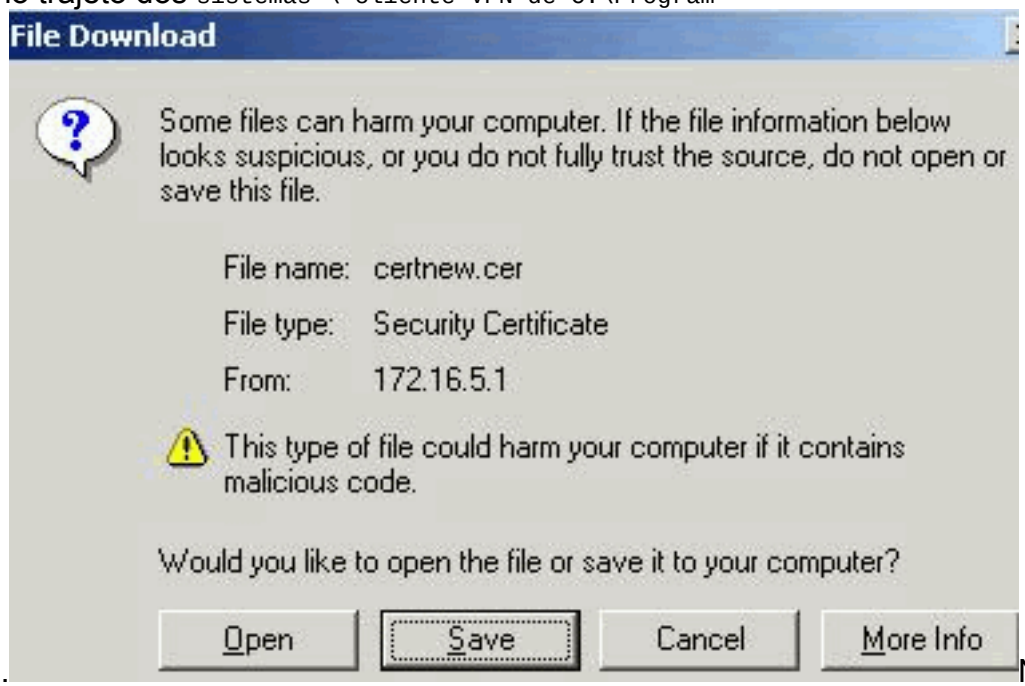


2. Termine estas etapas a fim transferir o certificado de CA do server de CA nomeado **CA1**, e instale-as no Cisco VPN Client.Execute o início de uma sessão da Web no server 172.16.5.1 de CA com a ajuda das credenciais fornecidas ao

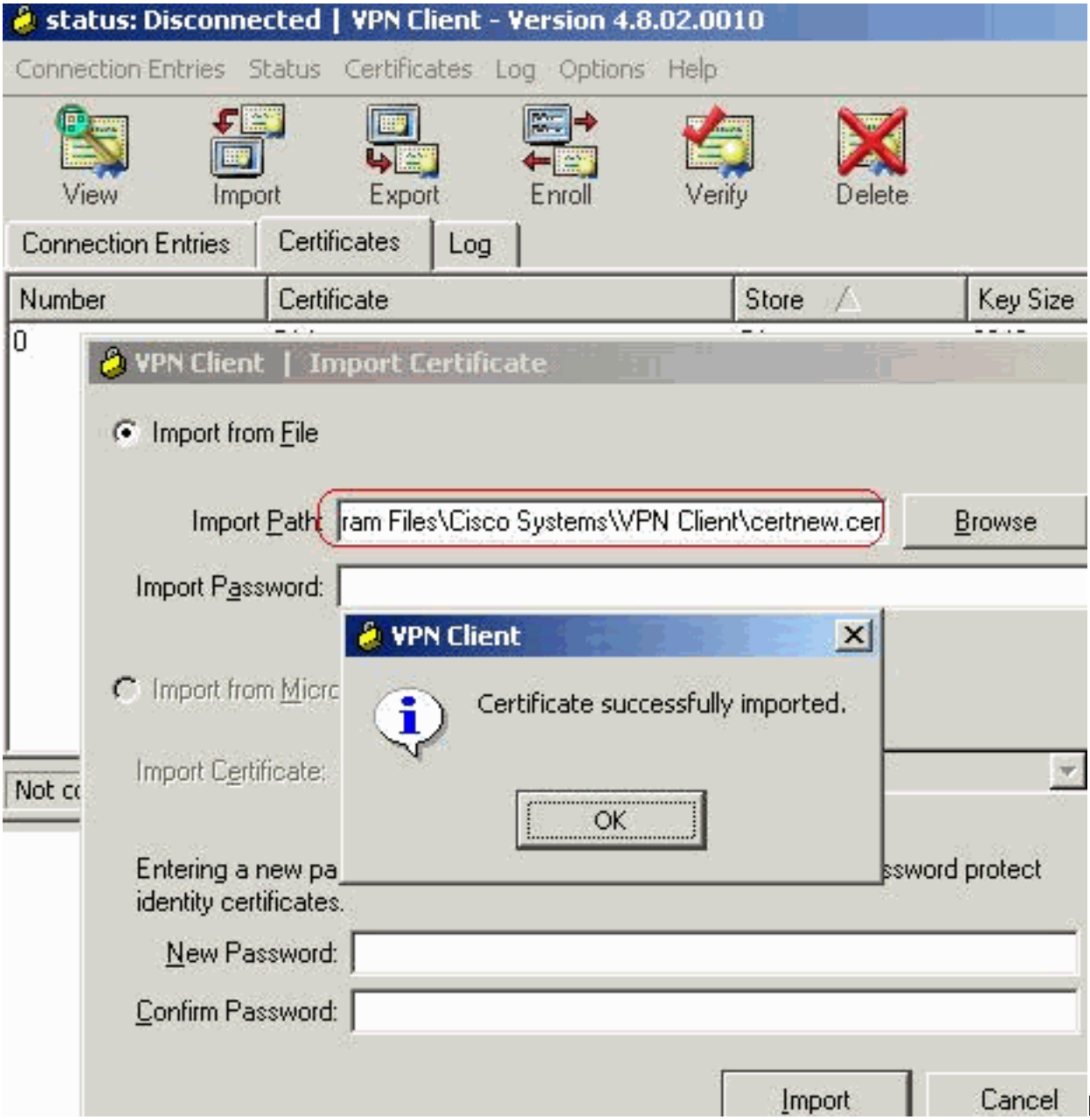


vpnuser.**Nota:** Certifique-se de que você manda um usuário esclarecer o usuário de cliente VPN com o server de CA.Clique a **transferência um certificado de CA, um certificate chain ou um CRL** a fim abrir o indicador, como mostrado. Clique o botão de rádio de **Base64** como o método de codificação, e clique o **certificado de CA da transferência**.

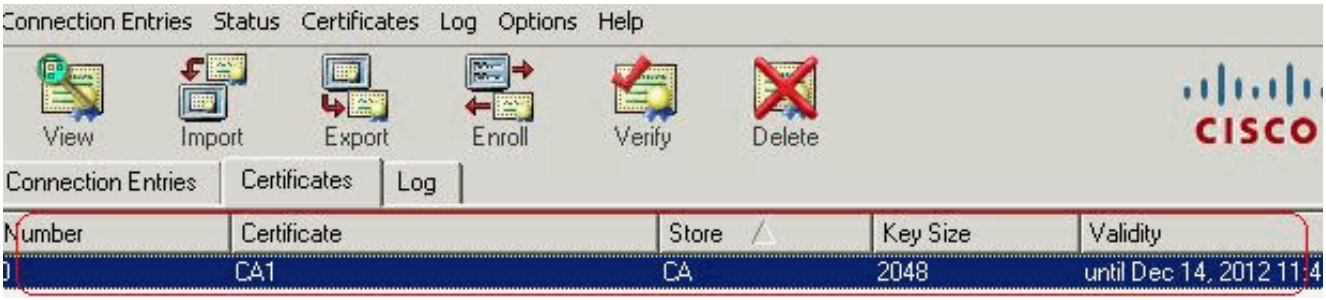
Salvar o certificado de CA com o nome de **certnew.cer em** seu computador. À revelia, armazena no trajeto dos `sistemas \ cliente VPN de C:\Program`



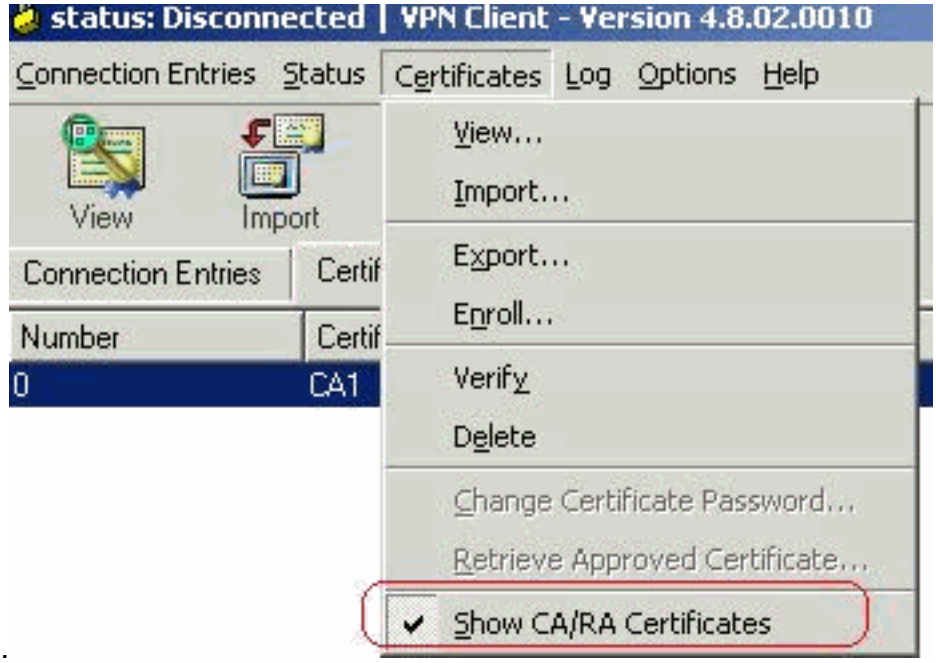
`Files\Cisco.` No cliente VPN, escolha a **aba > a importação dos Certificados**, e clique a **importação do** botão de **Fileradio**. O clique **consulta** a fim importar o certificado de CA dos `sistemas de C:\Program Files\Cisco do` lugar armazenado `\ cliente VPN`, como mostrado.**Importação do** clique. Um indicador do sucesso aparece, como mostrado.



Na aba dos Certificados, os certificados de CA CA1 aparecem, como mostrado.

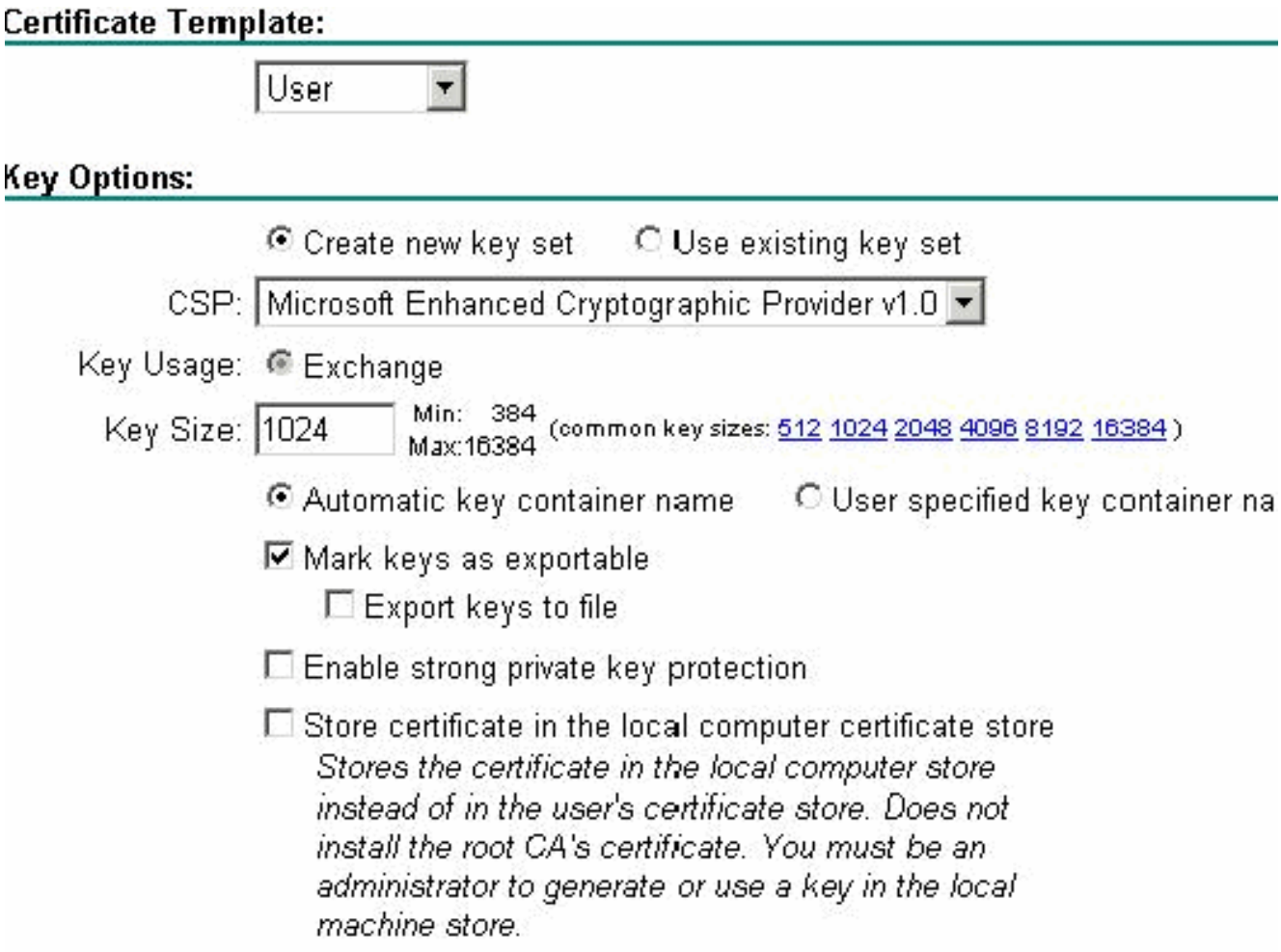


Nota: Certifique-se de que a opção dos **Certificados da mostra CA/RA** está escolhida, como mostrado, se não os certificados de CA não se deva aparecer no indicador do

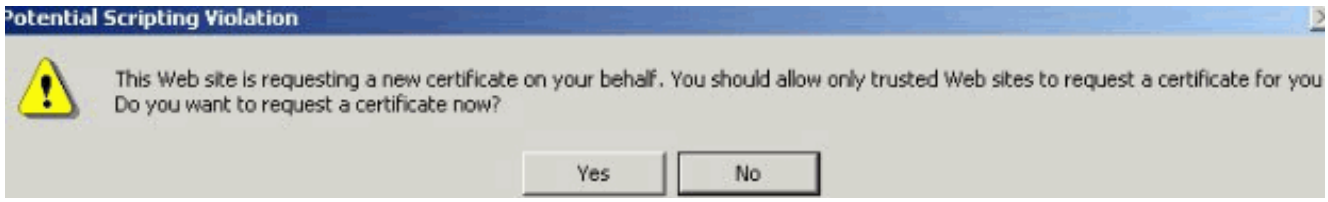


certificado.

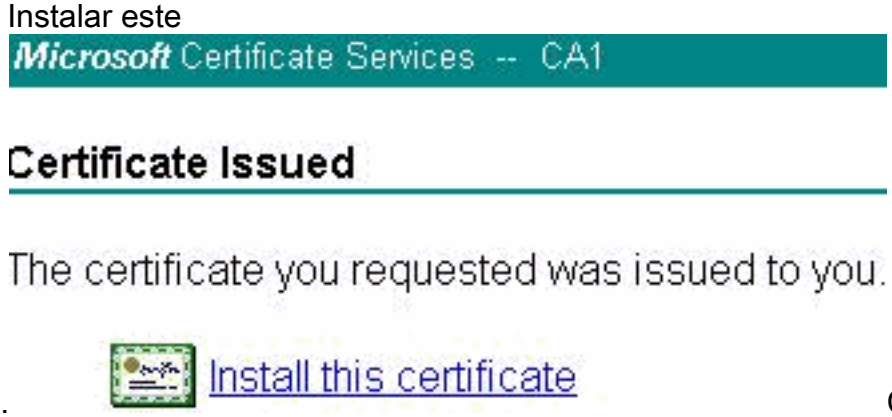
3. Termine estas etapas a fim transferir o certificado de identidade e instalá-lo no cliente VPN.No server CA1 de CA, escolha o **pedido um certificado > avançou o pedido do certificado > criam e submetem um pedido a este CA** a fim registrar-se para o certificado de identidade.Clique em
   Submit.



Clique **Yes** para continuar.

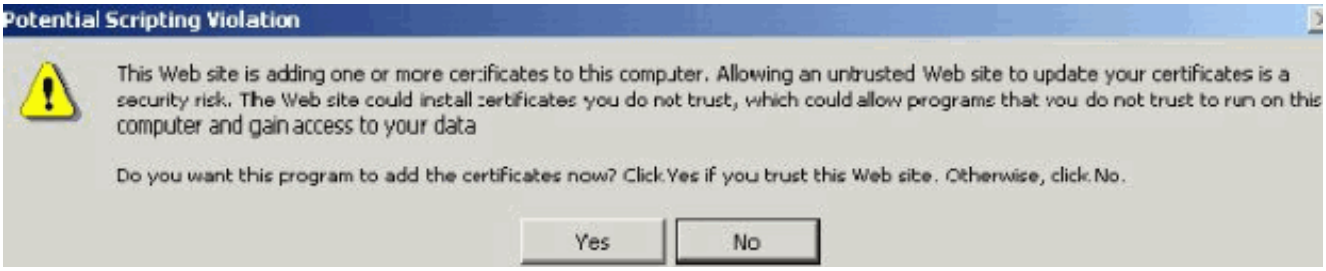


Clique em Instalar este certificado.

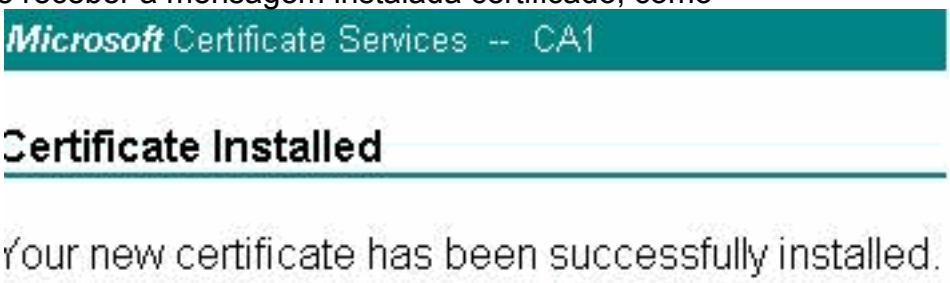


Clique **Yes** para

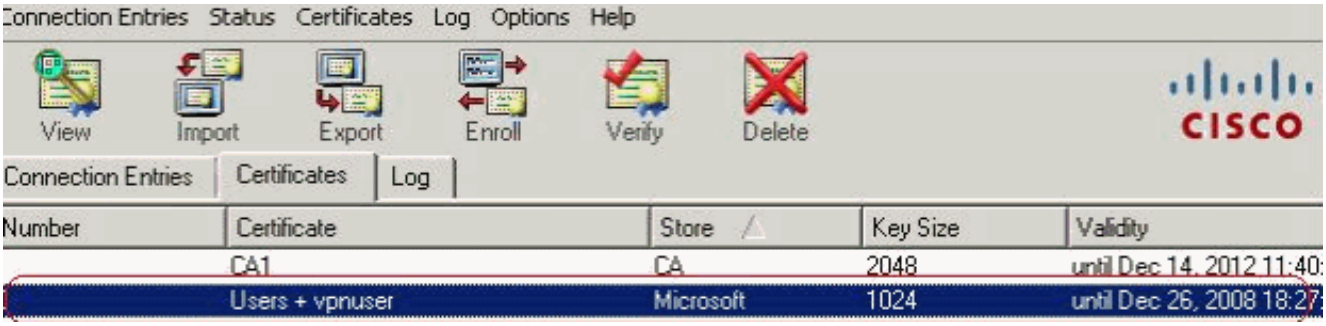
continuar.



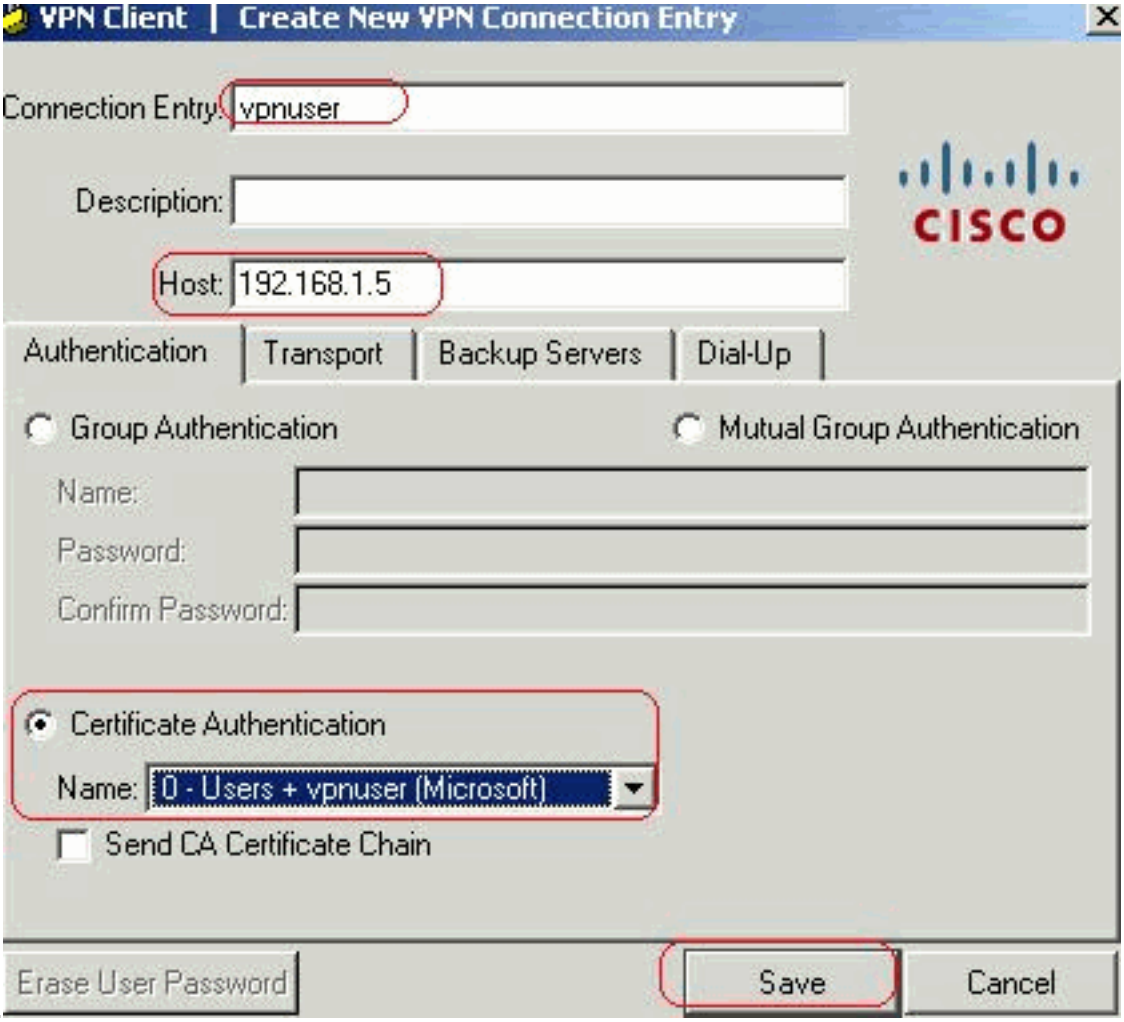
Você deve receber a mensagem instalada certificado, como



mostrado. Retire o cliente VPN e relance-o a fim fazer o certificado de identidade instalado começar aparecer na aba do certificado do cliente VPN, como
mostrado.

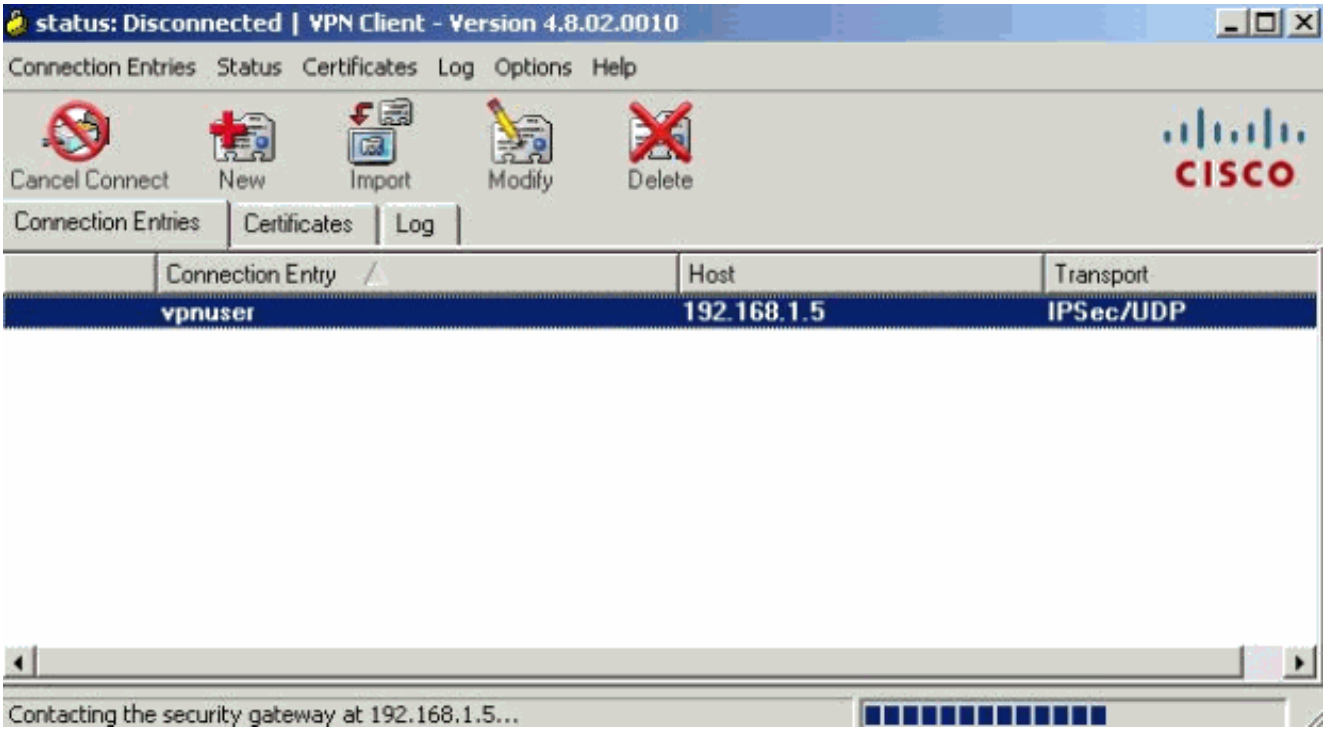


4. Nas entradas de conexão catalogue, clique **novo** a fim criar o **vpnuser da** entrada de conexão, como mostrado.Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT do peer remoto (roteável) ao campo do host.Clique o botão de rádio do **certificado de autenticação**, e escolha o certificado de identidade da lista de gota para baixo, como mostrado.Clique em

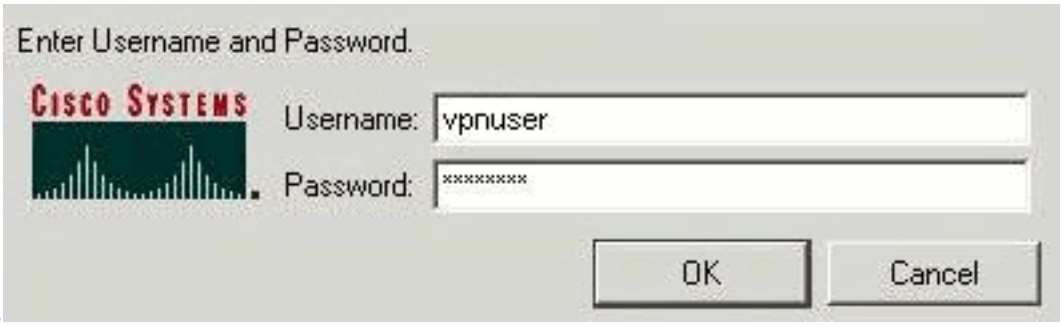


Salvar.

5. Clique em Conectar.



6. Quando alertado, incorpore a informação do nome de usuário e senha para o Xauth, e clique a **APROVAÇÃO** a fim conectar à rede

remota. 

7. O cliente VPN conecta com o ASA, como mostrado. 

Verificar

No ASA você pode emitir diversos comandos show na linha de comando a fim verificar o estado de um certificado.

Use esta seção para confirmar se a sua configuração funciona corretamente.

- Os indicadores do **comando crypto ca trustpoint da mostra** configuraram pontos confiáveis.`CiscoASA#show crypto ca trustpoints`

```
Trustpoint CA1:
    Subject Name:
    cn=CA1
    dc=TSWeb
    dc=cisco
    dc=com
          Serial Number: 7099f1994764e09c4651da80a16b749c
    Certificate configured.
```

- **O comando show crypto ca certificate** indica todos os Certificados instalados no sistema.`CiscoASA# show crypto ca certificate`

```
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=Configuration,DC=TSWeb,DC=cisco,
    DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
    [2]  http://ts-w2k3-acs.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=Configuration,DC=TSWeb,DC=cisco,
    DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
    [2]  http://ts-w2k3-acs.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


Certificate
  Subject Name:
    Name: CiscoASA.cisco.com
  Status: Pending terminal enrollment
  Key Usage: General Purpose
  Fingerprint:  1a022cf2 9771e335 12c3a530 1f9a0345
  Associated Trustpoint: CA1
```

- Os indicadores do **comando show crypto ca crls** puseram em esconderijo listas revogação de certificado (CRL).
- **O comando show crypto key mypubkey rsa** indica todos os pares de chave de criptografia gerados.

```
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#
```

- **O comando show crypto isakmp sa** indica a informação de túnel 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

1   IKE Peer: 10.1.1.5
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE
```

- **O comando show crypto ipsec sa** indica a informação do túnel de 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
```

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Estão aqui alguns possíveis erros que você pode encontrar:

- **ERRO: Não analisam gramaticalmente nem não verificam o certificado importado**Este erro pode ocorrer quando você instala o certificado de identidade e não tem o intermediário ou o certificado CA raiz correto autenticado com o ponto confiável associado. Você deve remover e reauthenticate com o intermediário ou o certificado CA raiz correto. Contacte seu fornecedor de terceira parte a fim verificar que você recebeu o certificado de CA correto.
- **O certificado não contém a chave pública de uso geral**Este erro pode ocorrer quando você tenta instalar seu certificado de identidade ao ponto confiável errado. Você tenta instalar um certificado de identidade inválido, ou o par de chaves associado com o ponto confiável não combina a chave pública contida no certificado de identidade. Emita o comando **cripto do trustpointname dos Certificados Ca da mostra** a fim verificar que você instalou seu certificado de identidade ao ponto confiável correto. Procure a linha que indica **pontos confiáveis associados**: Se o ponto confiável errado está listado, use os procedimentos descritos neste documento a fim remover e reinstalar o ponto confiável apropriado. Também, verifique que o par de chaves não mudou desde que o CSR foi gerado.
- **ERRO: ASA/PIX. Identificação remota inválida do certificado Sev=Warning/3 IKE/0xE3000081:**Se você tem problemas de autenticação com Certificados, este Mensagem de Erro pode aparecer no cliente VPN. Use o **automóvel do** comando crypto isakmp identity na configuração ASA/PIX a fim resolver a edição.

Informações Relacionadas

- Página de suporte adaptável da ferramenta de segurança de Cisco
- Página de Suporte do Cisco VPN Client
- Configurando o servidor Microsoft como o Certificate Authority (CA)
- Suporte Técnico e Documentação - Cisco Systems