Exemplo de configuração de L2TP sobre IPsec entre o concentrador do Windows 2000 e do VPN 3000 usando certificados digitais

Contents

Introduction

Este documento mostra o procedimento passo a passo usado para conectar a um VPN 3000 Concentrator a partir de um cliente Windows 2000 usando o cliente L2TP/IPSec incorporado. Supõe-se que você use certificados digitais (CA (Autoridade de Certificação) raiz independente sem o Protocolo de Registro de Certificado (CEP)) para autenticar sua conexão com o VPN Concentrator. Este documento usa o Microsoft Certificate Service para ilustração. Consulte o site da Microsoft para obter documentação sobre como configurá-lo.

Observação: este é apenas um exemplo porque a aparência das telas do Windows 2000 pode mudar.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento referem-se à série Cisco VPN 3000 Concentrator.

Objetivos

Neste procedimento, você concluirá estas etapas:

1. Obtenha um certificado raiz.
2. Obtenha um certificado de identidade para o cliente.
3. Crie uma conexão com o VPN 3000 com a ajuda do Network Connection Wizard.
4. Configurar o VPN 3000 Concentrator.

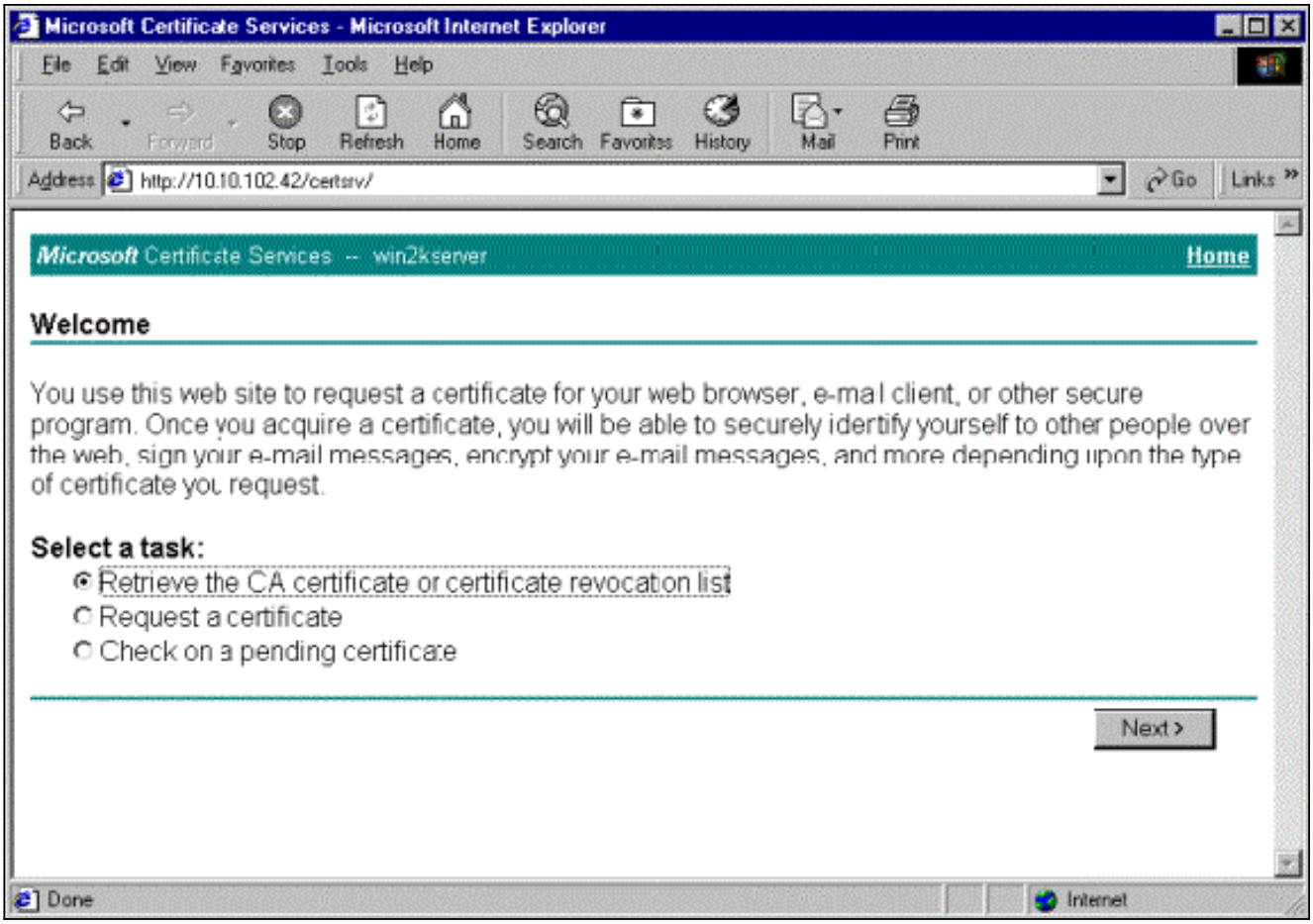
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

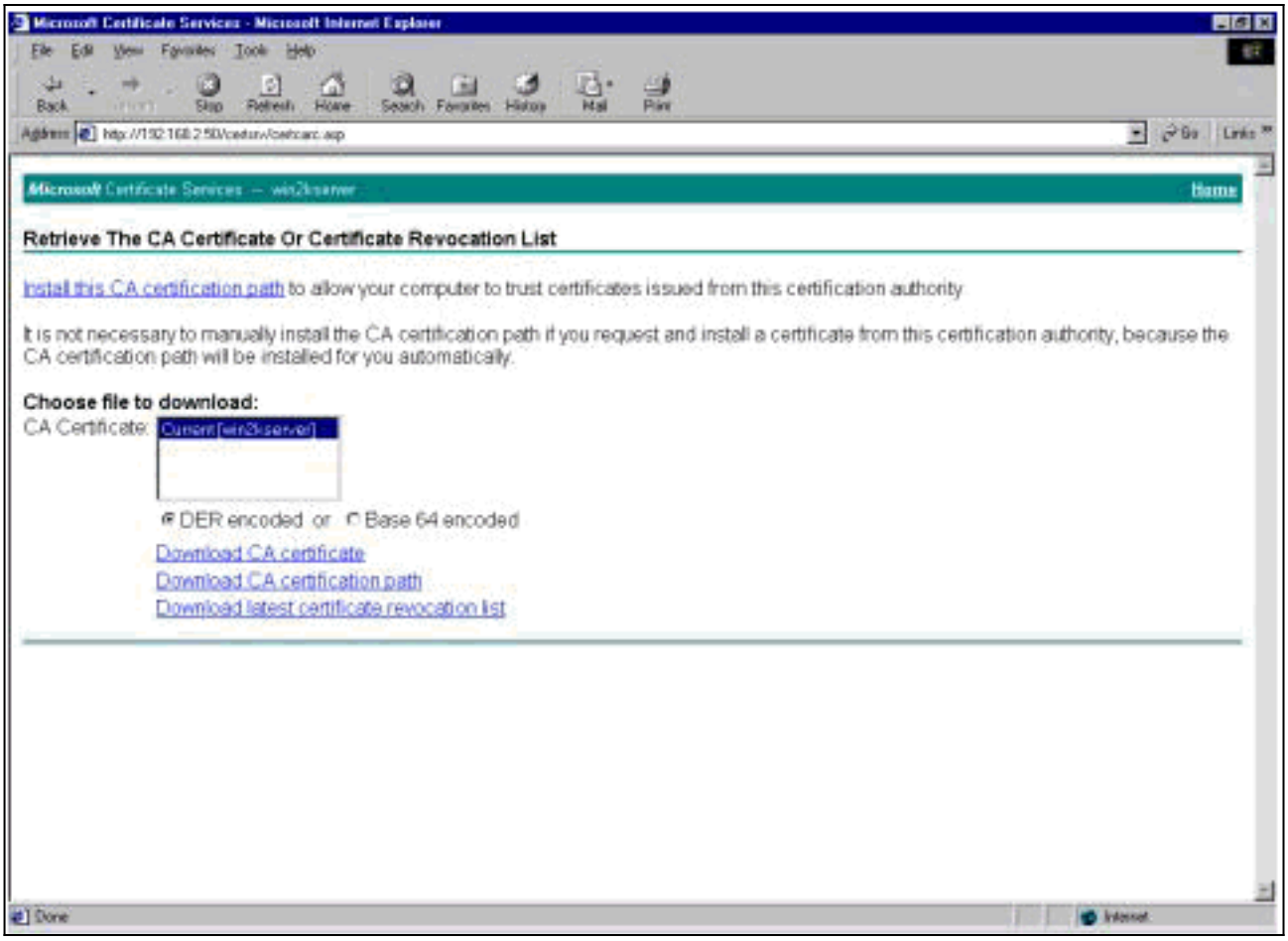
Obter um certificado raiz

Siga estas instruções para obter um certificado raiz:

1. Abra uma janela do navegador e digite o URL da Microsoft Certificate Authority (geralmente http://servername ou o endereço IP da CA/certsrv).A janela Bem-vindo para recuperações e solicitações de certificado é exibida.
2. Na janela Welcome (Bem-vindo), em Select a task (Selecionar uma tarefa), escolha **Retrieve the CA certificate or certificate revocation list (Recuperar o certificado CA ou a lista de revogação de certificados)** e clique em **Next**.



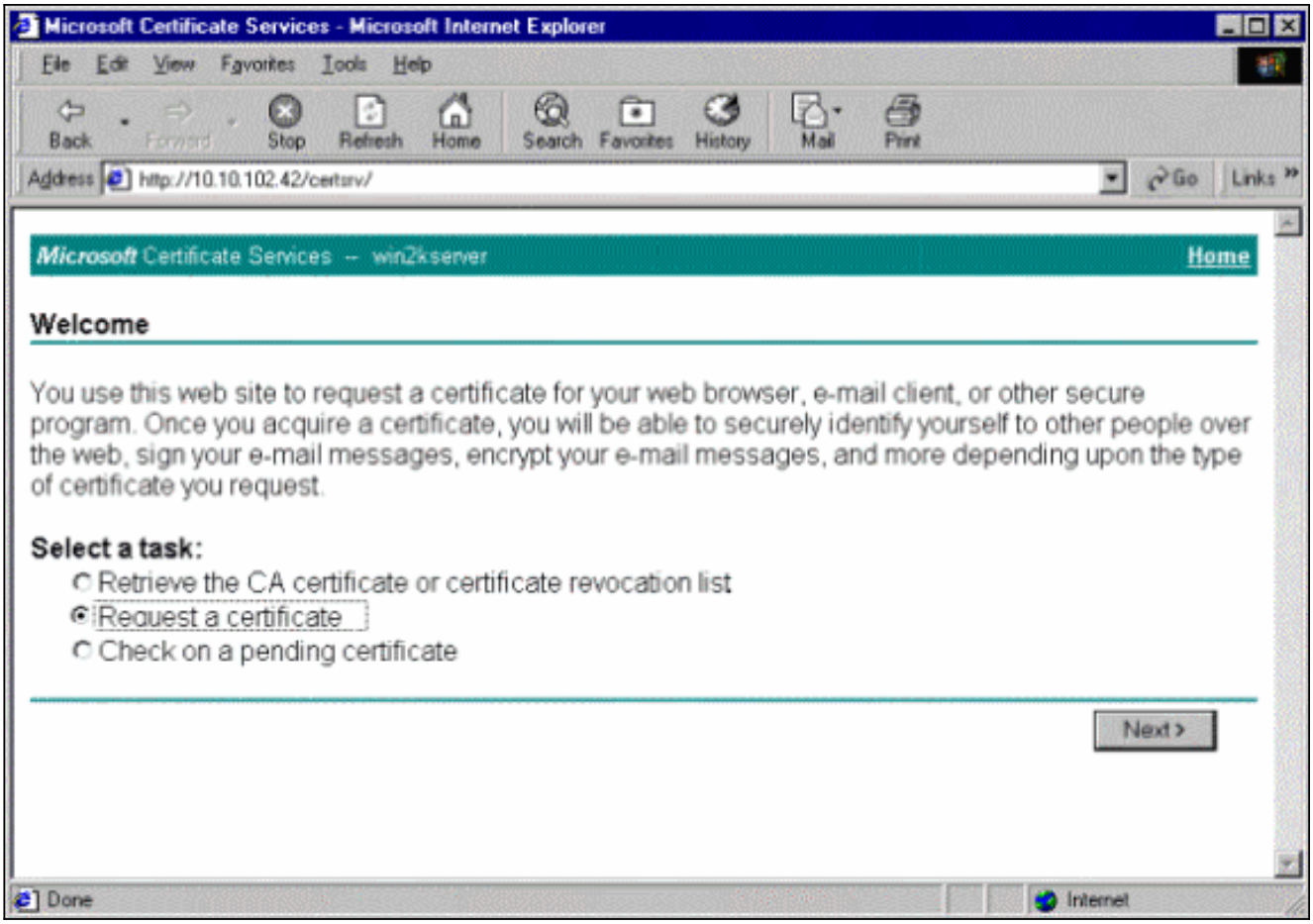
3. Na janela Recuperar o certificado CA ou lista de certificados revogados, clique em **Instalar este caminho de certificação CA** no canto esquerdo.Isso adiciona o certificado CA ao armazenamento de Autoridades de Certificação Raiz Confiáveis. Isso significa que todos os certificados emitidos por esta autoridade de certificação para este cliente são confiáveis.



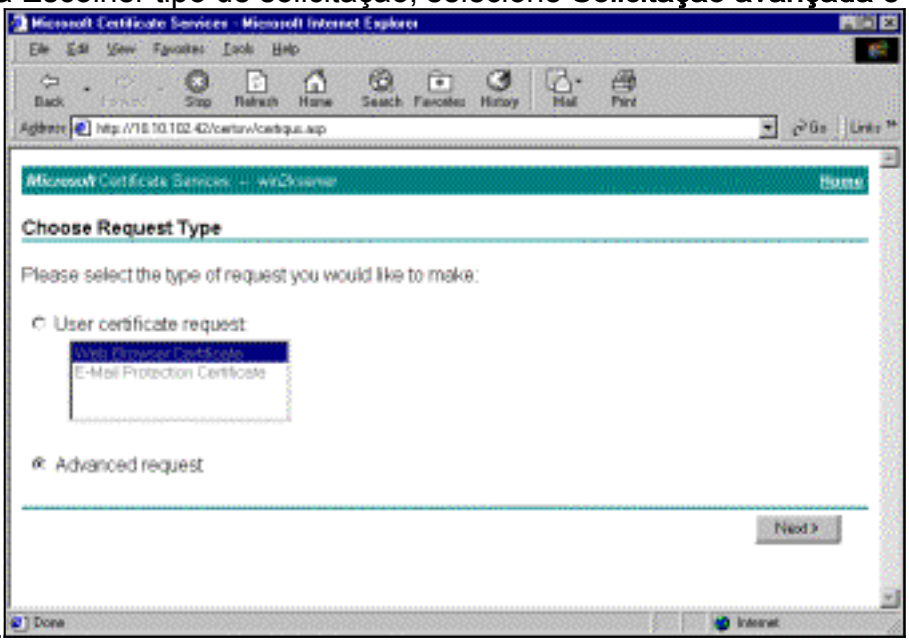
Obter um certificado de identidade para o cliente

Conclua estas etapas para obter um certificado de identidade para o cliente:

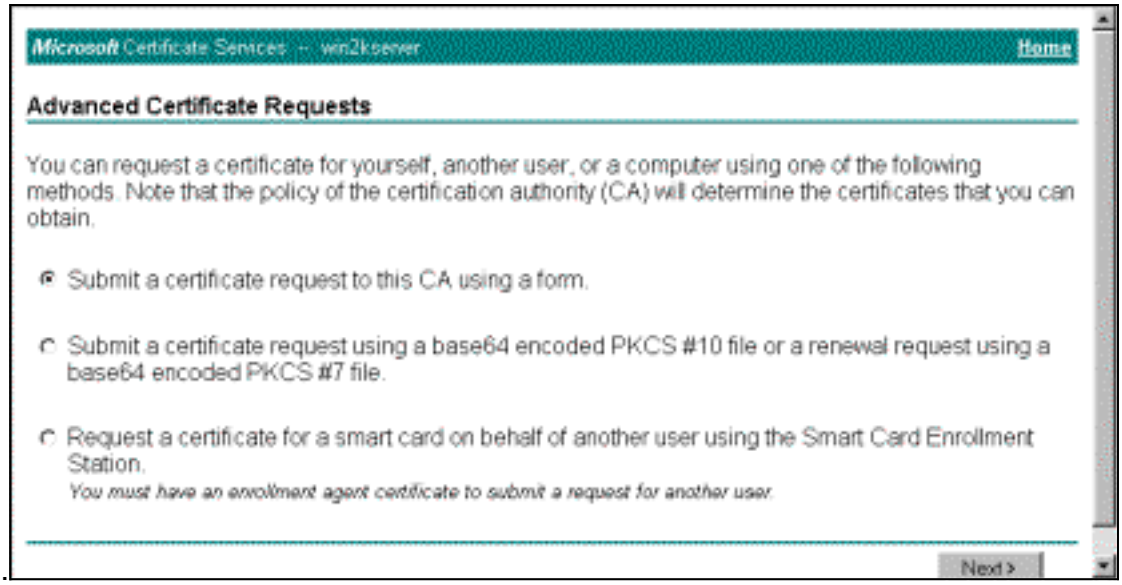
1. Abra uma janela do navegador e insira o URL da Microsoft Certificate Authority (geralmente http://servername ou o endereço IP da CA/certsrv).A janela Bem-vindo para recuperações e solicitações de certificado é exibida.
2. Na janela Bem-vindo, em Selecionar uma tarefa, escolha **Solicitar um certificado** e clique em **Próximo**.



3. Na janela Escolher tipo de solicitação, selecione **Solicitação avançada** e clique em **Próximo**.

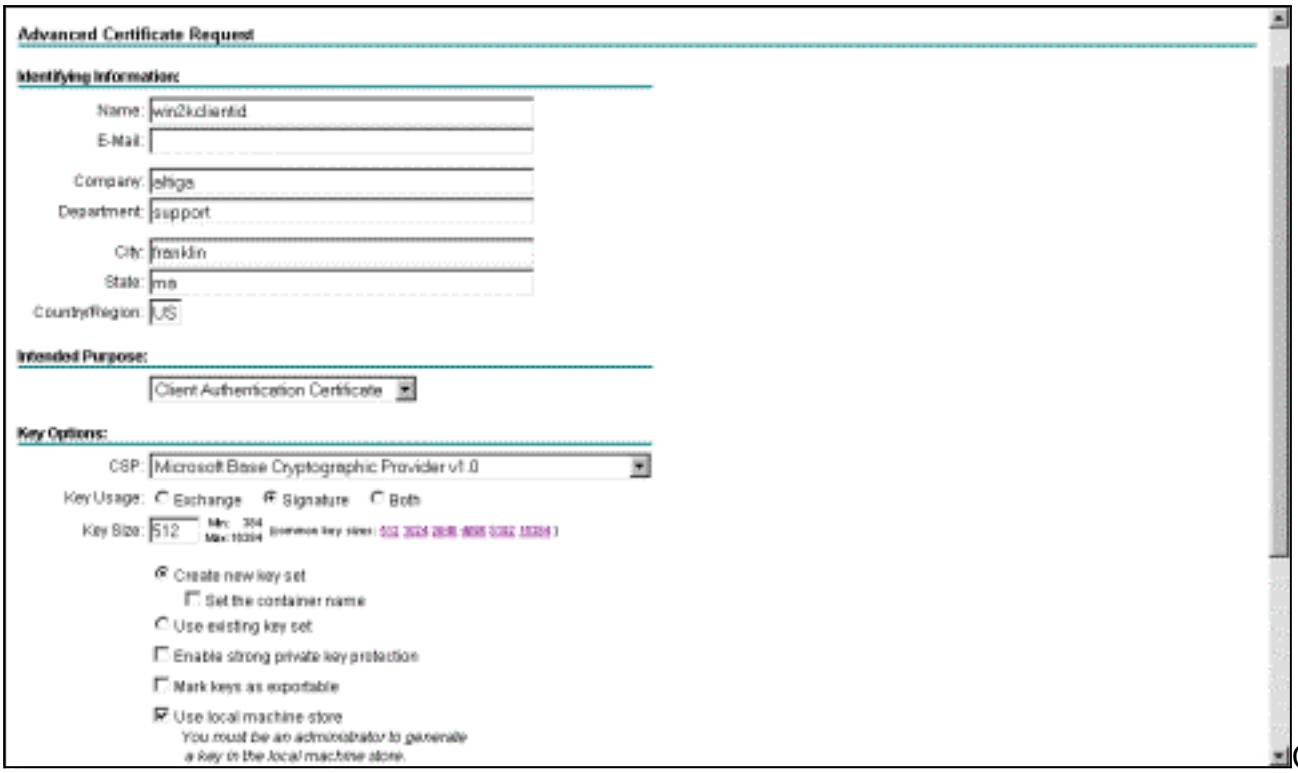


4. Na janela Solicitações avançadas de certificado, selecione **Submeter uma solicitação de certificado a esta CA usando um**



form.

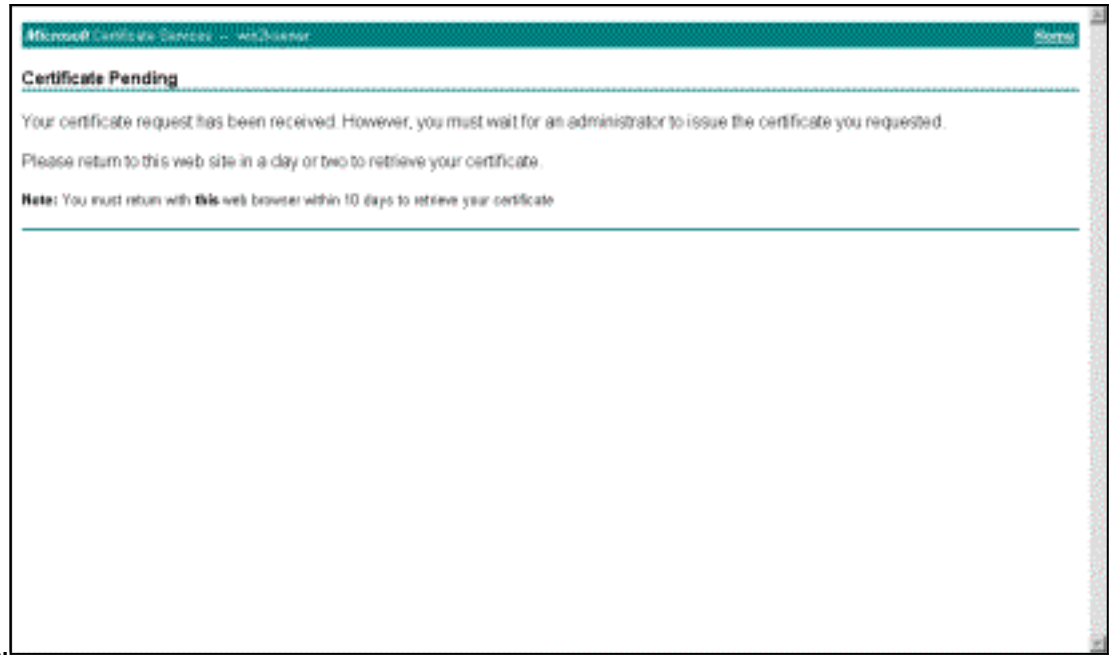
5. Preencha os campos conforme neste exemplo.O valor para Departamento (unidade organizacional) precisa corresponder ao grupo configurado no VPN Concentrator. Não especifique um tamanho de chave maior que 1024. Certifique-se de marcar a caixa de seleção **Usar armazenamento da máquina local**. Quando você finalizar, clique em Next.



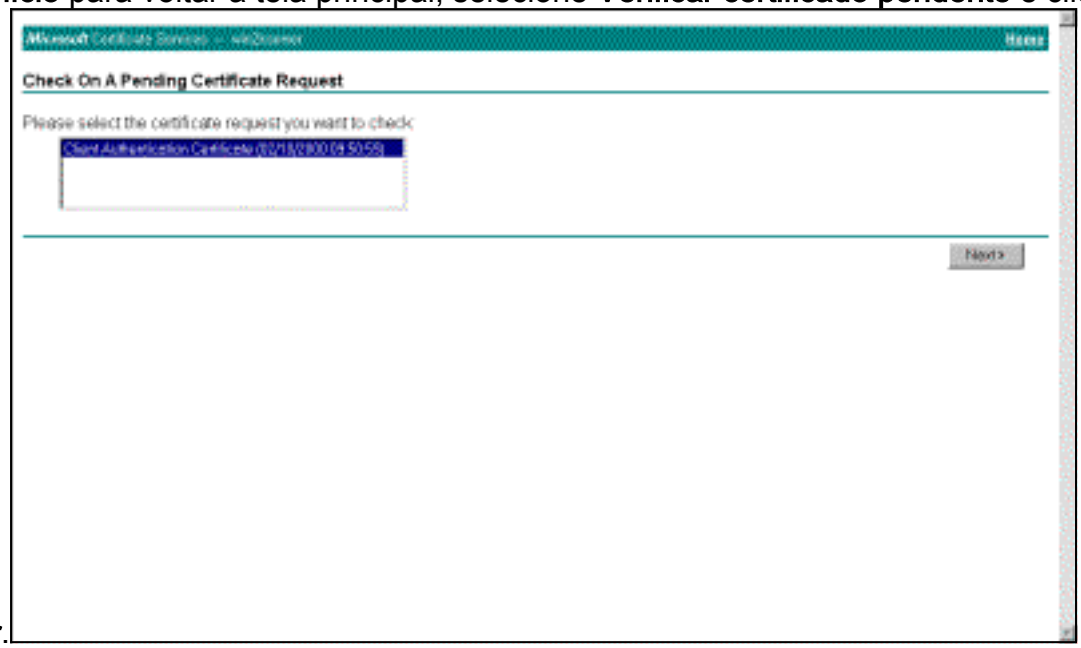
C

om base em como o servidor CA é configurado, essa janela às vezes é exibida. Em caso afirmativo, entre em contato com o administrador da

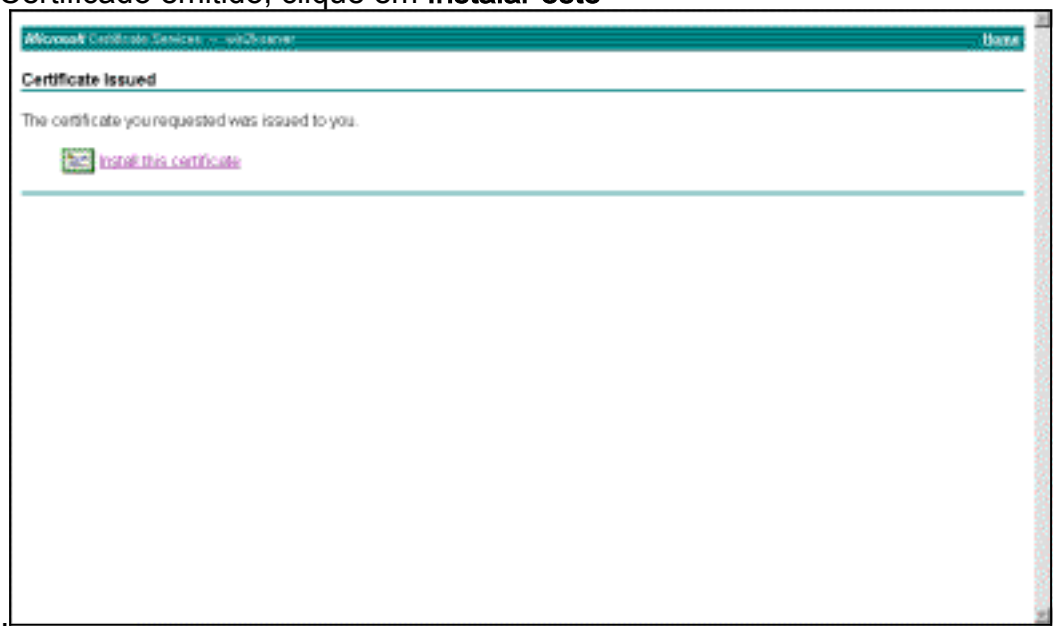
CA.



6. Clique em **Início** para voltar à tela principal, selecione **Verificar certificado pendente** e clique em **Avançar**.



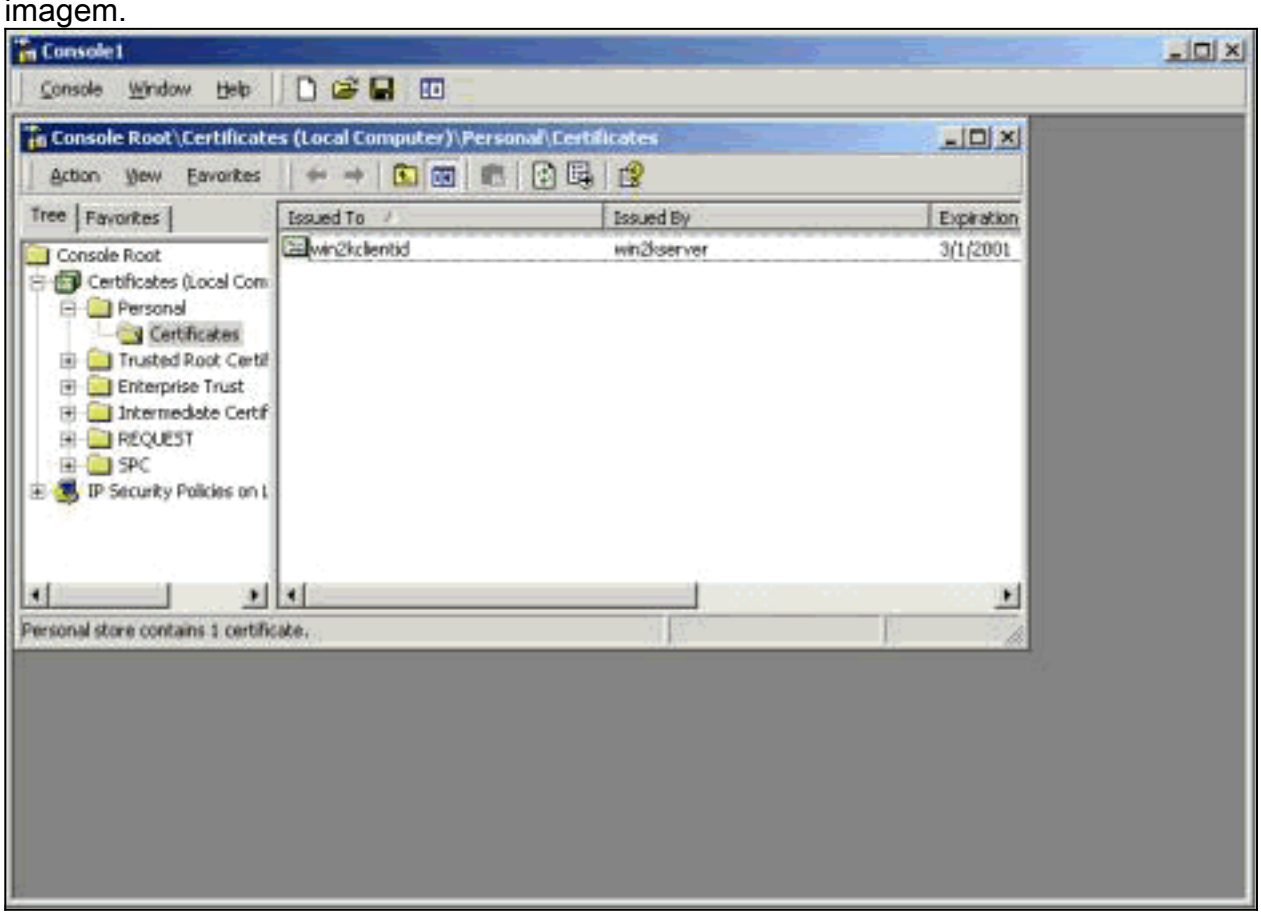
7. Na janela Certificado emitido, clique em **Instalar este certificado**.



8. Para exibir o certificado do cliente, selecione **Start > Run** e execute o Console de

Gerenciamento Microsoft (MMC).

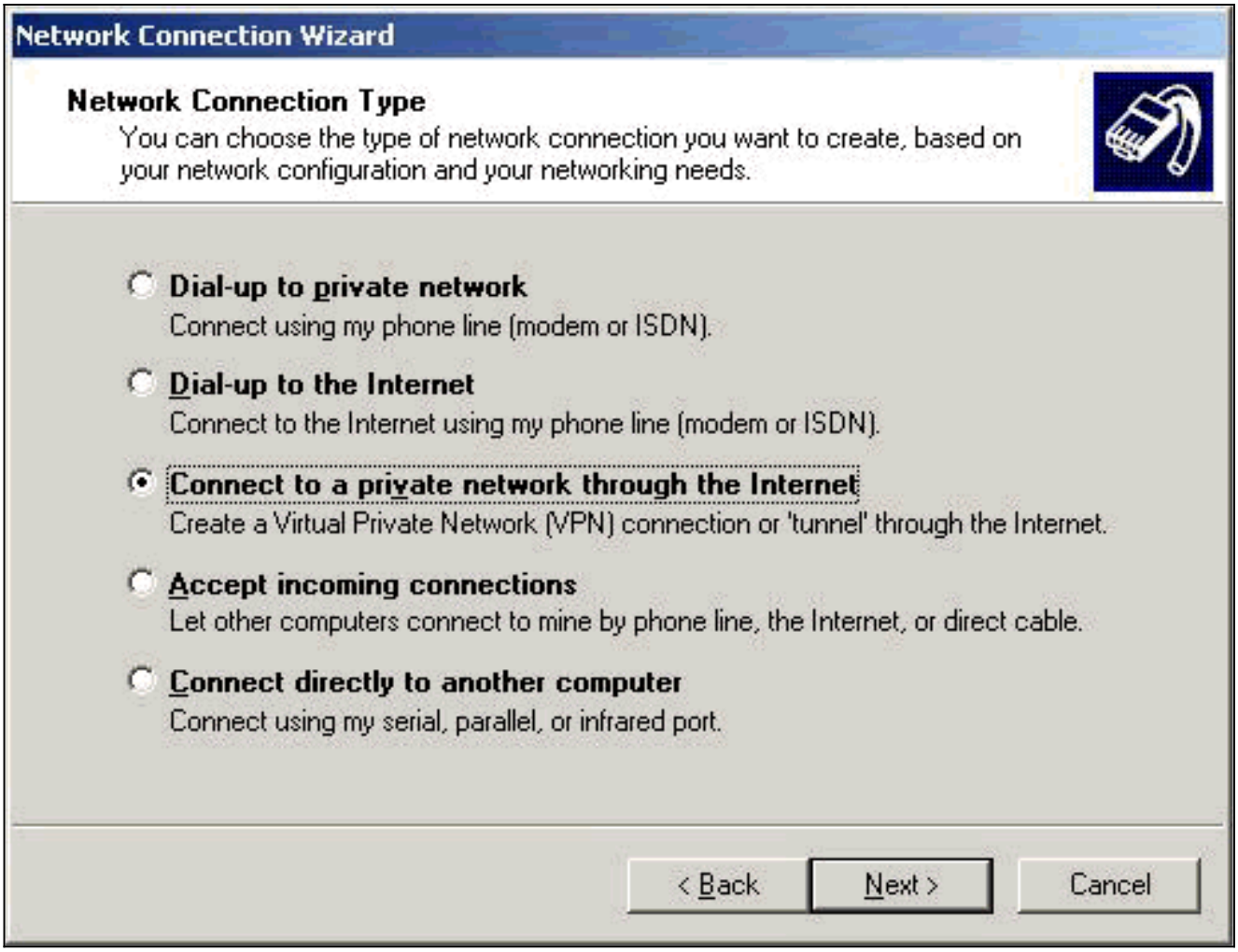
9. Clique em **Console** e escolha **Adicionar/remover snap-in**.
10. Clique em **Add** e escolha **Certificate** na lista.
11. Quando for exibida uma janela perguntando o escopo do certificado, escolha **Conta do Computador**.
12. Verifique se o certificado do servidor de CA está localizado nas Autoridades de Certificação Raiz Confiáveis. Verifique também se você tem um certificado selecionando **Raiz do Console > Certificado (Computador Local) > Pessoal > Certificados**, como mostrado nesta imagem.



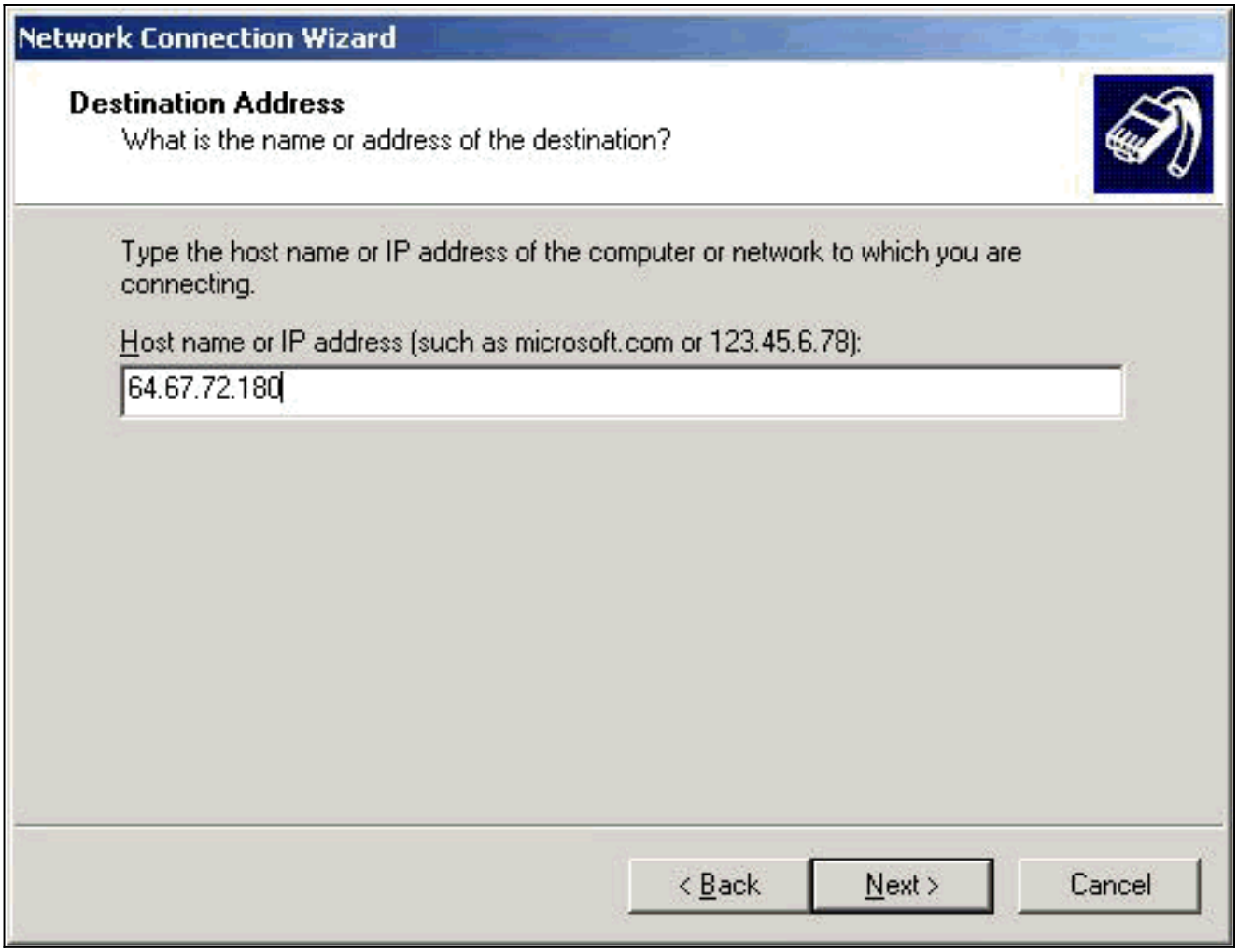
Crie uma conexão com o VPN 3000 usando o assistente de conexão de rede

Conclua este procedimento para criar uma conexão com o VPN 3000 com a ajuda do assistente de conexão de rede:

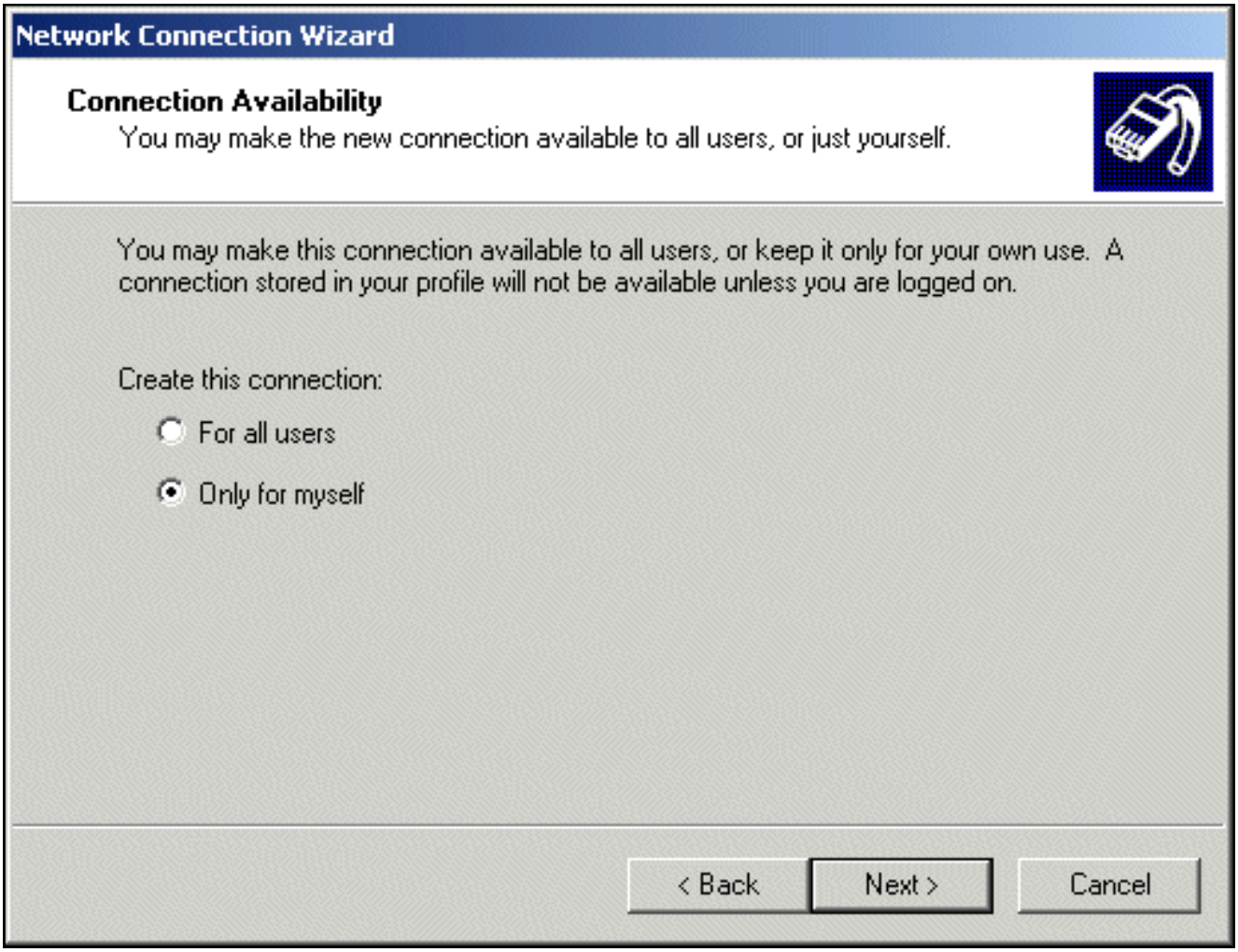
1. Clique com o botão direito do mouse em **Meus locais de rede**, escolha **Propriedades** e clique em **Fazer nova conexão**.
2. Na janela Tipo de conexão de rede, escolha **Conectar a uma rede privada pela Internet** e clique em
Avançar.



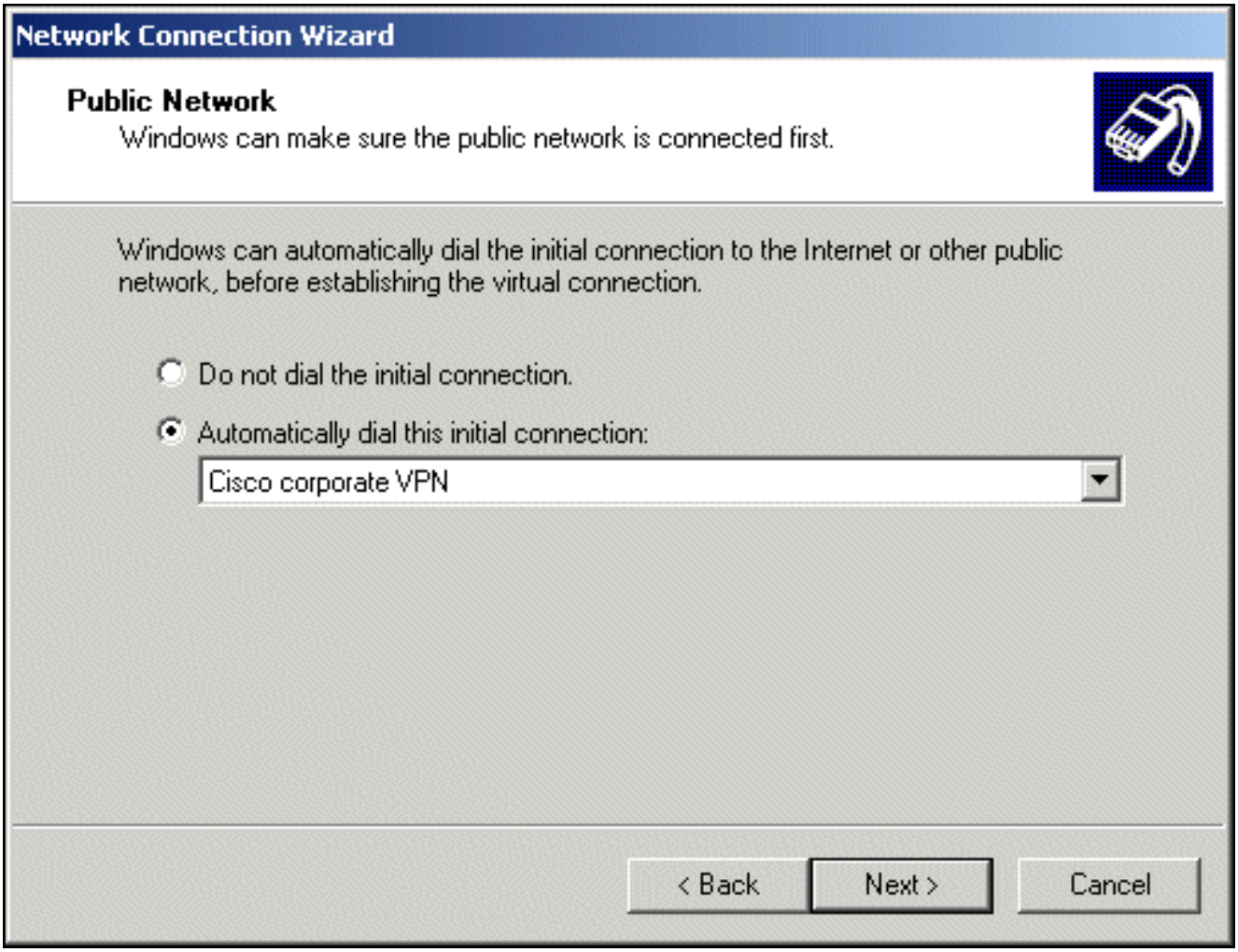
3. Insira o nome do host ou o endereço IP da interface pública do VPN Concentrator e clique em
Next.



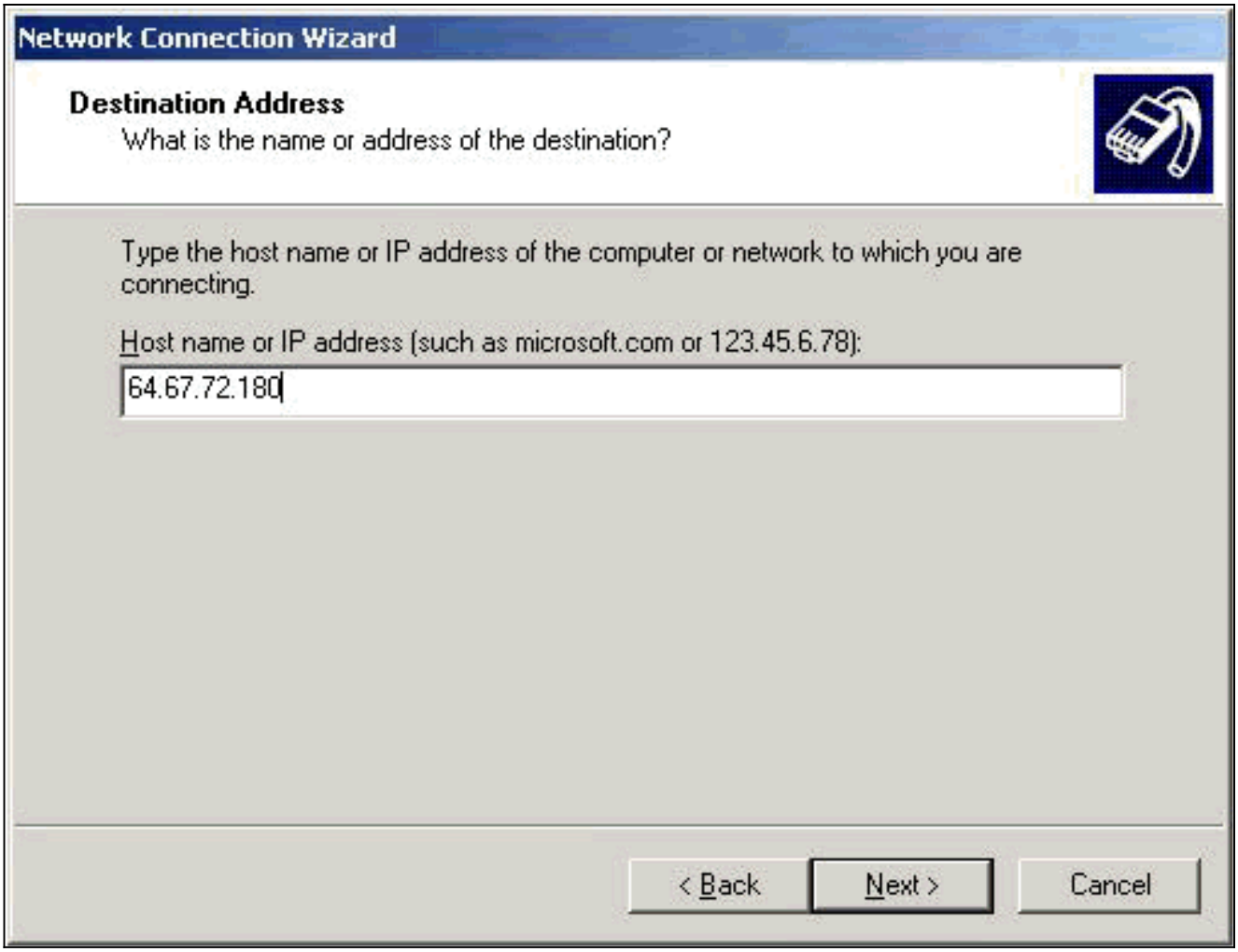
4. Na janela Disponibilidade da conexão, selecione **Somente para mim** e clique em **Próximo**.



5. Na janela Rede pública, selecione se deseja discar a conexão inicial (a conta do ISP) automaticamente.

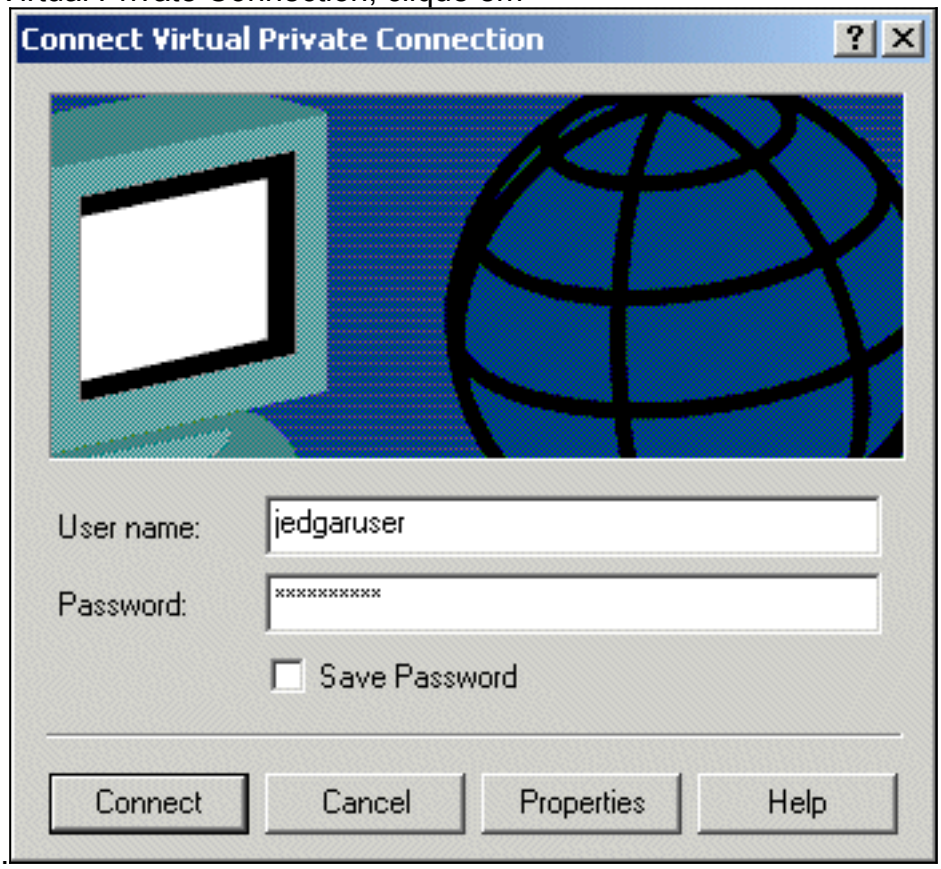


6. Na tela Endereço de destino, digite o nome do host ou o endereço IP do VPN 3000 Concentrator e clique em
Avançar.

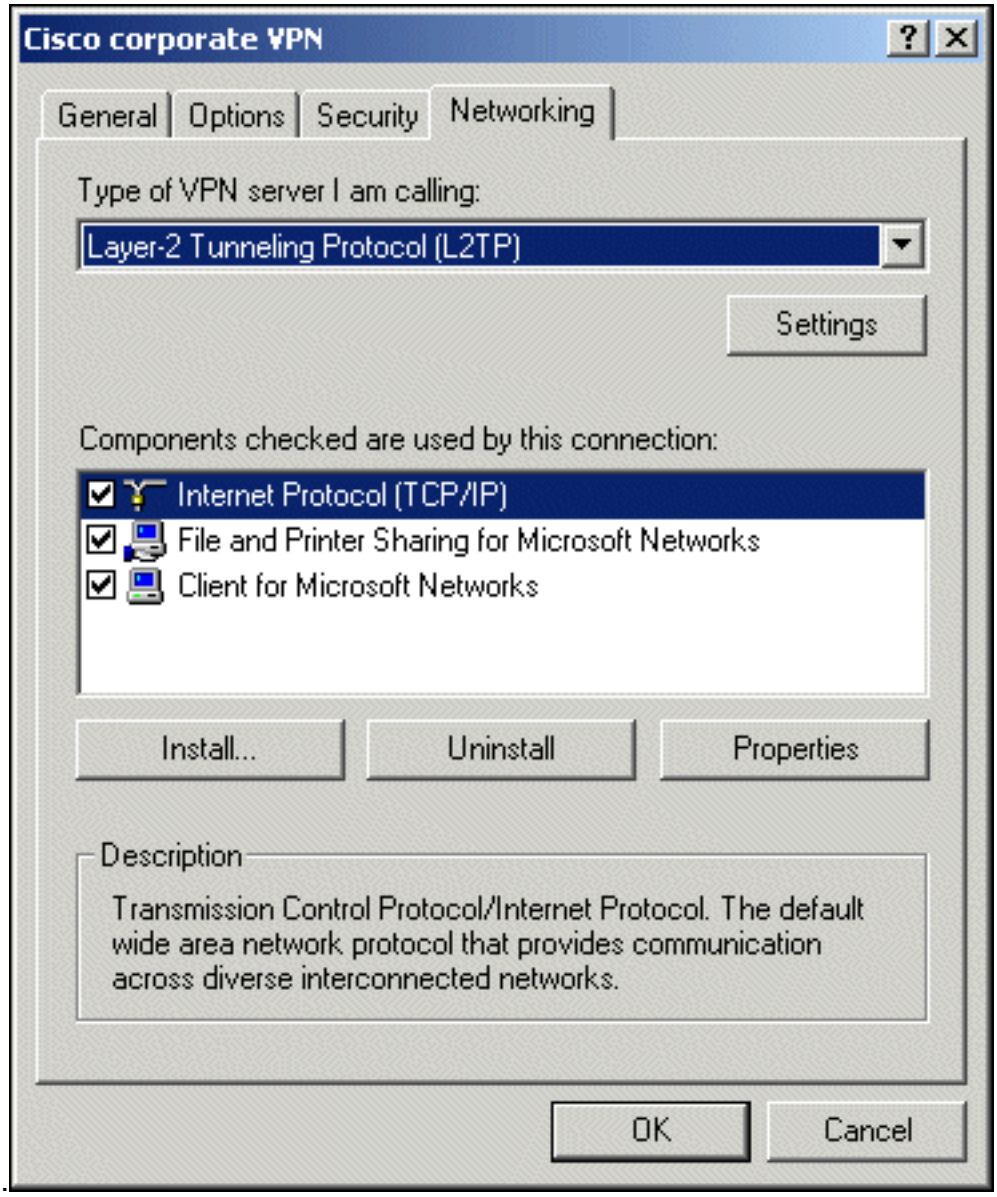


7. Na janela Network Connection Wizard, digite um nome para a conexão e clique em **Finish**.Neste exemplo, o nome da conexão é "Cisco Corporate VPN".

8. Na janela Virtual Private Connection, clique em **Properties**.

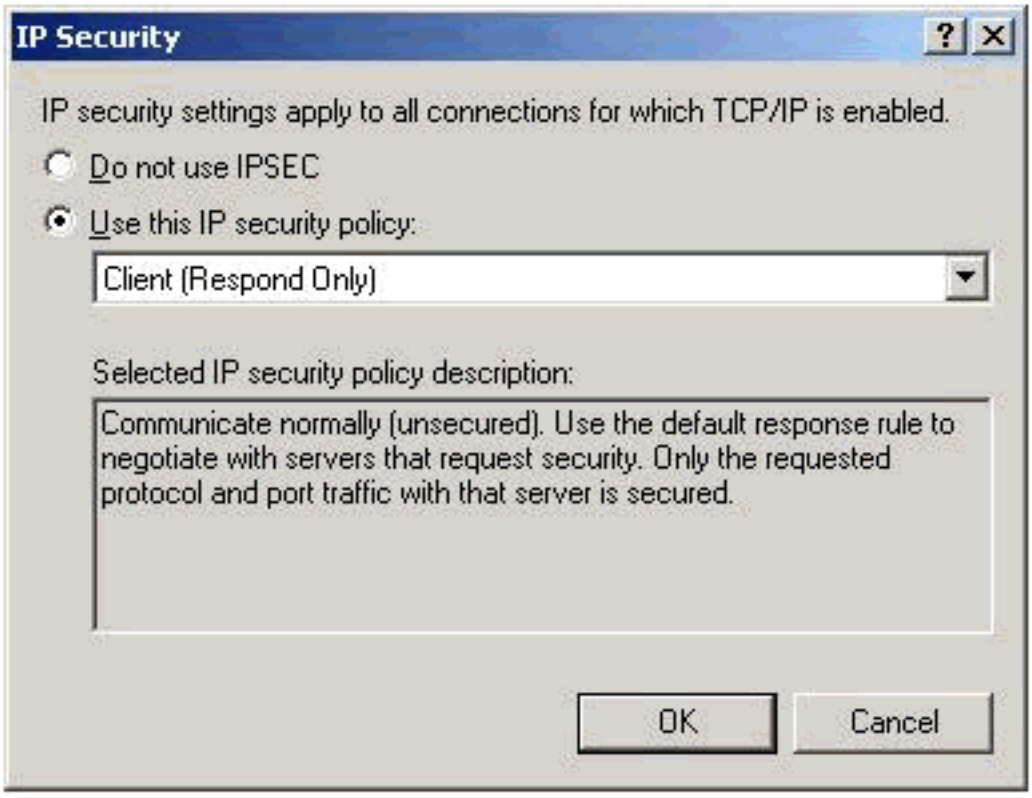


9. Na janela Propriedades, selecione a guia Rede.
10. Em Tipo de servidor VPN que estou chamando, escolha **L2TP** no menu suspenso, realce **Protocolo TCP/IP da Internet** e clique em



Propriedades.

11. Selecione **Avançado > Opções > Propriedades**.
12. Na janela IP Security, selecione **Use this IP security**



policy.

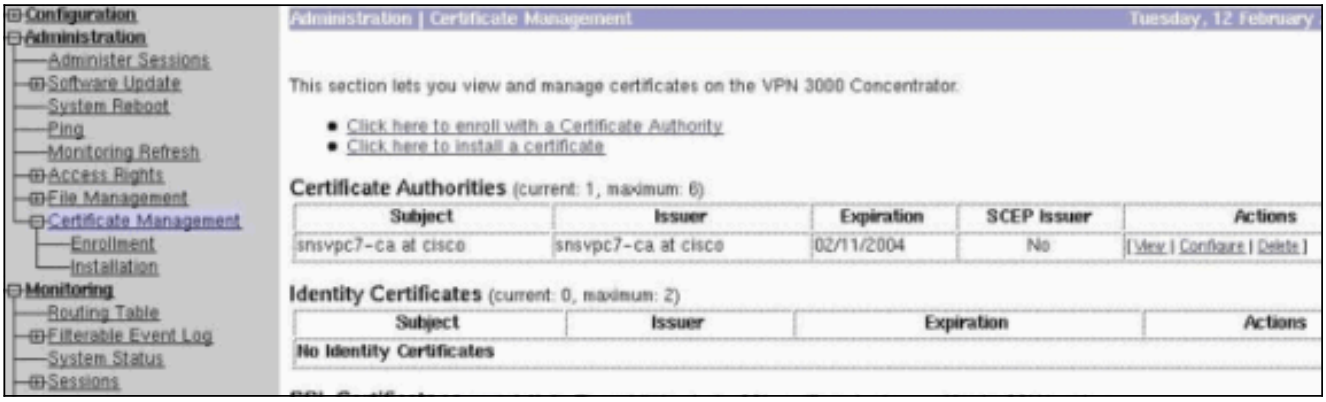
13. Escolha a política **Client (Respond Only)** no menu suspenso e clique em **OK** várias vezes até voltar à tela Connect.
14. Para iniciar uma conexão, insira seu nome de usuário e senha e clique em **Connect**.

Configurar o VPN 3000 Concentrator

Obter um certificado raiz

Conclua estes passos para obter um certificado raiz para o VPN 3000 Concentrator:

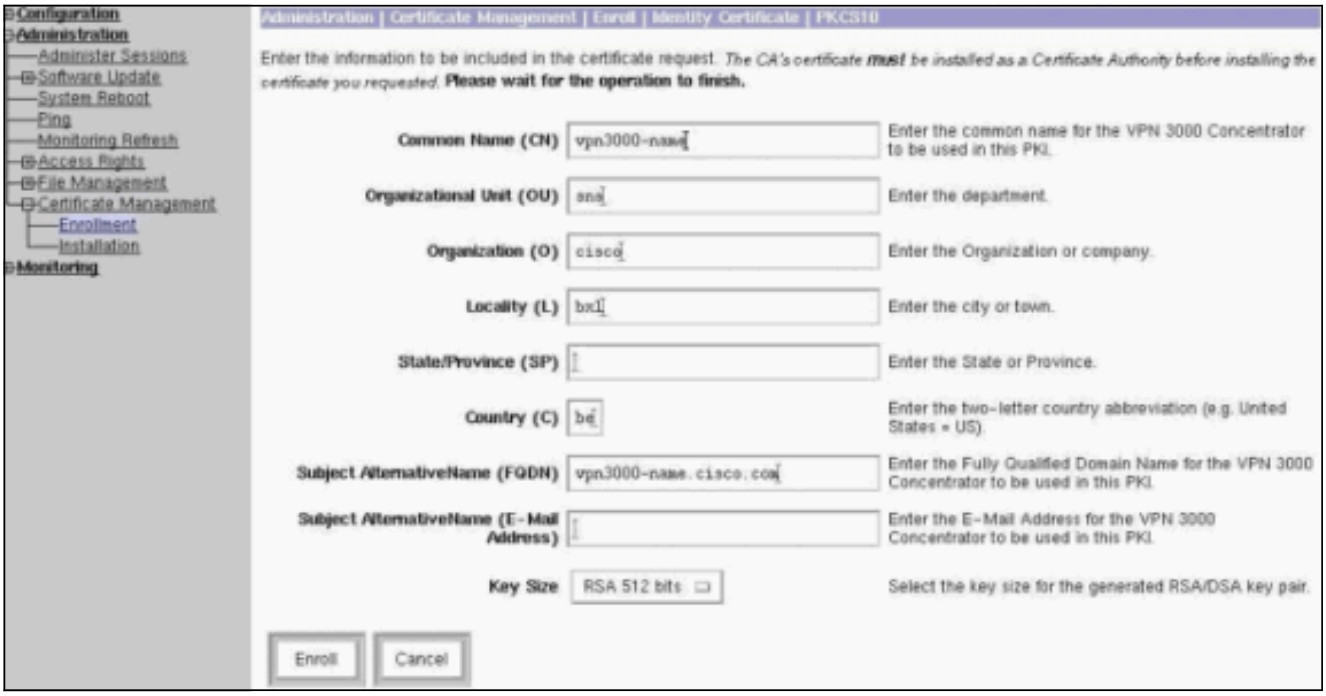
1. Aponte seu navegador para a CA (geralmente algo como http://ip_add_of_ca/certsrv/), **recupere o certificado CA ou a lista de certificados revogados** e clique em **Avançar**.
2. Clique em **Download CA certificate** e salve o arquivo em algum lugar do disco local.
3. No VPN 3000 Concentrator, selecione **Administration > Certificate Management** e clique em **Click here to install a certificate** e **Install CA Certificate**.
4. Clique em **Upload File from Workstation**.
5. Clique em **Browse** e selecione o arquivo de certificado CA que você acabou de baixar.
6. Realce o nome do arquivo e clique em **Instalar**.



Obtenha um certificado de identidade para o VPN 3000 Concentrator

Conclua estes passos para obter um certificado de identidade para o VPN 3000 Concentrator:

1. Selecione **ConfAdministration > Certificate Management > Enroll > Identity Certificate** e clique em **Enroll via PKCS10 Request (Manual)**. Preencha o formulário conforme mostrado aqui e clique em **Inscrever**.



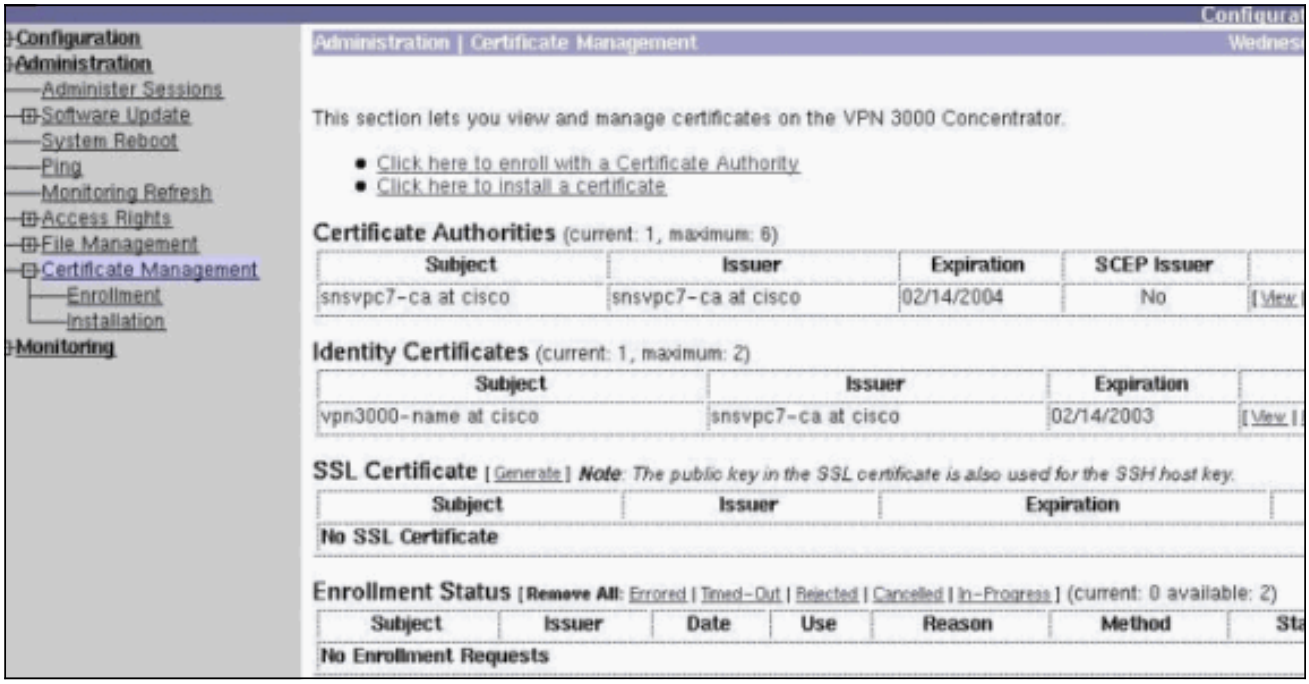
   Uma janela do navegador é exibida com a solicitação de certificado. Ele precisa conter texto semelhante a esta saída:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```

2. Aponte seu navegador para o servidor de CA, marque **Solicitar um certificado** e clique em **Avançar**.
3. Marque **Solicitação avançada**, clique em **Avançar** e selecione **Enviar uma solicitação de certificado usando um arquivo de #10 PKCS codificado na base64 ou uma solicitação de renovação usando um arquivo de #7 PKCS codificado na base64**.
4. Clique em Next. Recorte e cole o texto da solicitação de certificado mostrada anteriormente na área de texto. Clique em Submit.
5. Com base em como o servidor CA está configurado, você pode clicar em **Download CA certificate**. Ou assim que o certificado tiver sido emitido pela CA, volte para o servidor da CA e verifique **Check-on de um certificado pendente**.
6. Clique em **Avançar**, selecione sua solicitação e clique em **Avançar** novamente.
7. Clique em **Download CA certificate** e salve o arquivo no disco local.
8. No VPN 3000 Concentrator, selecione **Administration > Certificate Management > Install** e clique em **Install certificate obtain via enrollment**.Em seguida, você verá sua solicitação pendente com um status de "Em andamento", como nesta

imagem.

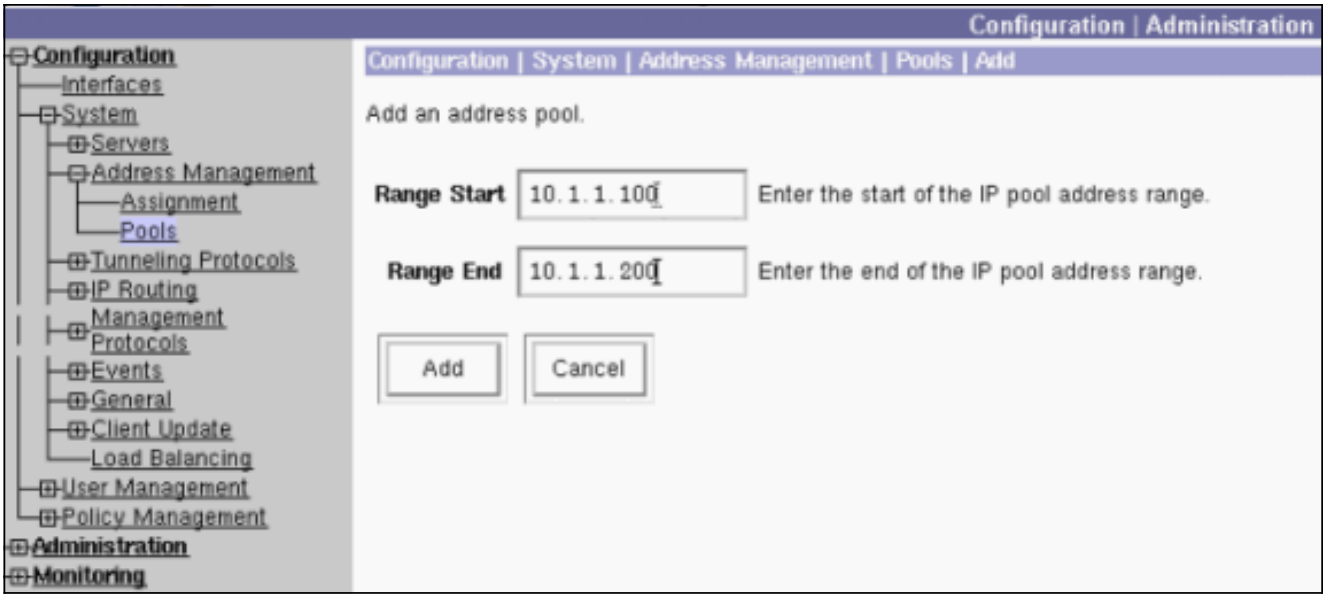
9. Clique em **Install**, seguido por **Upload File from Workstation**.
10. Clique em **Browse** e selecione o arquivo que contém o certificado emitido pela CA.
11. Realce o nome do arquivo e clique em **Instalar**.
12. Selecione **Administration > Certificate Management**. Uma tela semelhante a esta imagem é exibida.



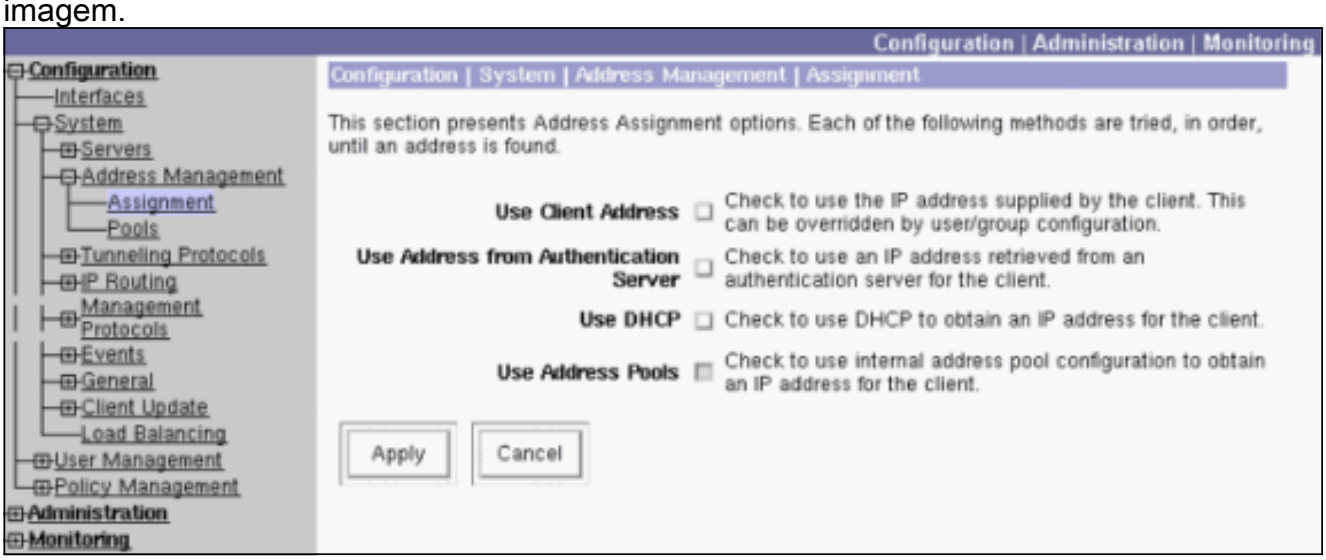
Configurar um pool para os clientes

Conclua este procedimento para configurar um pool para os clientes:

1. Para atribuir um intervalo disponível de endereços IP, aponte um navegador para a interface interna do VPN 3000 Concentrator e selecione **Configuration > System > Address Management > Pools > Add**.
2. Especifique um intervalo de endereços IP que não entrem em conflito com nenhum outro dispositivo na rede interna e clique em **Adicionar**.



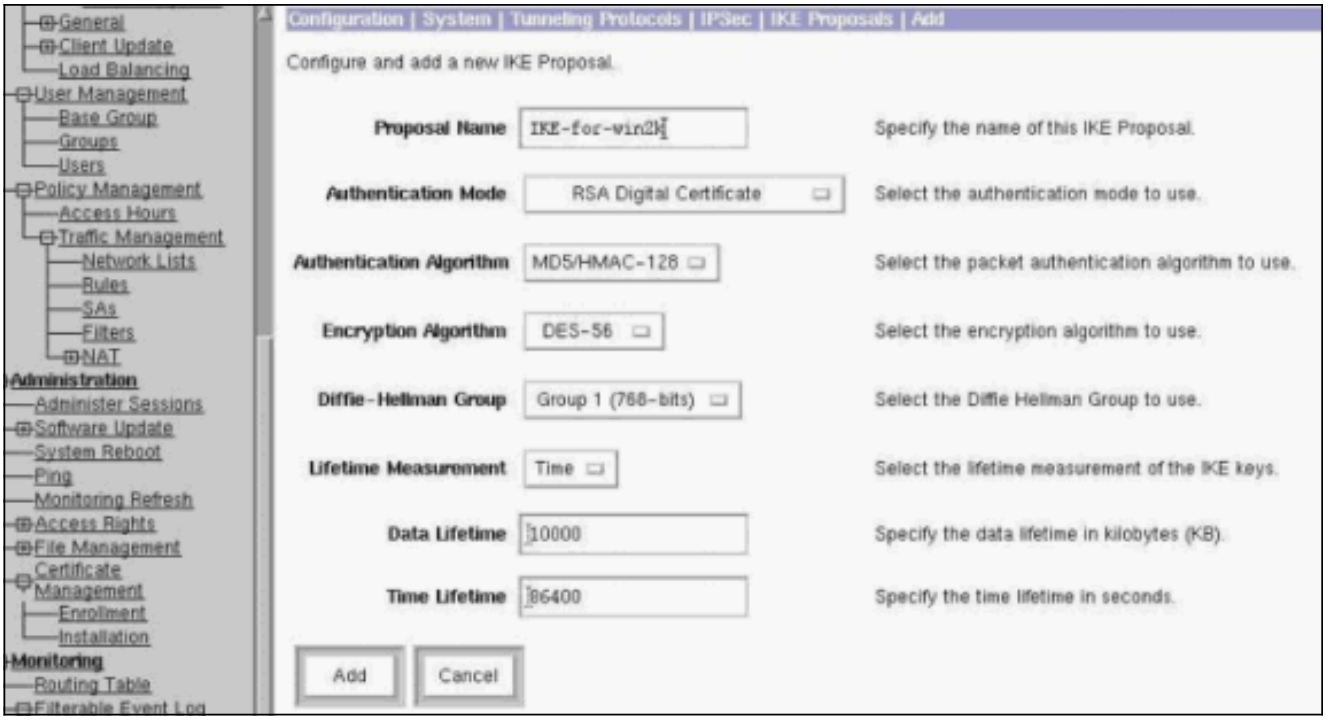
3. Para instruir o VPN 3000 Concentrator a usar o pool, selecione **Configuration > System > Address Management > Assignment**, marque a caixa **Use Address Pools** e clique em **Apply**, como nesta
imagem.



Configurar uma proposta de IKE

Conclua estas etapas para configurar uma proposta IKE:

1. Selecione **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals**, clique em **Add** e selecione os parâmetros, como mostrado nesta
imagem.



2. Clique em **Add**, realce a nova proposta na coluna direita e clique em **Ativate**.

Configurar a SA

Conclua este procedimento para configurar a Associação de Segurança (SA):

1. Selecione **Configuration > Policy Management > Traffic Management > SA** e clique em **ESP-L2TP-TRANSPORT**.Se essa SA não estiver disponível ou se você usá-la para alguma outra finalidade, crie uma nova SA semelhante a esta. Configurações diferentes para o SA são aceitáveis. Altere esse parâmetro com base na sua política de segurança.
2. Selecione o certificado digital configurado anteriormente no menu suspenso **Digital Certificate**. Selecione a proposta **IKE-for-win2k** Internet Key Exchange (IKE).**Observação:** isso não é obrigatório. Quando o cliente L2TP/IPSec se conecta ao VPN Concentrator, todas as propostas IKE configuradas na coluna ativa da página **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals** são tentadas na ordem.Esta imagem mostra a configuração necessária para a
SA:

Configurar o grupo e o usuário

Conclua este procedimento para configurar o Grupo e o Usuário:

1. Selecione **Configuration > User Management > Base Group**.
2. Na guia General (Geral), verifique se **L2TP over IPSec** está marcado.
3. Na guia IPSec, selecione **ESP-L2TP-TRANSPORT** SA.
4. Na guia PPTP/L2TP, desmarque todas as opções de **criptografia L2TP**.
5. Selecione **Configuration > User Management > Users** e clique em **Add**.
6. Digite o nome e a senha que você usa para se conectar do cliente Windows 2000. Certifique-se de selecionar **Grupo base** na Seleção de grupo.
7. Na guia General (Geral), verifique o protocolo de encapsulamento **L2TP over IPSec**.
8. Na guia IPSec, selecione **ESP-L2TP-TRANSPORT** SA.
9. Na guia PPTP/L2TP, desmarque todas as opções de **Criptografia L2TP** e clique em **Adicionar**.Agora você pode se conectar com a ajuda do L2TP/IPSec Windows 2000 Client.**Observação:** você optou por configurar o grupo base para aceitar a conexão L2TP/IPSec remota. Também é possível configurar um grupo que corresponda ao campo Unidade Organizacional (OU) do SA para aceitar a conexão de entrada. A configuração é idêntica.

Informações de debug

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7
```

```
271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
```

```
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE
```

```
429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4
```

```
454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED
```

```
474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!
```

```
496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76
```

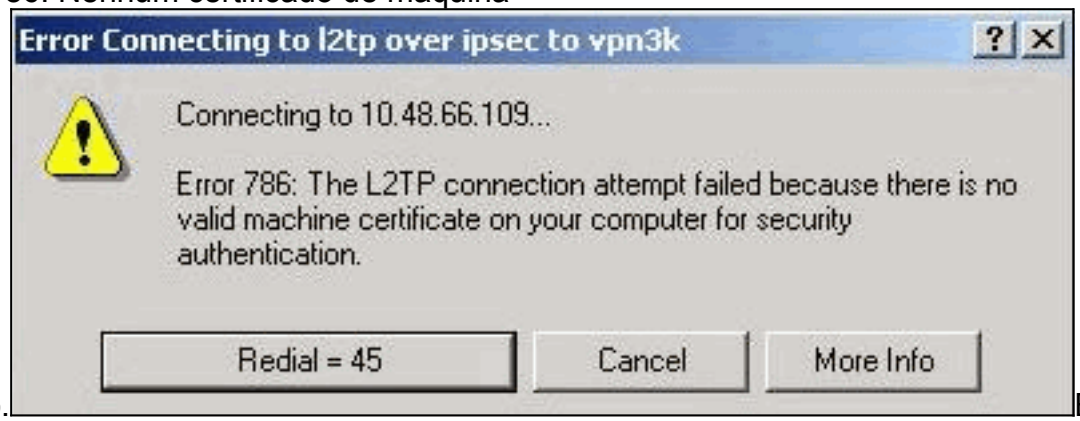
```
517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

Informações de solução de problemas

Esta seção ilustra alguns problemas comuns e os métodos de identificação e solução de problemas de cada um.

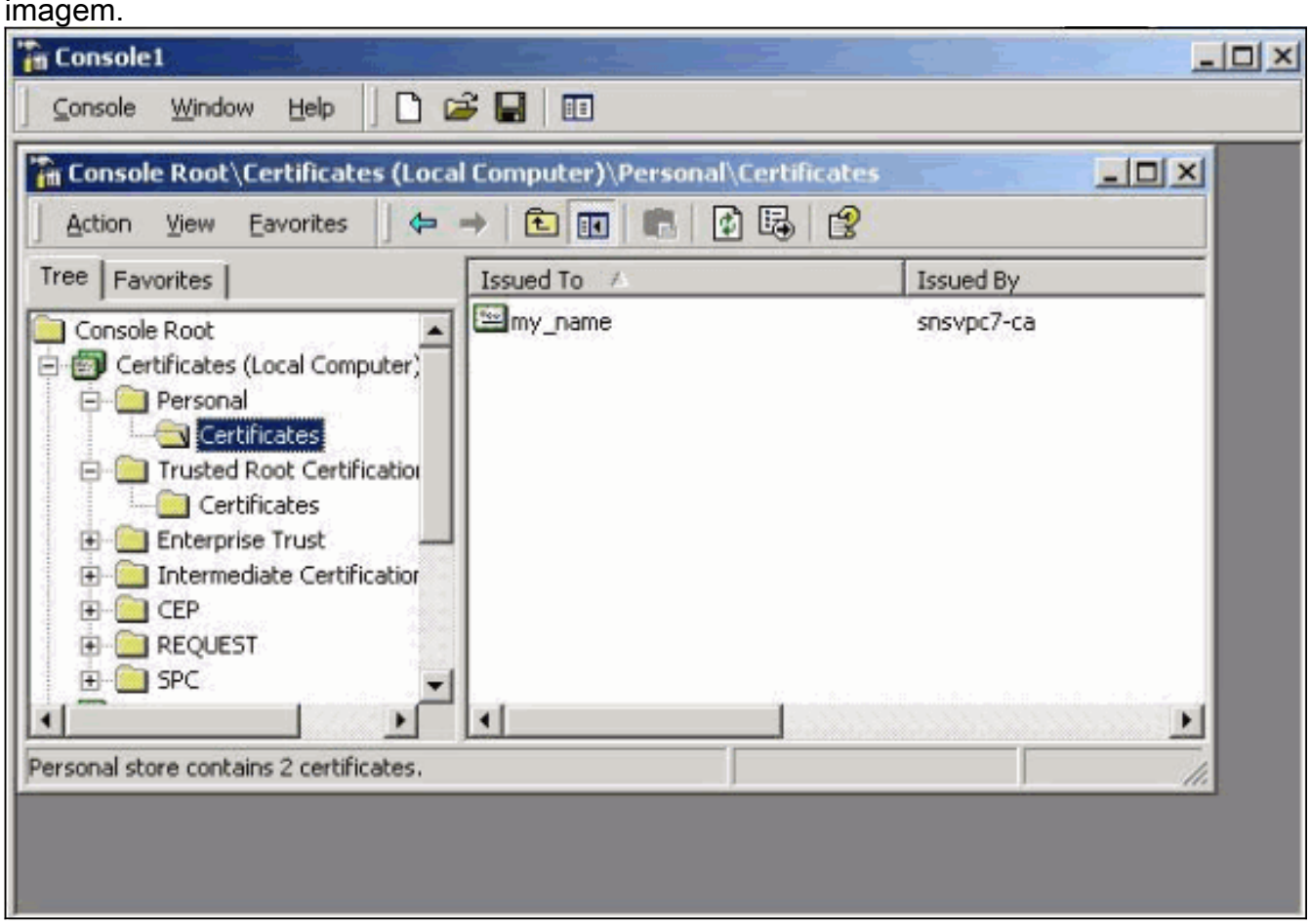
- Não é possível iniciar o servidor.

  Provavelmente, o serviço IPSec não foi iniciado. Selecione **Start > Programs > Administrative tools > Service** e verifique se o **serviço IPSec** está habilitado.
- Erro 786: Nenhum certificado de máquina válido.



  Este erro indica um problema com o certificado no computador local. Para examinar facilmente seu certificado, selecione **Start > Run** e execute o MMC. Clique em **Console** e escolha **Adicionar/remover snap-in**. Clique em **Add** e escolha **Certificate** na lista. Quando for exibida uma janela perguntando o escopo do certificado, escolha **Conta do Computador**.Agora você pode verificar se o certificado do servidor de CA está localizado nas **Autoridades de Certificação Raiz Confiáveis**. Você também pode verificar se tem um certificado selecionando

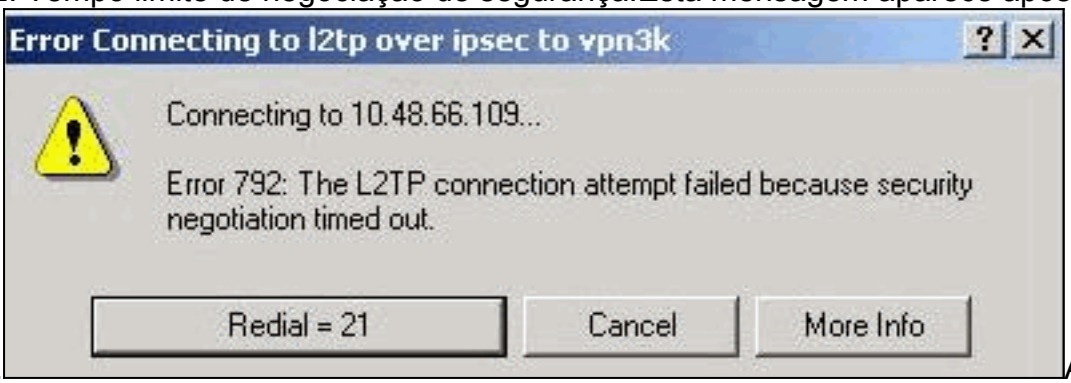
Raiz do Console > Certificado (Computador Local) > Pessoal > Certificados, como mostrado nesta
imagem.



Clique no **certificado**. Verifique se tudo está correto. Neste exemplo, há uma chave privada associada ao certificado. No entanto, este certificado expirou. Essa é a causa do

problema.

- Erro 792: Tempo limite de negociação de segurança.Esta mensagem aparece após um longo



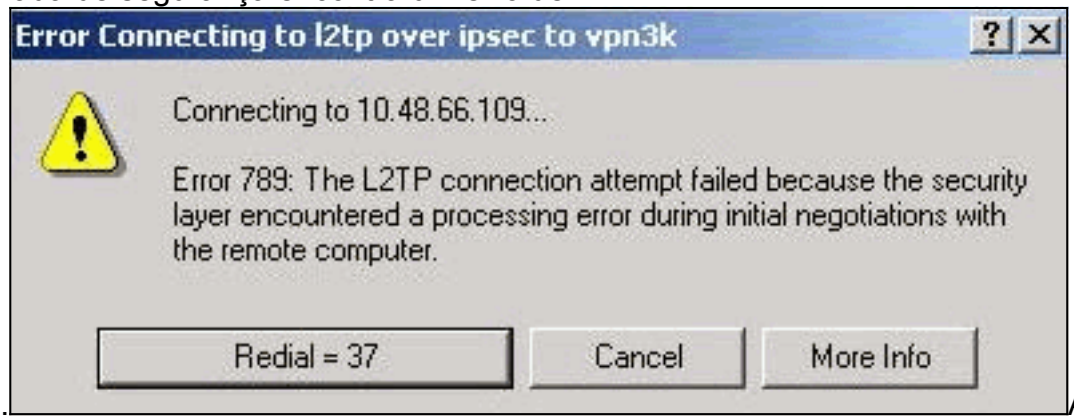
período.Ative as depurações relevantes conforme explicado nas Perguntas frequentes do Cisco VPN 3000 Concentrator. Leia-as. Você precisa ver algo semelhante a esta saída:

```
9337 02/15/2002 15:06:13.500 SEV=8 IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
```

```
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```

Isso indica que a proposta IKE não foi configurada corretamente. Verifique as informações da seção Configurando uma proposta IKE deste documento.

- Erro 789: A camada de segurança encontra um erro de processamento.



Ative as depurações relevantes conforme explicado nas Perguntas frequentes do Cisco VPN 3000 Concentrator. Leia-as. Você precisa ver algo semelhante a esta saída:

```
11315 02/15/2002 15:36:32.030 SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- Versão usadaSelecione **Monitoring > System Status** para exibir esta saída:

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB
```

Informações Relacionadas

- Negociação IPSec/suporte de produto de protocolos IKE
- Suporte Técnico - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.