

# ASA/PIX 7.x e autenticação IPSec do cliente VPN usando Certificados digitais com exemplo de configuração de Microsoft CA

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Produtos Relacionados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração ASA](#)

[Sumário de configuração ASA](#)

[Configuração de cliente de VPN](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## [Introdução](#)

Este documento descreve como instalar manualmente um certificado digital de terceiros no Cisco Security Appliance (ASA/PIX) 7.x, assim como clientes VPN, para autenticar os peers IPSec com o servidor do Microsoft Certificate Authority (CA).

## [Pré-requisitos](#)

### [Requisitos](#)

Este documento exige que você tem o acesso a um Certificate Authority (CA) para o certificado de registro. 3ª parte que apoiada vendedores de CA inclui Baltimore, Cisco, confiam, iPlanet/Netscape, Microsoft, RSA, e Verisign.

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

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

## [Componentes Utilizados](#)

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

- ASA 5510 que executa a versão de software 7.2(2) e a versão 5.2(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 7.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 da RFC1918 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](#)

Termine estas etapas a fim instalar um certificado digital do vendedor da 3ª parte no ASA:

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

[Etapa 2. Gerencia o par de chaves RSA](#)

[Etapa 3. Crie o ponto confiável.](#)

[Etapa 4. Gerencia o certificado de registro.](#)

[Etapa 5. Autentique o ponto confiável](#)

[Etapa 6. Instale o certificado](#)

[Etapa 7. 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. **A configuração do clique**, e clica então **propriedades**.
2. Expanda a **administração do dispositivo**, 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 16:25:49.580 IST Fri Dec 28 2007
```

[Etapa 2. Gerencia o par de chaves RSA](#)

A chave pública gerada RSA é combinada com a informação de identidade do ASA para formar um pedido do certificado PKCS#10. Você deve distintamente identificar o nome chave com o ponto confiável para que você cria o par de chaves.

### Procedimento ASDM

1. **A configuração do clique**, e clica então **propriedades**.
2. Expanda o **certificado**, e escolha o **par de chaves**.
3. Clique em **Add**.
4. Dê entrada com o nome chave, escolha o tamanho do módulo, e selecione o tipo do uso. **Nota:** O tamanho recomendado do par de chaves é 1024.
5. O clique **gerencie agora**. O par de chaves que você criou deve ser alistado na coluna do nome do par de chaves.

### 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)#
```

[Etapa 3. Crie o ponto confiável](#)

Os pontos confiáveis são exigidos declarar o Certificate Authority (CA) que seu ASA usará.

## Procedimento ASDM

1. **A configuração do clique**, e clica então **propriedades**.
2. Expanda o **certificado**, e expanda então o **ponto confiável**.
3. Escolha a **configuração**, e clique-a então **adicionam**.
4. Configurar estes valores:**Nome do ponto confiável**: O nome do ponto confiável deve ser relevante ao uso pretendido. (Este exemplo usa o *CA1*.)**Par de chaves**: Selecione o par de chaves gerado em [etapa 2](#). (my.CA.key)
5. Assegure-se de que a **Inscrição manual** esteja selecionada.
6. Clique **parâmetros do certificado**.A caixa de diálogo dos parâmetros do certificado aparece.
7. Clique **editam**, e configuram 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**.
8. Uma vez que os valores apropriados são adicionados, clique a **APROVAÇÃO**.
9. Na caixa de diálogo dos parâmetros do certificado, incorpore o FQDN ao campo FQDN da especificação.Este valor deve ser o mesmo FQDN que você se usou para o Common Name (CN).
10. Clique em **OK**.
11. Verifique que o par de chaves correto está selecionado, e clique o botão de rádio da **Inscrição manual do uso**.
12. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.

## Exemplo da linha de comando

```
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=wepvpn.cisco.com,OU=TSWEB, O=Cisco
Systems,C=US,St=North Carolina,L=Raleigh !--- Defines
x.500 distinguished name. CiscoASA(config-ca-
trustpoint)#keypair my.CA.key !--- Specifies key pair
generated in Step 2. CiscoASA(config-ca-trustpoint)#fqdn
CiscoASA.cisco.com !--- Specifies subject alternative
name (DNS:). CiscoASA(config-ca-trustpoint)#exit
```

## [Etapa 4. Gerencia o certificado de registro](#)

## Procedimento ASDM

1. **A configuração do clique**, e clica então **propriedades**.
2. Expanda o **certificado**, e escolha o **registro**.
3. Verifique que o ponto confiável criado em [etapa 3](#) está selecionado, e o clique **se registra**.Uma caixa de diálogo parece que alista o pedido do certificado de registro (igualmente referido como uma solicitação de assinatura de certificado).
4. Copie o pedido do registro PKCS#10 a um arquivo de texto, e submeta então o CSR salvar a seu vendedor da 3ª parte (tal como Microsoft CA) segundo as indicações deste procedimento:Entre ao server 172.16.5.1 de CA com os credantials do usuário fornecidos ao

server do vpn. **Nota:** Certifique-se de você mandar um usuário esclarecer o ASA (server do vpn) com o server de CA. Clique o **pedido um certificado > avançou o pedido do certificado**, e selecionam-no então **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 no campo de texto da **solicitação salva**, e o clique **submete-se**. Clique o botão de rádio **codificado Base64**, e clique o **certificado da transferência**. Quando a caixa do dialob da transferência do arquivo aparece, salvar a com o nome **cert\_client\_id.cer**, que é o certificado de identidade a ser instalado no ASA.

### Exemplo da linha de comando

```
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:
MIICHjCCAYcCAQAwgAxEADAQBgNVBACTB1JhbGVpZ2gxZmZzAVBgNVBAGT
Dk5vcnRo
IENhcm9saW5hMQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ21zY28gU31z
dGVtczE0
MAwGA1UECxMFVFNXRUIxGzAZBgNVBAMTEmNpc2NvYXNhLmNpc2NvLmNv
bTEhMB8G
CSqGSIb3DQEJAhYSY21zY29hc2EuY21zY28uY29tMIGfMA0GCSqGSIb3
DQEBAQUA
A4GNADCBiQKBgQCmM/2VteHnhihS1uOj0+hWa5KmOPpI6Y/MMWmqgBaB
9M4yTx5b
Fm886s8F73WsfQPynBDFBSsejDOnBpFYzKsGf7TUMQB2m2RFaqfyNxYt
3oMXSNPO
m1dZ0xJVnRIp9cyQp/983pm5PfDD6/ho0nTktx0i+1cEX0luBMh7oKar
gwIDAQAB
oD0wOwYJKoZIhvcNAQkOMs4wLDALBgNVHQ8EBAMCBaAwHQYDVR0RBByw
FIISY21z
Y29hc2EuY21zY28uY29tMA0GCSqGSIb3DQEBAUUA4GBABrxpY0q7SeO
HZf3yEJq
po6wG+oZpsvpYI/HemKulaRc783w4BMO5lulIEhHgRqAxrTbQn0B7JPI
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)#
```

### [Etapa 5. Autentique o ponto confiável](#)

Uma vez que você recebe o certificado de identidade do vendedor da 3ª parte, você pode continuar com esta etapa.

## Procedimento ASDM

1. Salvar o certificado de identidade a seu computador local.
2. Se você foi fornecido um certificado base64-encoded que não venha como um arquivo, você deve copiar a mensagem base64, e cola-a 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, o ícone do arquivo deve indicar como um certificado como mostrado.
4. Fazer duplo clique o arquivo certificado. **Nota:** Se “Windows não tem bastante informação a verificar que a mensagem deste certificado” parece no tab geral, você deve obter a CA raiz do vendedor da 3ª parte ou o certificado de CA intermediário antes que você continue com este procedimento. Contacte seu vendedor da 3ª 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 situado acima de 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. Termine estas etapas a fim transferir o certificado de CA do server de CA nomeado *CA1*: Entre ao server 172.16.5.1 de CA com os credantials do usuário fornecidos ao server do vpn. Clique a **transferência um certificado de CA, um certificate chain ou um CRL**, e selecione então o botão de rádio de **Base64** a fim especificar o método de codificação. Clique o **certificado de CA da transferência**. Salvar o certificado de CA a seu computador com o nome **certnew.cer**.
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 o escolha **enviam a > bloco de notas**.)
11. A mensagem base64-encoded deve parecer similar ao certificado nesta imagem:
12. Dentro do ASDM, a **configuração do clique**, e clica então **propriedades**.
13. Expanda o **certificado**, e escolha a **autenticação**.
14. Clique a **entrada o texto do certificado** no botão de rádio do **hexadecimal ou do formato base64**.
15. Cole o certificado de CA base64-formatted de seu editor de texto na área de texto.
16. O clique **autentica**.
17. Clique em **OK**.

## Exemplo da linha de comando

```
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
MRMwEQYKCZImiZPyLQGByDY29tMRUwEwYKCZImiZPyLQGByFY21z
Y28xFTAT
BgoJkiaJk/IsZAEZFgVUU1dllyjEMMAoGAlUEAxMDQ0EzMB4XDTA3MTIx
NDA2MDE0
MloXDTEyMTIxNDA2MTAxNvowUTETMBEGCgmSJomT8ixkARkWA2NvbTEV
MBMGCgms
JomT8ixkARkWBWNpc2NvMRUwEwYKCZImiZPyLQGByFVFNXZWIxDDAK
```

```

BgNVBAMT
A0NBMTCCAS1wDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOqP7seu
VvyiLmA9
BSGzMz3sCtR9TCMWOx7qM8mmiD0o7OkGAPAvmtHrK431iMuaeKBpo5Zd
4TNgNtjX
bt6czaHpBuyIsyoZ0OU1PmwAMuiMAD+mL9IqTbdosJfy7Yhh2vWeMij
cQnwdOq+
Kx+sWaeNCjslrxeuaHpIBTuaNOckueBUBjxgpJuNPAk1G8YwBfaTV4M7
kZf4dbQI
y3GoFGmh8zGx6ys1DEaUQxRVwhDbMIvwqYBXWKH4uC04xxQmr//Sct1t
dWQcvk2V
uBwCsptW7C1akTqfm5XK/d//z2eUuXrHYySQcfoFyk1vE6/Q1o+fQeSS
z+T1DhXx
wPXRO18CAwEAAaOCAW8wggFrMBMGCSsGAQQBgjcUAQOGHgQAQwBBMAsg
A1UdDwQE
AwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBbBTZrb8I8jqI8RRD
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
1XXc68DKoZY09pPq877uTaou8cLtuipOmeOyZgJON+xaZx2EwGPn149
zpXv5tqt 9Ms7ABAU+pRIoi/EfjQgMSQGF1457cIH7dx1VD+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 6. Instale o certificado](#)

### Procedimento ASDM

Use o certificado de identidade fornecido pelo vendedor da 3ª parte para executar estas etapas:

1. Clique a **configuração**, e clique então **propriedades**.
2. Expanda o **certificado**, e escolha então o **certificado de importação**.
3. Clique a **entrada o texto do certificado** no botão de rádio do hexadecimal ou do formato **base64**, e cole o certificado de identidade base64 no campo de texto.
4. Clique a **importação**, e clique então a **APROVAÇÃO**.

**Exemplo da linha de comando**

## 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+gAwIBAgIKYR7lmwAAAAAABzANBgkqhkiG9w0BAQUFADBBR
MRMwEQYK
CZImiZPyLQGBGRYDY29tMRUwEwYKCZImiZPyLQGBGRYFY2lzY28xFTAT
BgoJkiaJ
k/IsZAEZFgVUU1dlYjEMMAoGAlUEAxMDQ0ExMB4XDTA3MTIxNTA4MzUz
OVoxDTA5
MTIxNDA4MzUzOVowdjELMAkGA1UEBhMCVVMxZjZAVBgNVBAGTDk5vcnRo
IENhcm9s
aW5hMRAwDgYDVQQHEwdSYWxlaWdoMRYwFAYDVQQKEw1DaXNjb3R5b3R5
ZW1zMSQw
IgwYDVQDExtDaXNjb3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5
KoZiHvcN
AQEBBQADgY0AMIGJAoGBALjiCqgzI1a3W2Yac1AI03NdI8UpW5JHK14C
qB9j3HpX
BmfXVF5/mNPUI5tCq4+vC+il05T4DQGhTMAdmLEyDp/oSQVauUsY7zCO
sS8iqxqO
2zjwLcz3jgcZfy1S08tzkanMstkD9yK9QUsKMgWqBT7EXiRkgGBvjkF/
CaeqnGRN
AgMBAAGjggLeMIIC2jALBgNVHQ8EBAMCBaAwHQYDVR0RBBywFIISQ2lz
Y29BU0Eu
Y2lzY28uY29tMB0GA1UdDgQWBbBQsJC3bSQzeGv4tY+MeH7KM10xCFjAf
BgNVHSME
GDAWgBTZrb8I8jqI8RRDL3mYfnQJpAP1WCCAQMGA1UdHwSB+zCB+DCB
9aCB8qCB
74aBtWxkYXA6Ly8vQ049Q0ExLENOPVRTLVcySzMtQUNTLENOPUNEUCxD
Tj1QdWJs
aWM1MjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWdl
cmF0aW9u
LERDPVRTV2ViLERDPWNpc2NvLERDPWNvbT9jZXJ0aWZpY2F0ZVJldm9j
YXRpb25M
aXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1zdHJpYnV0aW9uUG9pbmSG
NW50dHA6
Ly90cy13MmszLWFjcy50c3dlYi5jaXNjb3R5b3R5b3R5b3R5b3R5b3R5b3R5
QTEuY3Js
MIIBHQYIKwYBBQUHAQEegEPMIIBCzCBqQYIKwYBBQUHMAKGgZxsZGFw
Oi8vL0NO
PUNBMSxDTj1BSUESQ049UHVibG1jJTIwS2V5JTIwU2Vydm1jZXMsQ049
U2Vydm1j
ZXMsQ049Q29uZmlndXJhdGlvbixEQz1UU1dlYixEQz1jaXNjb3R5b3R5b3R5
b20/Y0FD
ZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnpZmljYXRpb25B
dXR0b3R5
dHkwXQYIKwYBBQUHMAKUWh0dHA6Ly90cy13MmszLWFjcy50c3dlYi5j
aXNjb3R5
b20vQ2VydeVucm9sbC9UUy1XMksZLUFDUy5UU1dlYi5jaXNjb3R5b3R5b3R5
Q0ExLmNy
dDAhBgkrBgEEAYI3FAIEFB4SAFCAZQBIAFMAZQByAHYAZQByMAwGA1Ud
EwEB/wQC
MAAwEwYDVR0lBAwwCgYIKwYBBQUHAWEdQYJKoZIhvcNAQEFBQADggEB
AIqCaA9G
+8h+3IS8rfVAGzcWAEVRXCyBlx0Npr/jlocGJ7QbQxkjKEswXq/O2xDB
7wXQaGph
zRq4dxAL111JkIjhfeQY+7VSkz1GEpuBnENTohdhtz5vBjGlcROXIs8
+3Ghg8hy
```



```
YZZEM73e8EC0sEMedFb+KYpAFy3PPy4l8EHe4MJbdjUp/b901516IzQP
5151YB0y
NSLsYWqjkCBg+aUO+WPFk4jICr2XUOK74oWTPFNpfv2x4VFI/Mpcs87y
chngKB+8
rPHChSsZsw9upzPEH2L/O34wm/dpuLuHirrwWnF1zCnqfcyHcETieZtS
tlnwLpsc 1L5nuPsd8MaexBc= -----END CERTIFICATE----- quit
INFO: Certificate successfully imported
CiscoASA(config)#
```

## [Etapa 7. 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 VPN > o IKE > o > Add das políticas** a fim criar uma política de ISAKMP 65535 segundo as indicações desta imagem.
2. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.
3. Escolha a **configuração > o VPN > o IPsec > transformam o >Add dos grupos** a fim criar uma transformação ajustada (*myset*) segundo as indicações desta imagem:
4. Clique a **APROVAÇÃO**, e **aplique-a** então
5. Escolha a **configuração > o >Add VPN > de IPsec > de regras do IPsec** a fim criar um crypto map com a política dinâmica da prioridade 10 segundo as indicações desta imagem:
6. Clique a **APROVAÇÃO**, e **aplique-a** então
7. Escolha a **configuração > o VPN > a Política interna de grupo do > Add da política do general > do grupo** a fim criar uma política **Defaultgroup** do grupo segundo as indicações destas imagens.
8. Clique a **APROVAÇÃO**, e **aplique-a** então
9. Escolha a **configuração > o VPN > o gerenciamento de endereços IP > das associações IP > Add** a fim configurar o vpnpool do conjunto de endereços para que os usuários de cliente VPN sejam atribuídos dinamicamente.
10. Clique a **APROVAÇÃO**, e **aplique-a** então
11. Escolha a **configuração > o > Add VPN > de general > de usuários** a fim criar um **vpnuser** da conta de usuário para o acesso de cliente VPN.
12. Adicionar este usuário a **DefaultRAGroup**.
13. Clique a **APROVAÇÃO**, e **aplique-a** então
14. Edite o **DefaultRAGroup** como descrito neste procedimento: Escolha a **configuração > o VPN > o general > o grupo de túneis > editam**. Escolha **Defaultgroup** da lista de drop-down da política do grupo. Escolha o **LOCAL** da lista de drop-down do grupo de Authentication Server. Escolha o **vpnpool** da lista de drop-down da atribuição de endereço de cliente.
15. Clique a **APROVAÇÃO**, e **aplique-a** então.

### 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 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

```

## [Sumário de configuração 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	908fad3b	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	cf0ea22	2992f463	9412b388
84bf8b33	bd9f589a	e7087262	a4472e69	775ab608	e5714857
4f887163	705220e3	aca870be	b107ab8d	73faf76d	b3550553
1a2b873f	156f9dff	5386c839	1380fda8	945a7f6c	c2e9d5c8
83e2e761	394dd4da	63eaeffc	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
b1eb2b35	0c469443	1455c210	db308bf0	a9805758	a878b82d
38c71426	afffd272	dd6d7564	1cbe4d95	b81c02b2	9b56ec2d
5a913a9f	9b95cafd	dfcf67	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	e4bf2b24	9bf0d7d1	99865cc4	94e5547c	f03e3d3e
3b766011	e94a3657	6cc35b92	860152d4	f06b2b15	df306433

```
c1bcc282 80558d70 d22d72e7 eed3195b d575dceb c0caa196
34f693ea f3beee4d aa2ef1c2 edba288f 3a678ecb 3809d0df
b1699c76 13018f9f 5e3dce95 efe6da93 f4cb3b00 102efa94
48a22fc4 7e342031 2406165e 39edc207 eddc6554 3fa9f396 ad
quit crypto isakmp enable outside crypto isakmp policy
65535 authentication rsa-sig encryption 3des hash md5
group 2 lifetime 86400 crypto isakmp identity auto
tunnel-group DefaultRAGroup general-attributes address-
pool vpnpool default-group-policy Defaultgroup tunnel-
group DefaultRAGroup ipsec-attributes trust-point CA1
telnet timeout 5 ssh timeout 5 console timeout 0 !
class-map inspection_default match default-inspection-
traffic ! ! policy-map type inspect dns preset_dns_map
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
preset_dns_map inspect ftp inspect h323 h225 inspect
h323 ras inspect netbios inspect rsh inspect rtsp
inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
policy global_policy global prompt hostname context
Cryptochecksum:e150bc8bab11b41525784f68d88c69b0 : end
CiscoASA#
```

## Configuração de cliente de VPN

Termine estas etapas a fim configurar o cliente VPN:

1. Selecione 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 instalá-lo no Cisco VPN Client:Entre ao server 172.16.5.1 de CA com os credantials do usuário fornecidos ao vpnuser.**Nota:** Certifique-se de você mandar 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**, e selecione então o botão de rádio de **Base64** a fim especificar o método de codificação.Clique o **certificado de CA da transferência**.Salvar o certificado de CA a seu computador com o nome **certnew.cer**. À revelia, o arquivo salvar a **C:\Program Files\Cisco sistemas \ cliente VPN**.No cliente VPN, clique a aba dos **Certificados**, e escolha então a **importação**.Clique a **importação** do botão de rádio do **arquivo**, e clique-a então **consultam** a fim importar o certificado de CA dos sistemas de **C:\Program Files\Cisco** do lugar armazenado **\ cliente VPN**.Clique a **importação**.Uma caixa de diálogo parece que indica que o certificado esteve importado com sucesso.Os certificados de CA CA1 aparecem na aba dos **Certificados**.**Nota:** Certifique-se que a opção dos **Certificados da mostra CA/RA** está selecionada; se não, os certificados de CA não aparecerão 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 **sim** para continuar.Clique em **Instalar este certificado**.Clique **sim** para continuar.Você deve receber a mensagem instalada certificado segundo as indicações desta imagem:Retire e relance então o cliente VPN a fim permitir que o certificado de identidade instalado apareça na aba dos **Certificados** do cliente VPN segundo as indicações desta imagem:
4. Termine estas etapas a fim criar uma entrada de conexão (**vpnuser**):Clique a aba das entradas de conexão, e clique então **novo**.Incorpore o endereço IP de **Um ou Mais**

Servidores Cisco ICM NT do peer remoto (roteável) ao campo do host. Selecione o botão de rádio do **certificado de autenticação**, e escolha o certificado de identidade da lista de drop-down. Clique em Salvar.

5. Clique em Conectar.

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

7. O cliente VPN conecta com o ASA segundo as indicações desta imagem:

## Verificar

No ASA você pode usar 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.

- **mostre o ponto confiável cripto Ca** — Os indicadores configuraram pontos

```
CiscoASA#show crypto ca trustpoints Trustpoint CA1: Subject Name: cn=CA1 dc=TSWeb dc=cisco dc=com Serial Number: 7099f1994764e09c4651da80a16b749c Certificate configured.
```

- **mostre o certificado Ca cripto** — Indica todos os Certificados instalados no

```
CiscoASA#show crypto ca certificates Certificate Status: Available Certificate Serial Number: 3f14b70b000000000001f 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.tsw eb.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 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.tsw eb.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
```

- **mostre crls criptos Ca** — Os indicadores puseram em esconderijo listas revogação de certificado (CRL).

- **rsa do mypubkey do show crypto key** — Indica todos os pares de chave de criptografia

```
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#
```

- **mostre isakmp cripto 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

- **mostre IPsec cripto sa** — Dislays 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 a OIT para exibir uma análise da saída do comando show.

## [Troubleshooting](#)

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estão aqui alguns possíveis erros que você pôde 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 vendedor da 3ª 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. Use 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:** Você pôde receber este erro no cliente VPN se um problema ocorre com os Certificados durante a autenticação. A fim resolver esta edição, use o **comando auto cripto da identidade do isakmp** na configuração ASA/PIX.

## [Informações Relacionadas](#)

- [Página de suporte adaptável da ferramenta de segurança de Cisco](#)
- [Página de Suporte do Cisco VPN Client](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [Referências do comando Cisco Secure PIX Firewall](#)
- [Avisos de campo de produto de segurança \(incluindo PIX\)](#)

- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)