

L2TP over IPsec tussen Windows 2000 en VPN 3000 Concentrator met behulp van digitaal certificaatconfiguratievoorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Doelstellingen](#)

[Conventies](#)

[Verkrijg een basiscertificaat](#)

[Een identiteitsbewijs voor de klant verkrijgen](#)

[Een verbinding met VPN 3000 maken met de wizard Netwerkverbinding](#)

[De VPN 3000 concentrator configureren](#)

[Verkrijg een basiscertificaat](#)

[Verkrijg een Identiteitscertificaat voor VPN 3000 Concentrator](#)

[Een pool voor de clients configureren](#)

[Een IKE-voorstel configureren](#)

[De SA configureren](#)

[De groep en gebruiker configureren](#)

[Debuginformatie](#)

[Informatie over probleemoplossing](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document toont de stapsgewijze procedure die wordt gebruikt om verbinding te maken met een VPN 3000 Concentrator vanuit een Windows 2000-client met behulp van de ingebouwde L2TP/IPSec-client. Er wordt aangenomen dat u digitale certificaten (stand-alone root Certification Authority (CA) zonder Certificate Enrollment Protocol (CEP)) gebruikt om uw verbinding met de VPN Concentrator te verifiëren. Dit document gebruikt de Microsoft Certificate Service ter illustratie. Raadpleeg de [Microsoft](#) -website voor documentatie over het configureren van de website.

Opmerking: dit is alleen een voorbeeld omdat het uiterlijk van de Windows 2000-schermen kan wijzigen.

[Voorwaarden](#)

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is voor de Cisco VPN 3000 Concentrator-reeks.

Doelstellingen

In deze procedure, voltooit u deze stappen:

1. Verkrijg een wortelcertificaat.
2. Verkrijg een identiteitsbewijs voor de klant.
3. Maak een verbinding met VPN 3000 met behulp van de wizard Netwerkverbinding.
4. Configureer de VPN 3000 Concentrator.

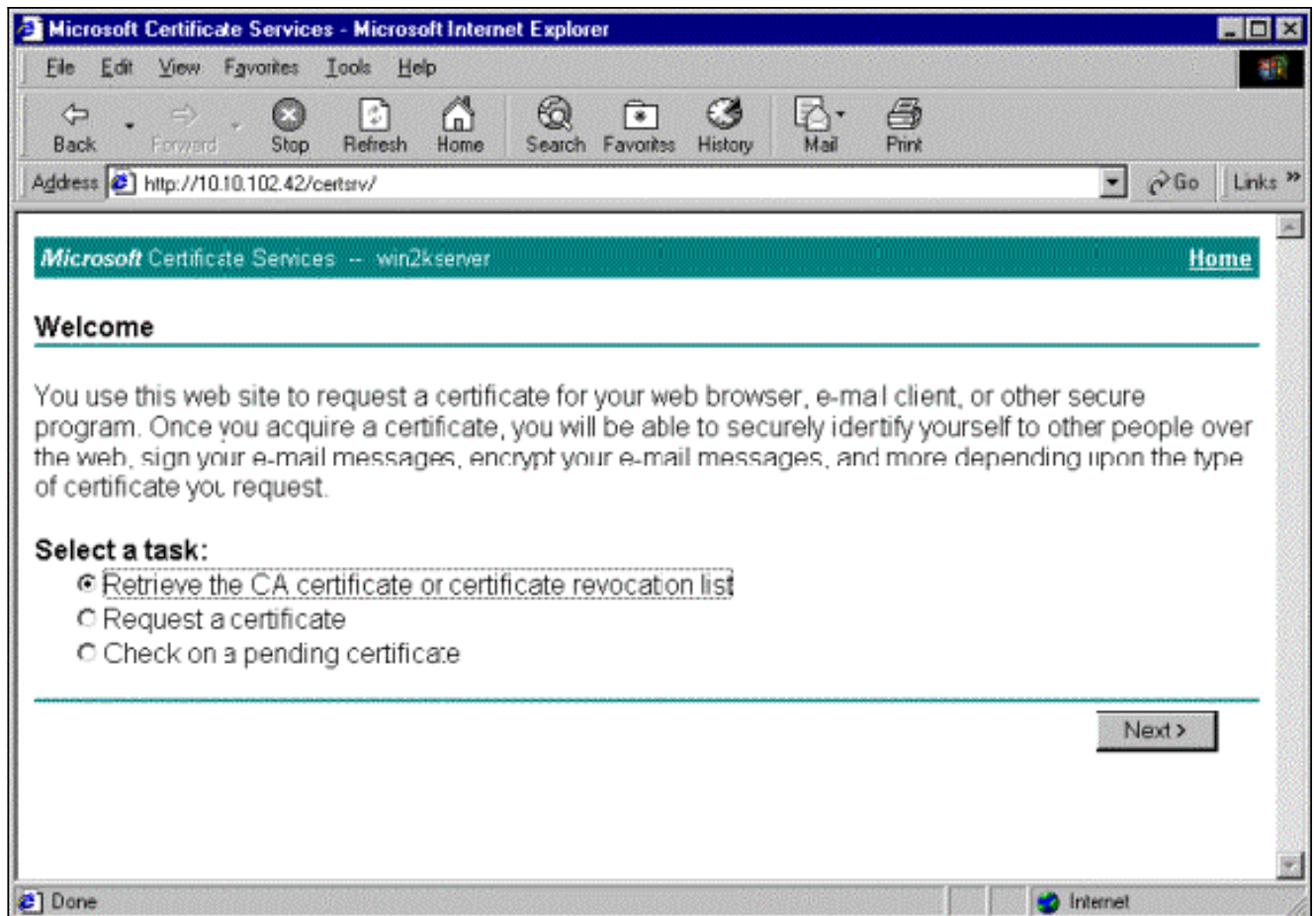
Conventies

Raadpleeg [Cisco Technical Tips Conventions](#) (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

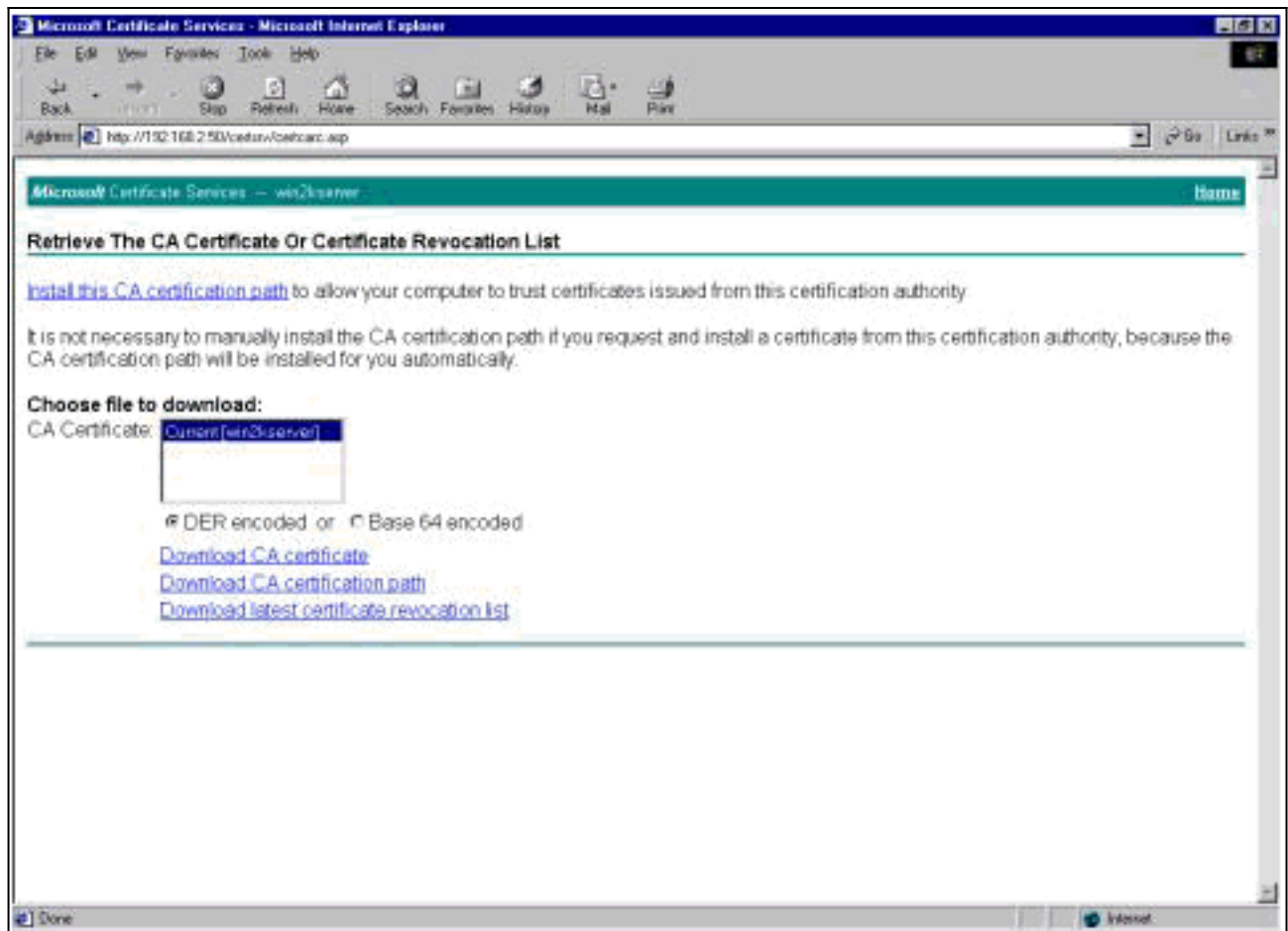
Verkrijg een basiscertificaat

Vul deze instructies in om een basiscertificaat te verkrijgen:

1. Open een browservenster en typ de URL voor de Microsoft Certificate Authority (meestal <http://servername> of het IP-adres van CA/certsrv). Het welkomsvenster voor het ophalen van certificaten en het weergeven van verzoeken.
2. Kies in het welkomsvenster onder **Selecteer een taak** de lijst met **CA-certificaten of certificaatintrekking ophalen** en klik op **Volgende**.



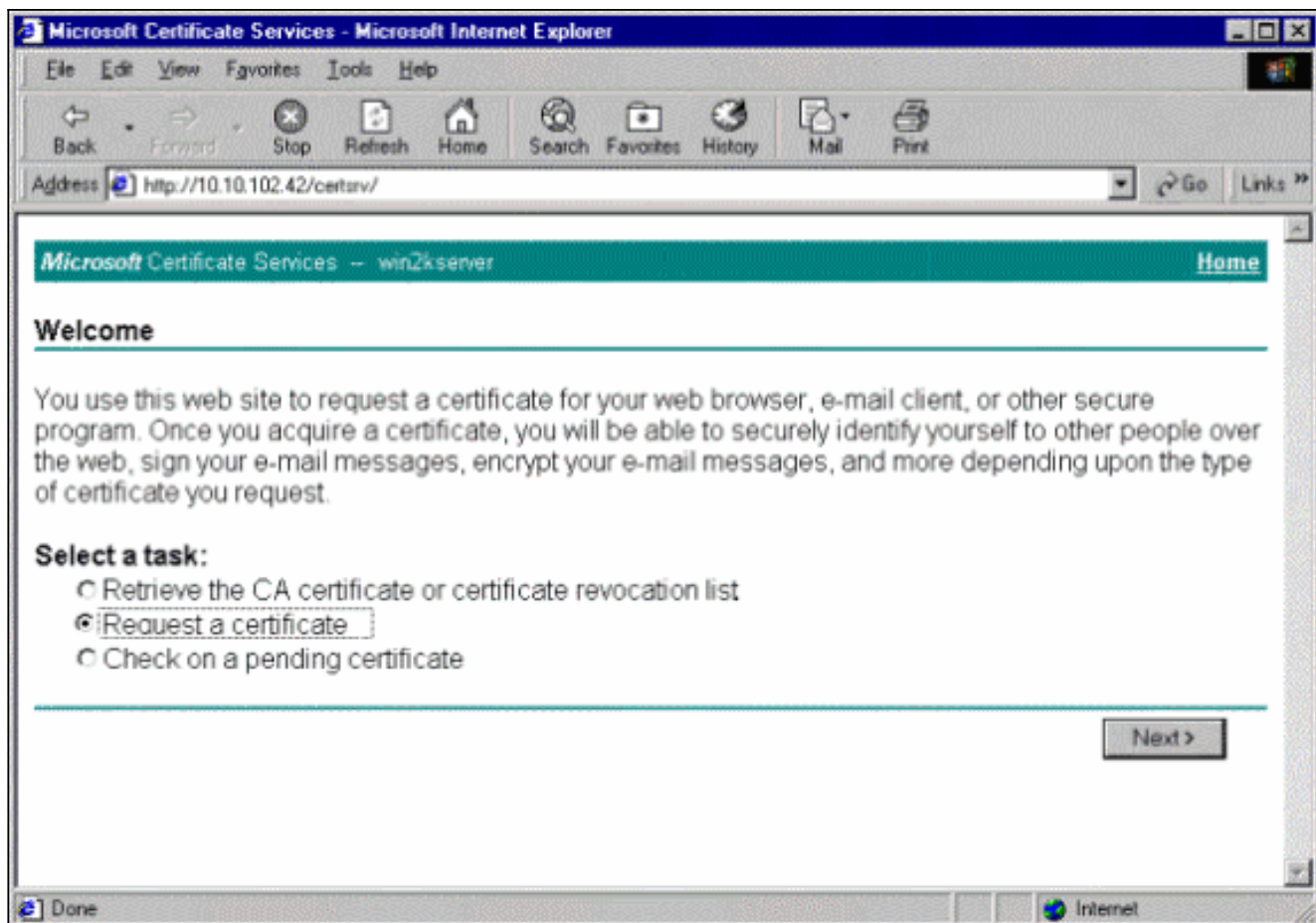
3. Klik in het venster Lijst met CA-certificaten of certificaatherroeping op **Installeren dit CA-certificeringspad** in de linkerhoek. Dit voegt het CA-certificaat toe aan het Trusted Root Certificate Authorities-archief. Dit betekent dat alle certificaten die deze CA afgeeft aan deze client worden vertrouwd.



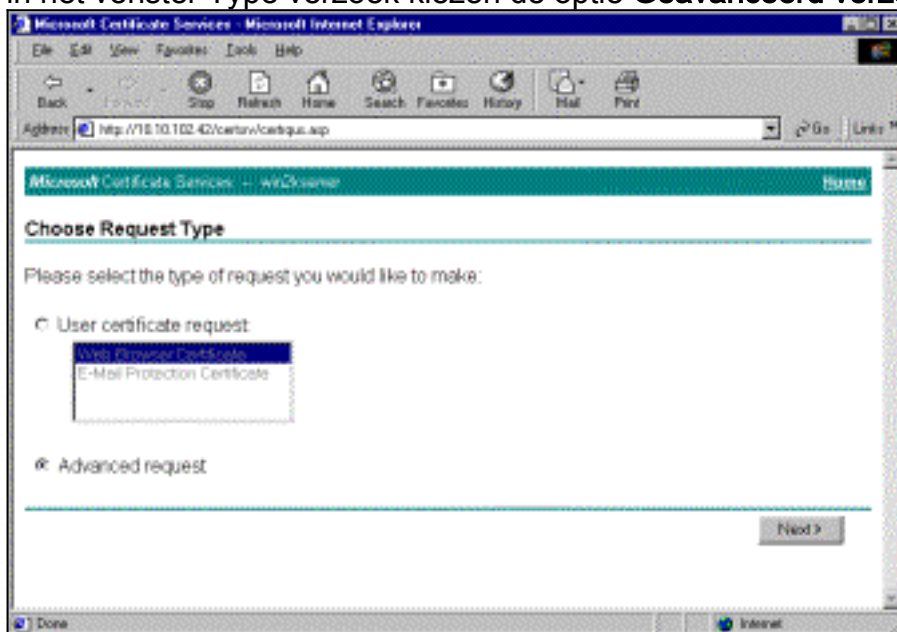
[Een identiteitsbewijs voor de klant verkrijgen](#)

Voltooi deze stappen om een identiteitsbewijs voor de cliënt te verkrijgen:

1. Open een browservenster en voer de URL in voor de Microsoft Certificate Authority (meestal <http://servername> of IP-adres van CA/certsrv). Het welkomsvenster voor het ophalen van certificaten en het weergeven van verzoeken.
2. Kies in het welkomsvenster onder Een taak selecteren de optie **Certificaat aanvragen** en klik op **Volgende**.

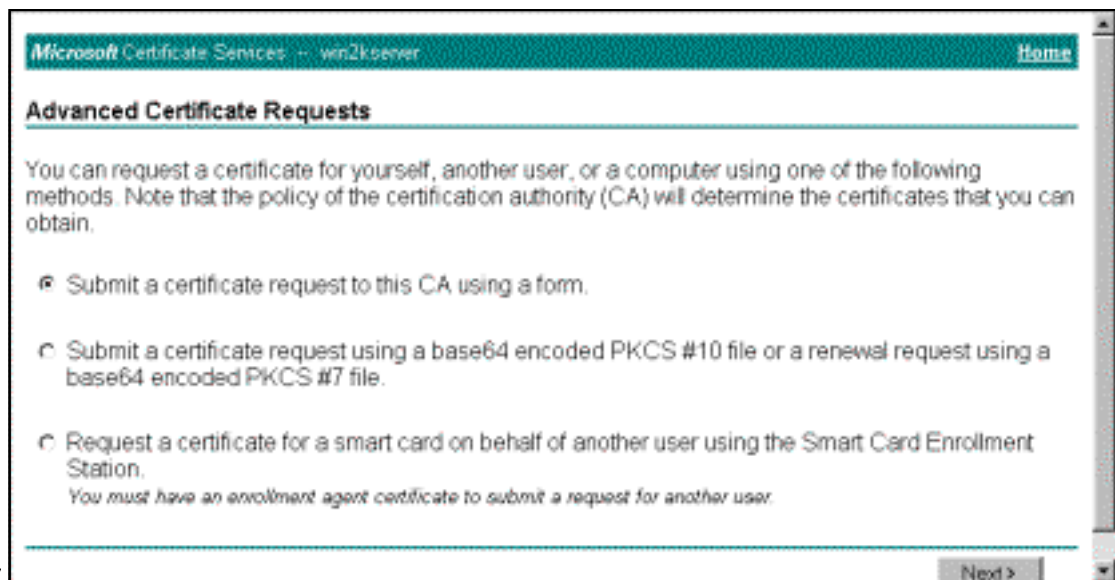


3. Selecteer in het venster Type verzoek kiezen de optie **Geavanceerd verzoek** en klik op



Volgende.

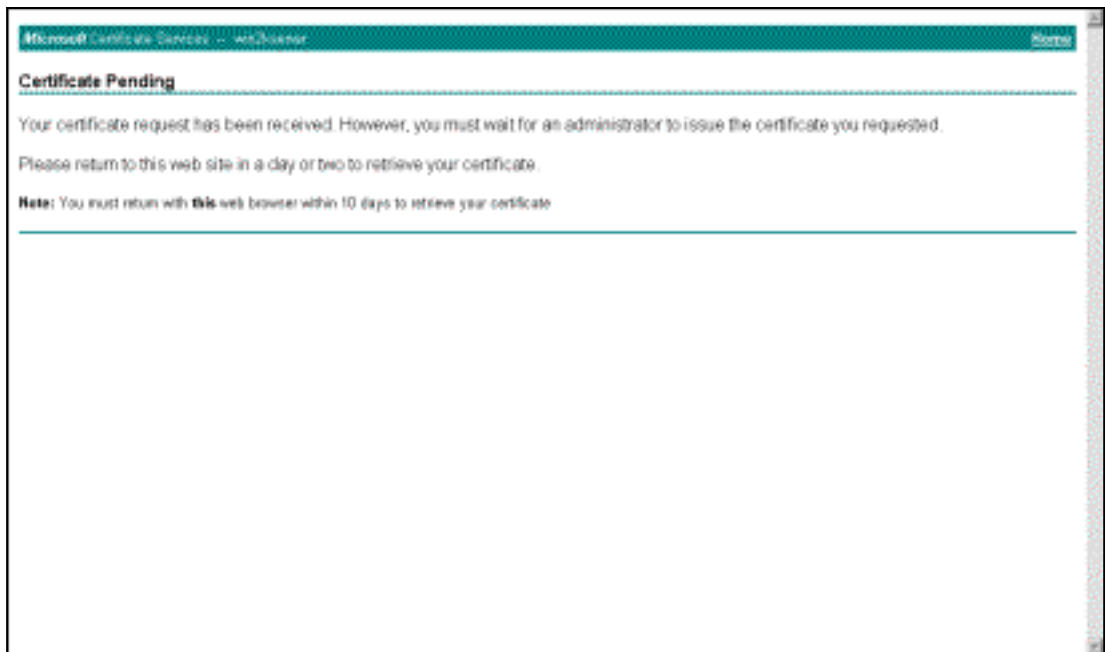
4. Selecteer in het venster Geavanceerde certificaataanvragen de optie **Certificaataanvraag** indienen bij deze certificeringsinstantie met behulp van een



formulier.

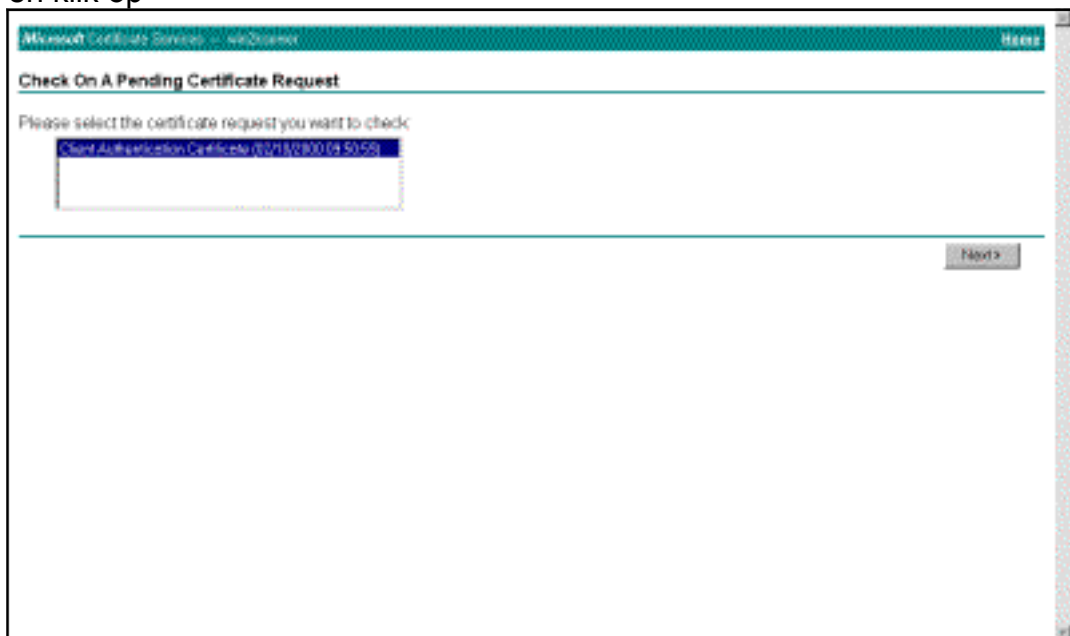
5. Vul de velden in zoals in dit voorbeeld. De waarde voor Afdeling (organisatorische eenheid) moet overeenkomen met de groep die op de VPN Concentrator is geconfigureerd. Specificeer geen sleutelgrootte groter dan 1024. Zorg ervoor dat u het selectievakje **Lokale machine-opslag gebruiken** aanvinkt. Klik op **Volgende** als u klaar bent.

p basis van de configuratie van de CA-server wordt dit venster soms weergegeven. Als dit het geval is, neemt u contact op met de CA-



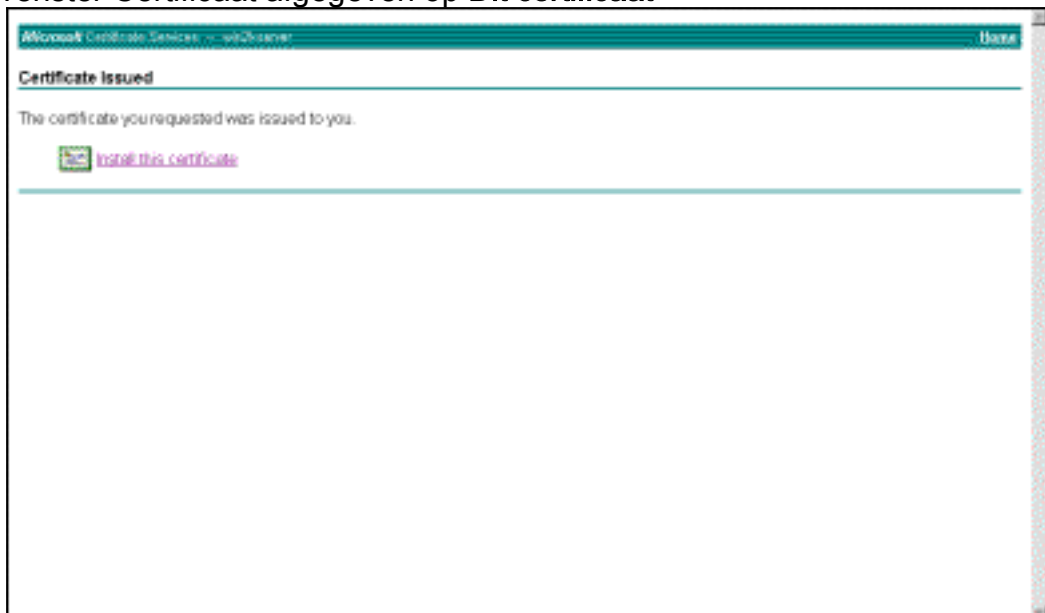
beheerder.

6. Klik op **Home** om terug te keren naar het hoofdscherm, selecteer **Controle op hangend certificaat** en klik op



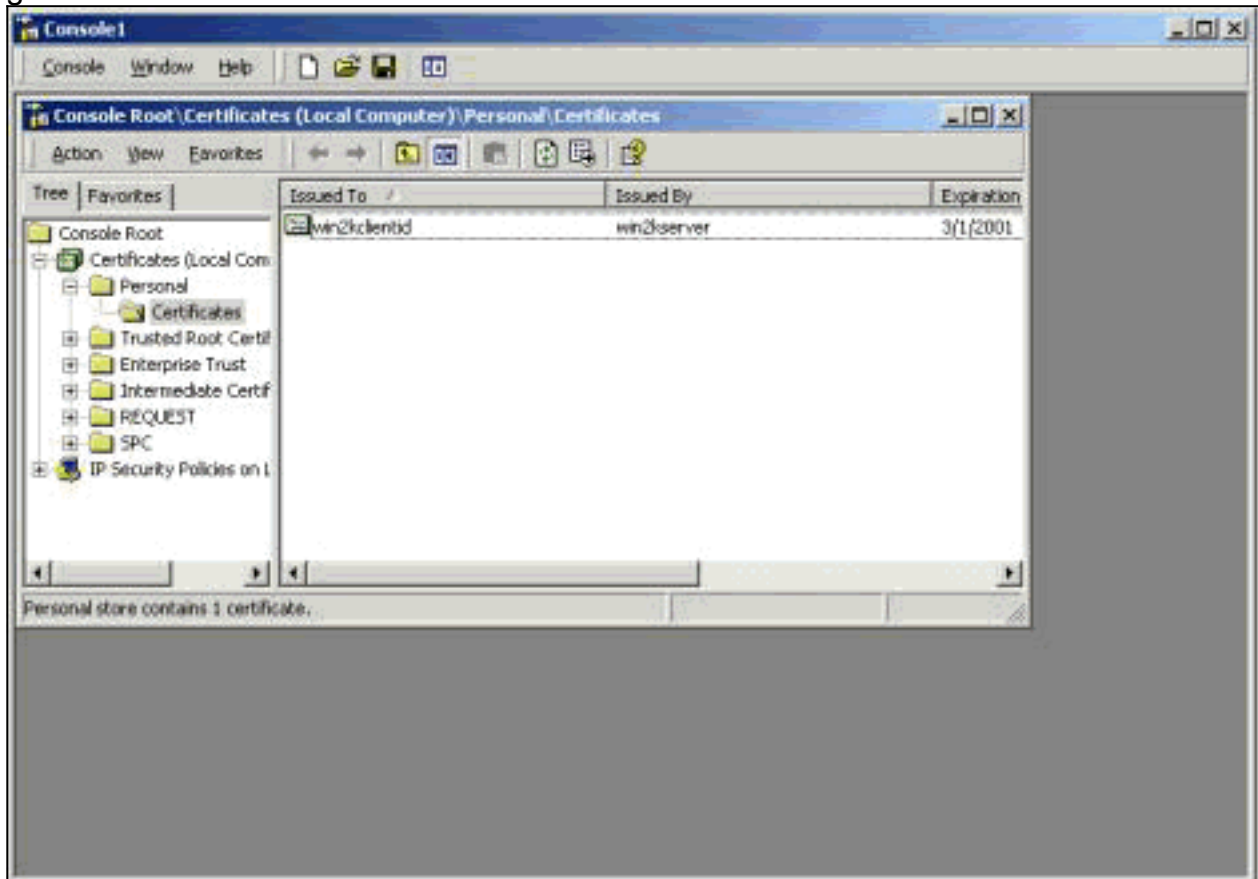
Volgende.

7. Klik in het venster Certificaat afgegeven op **Dit certificaat**



installeren.

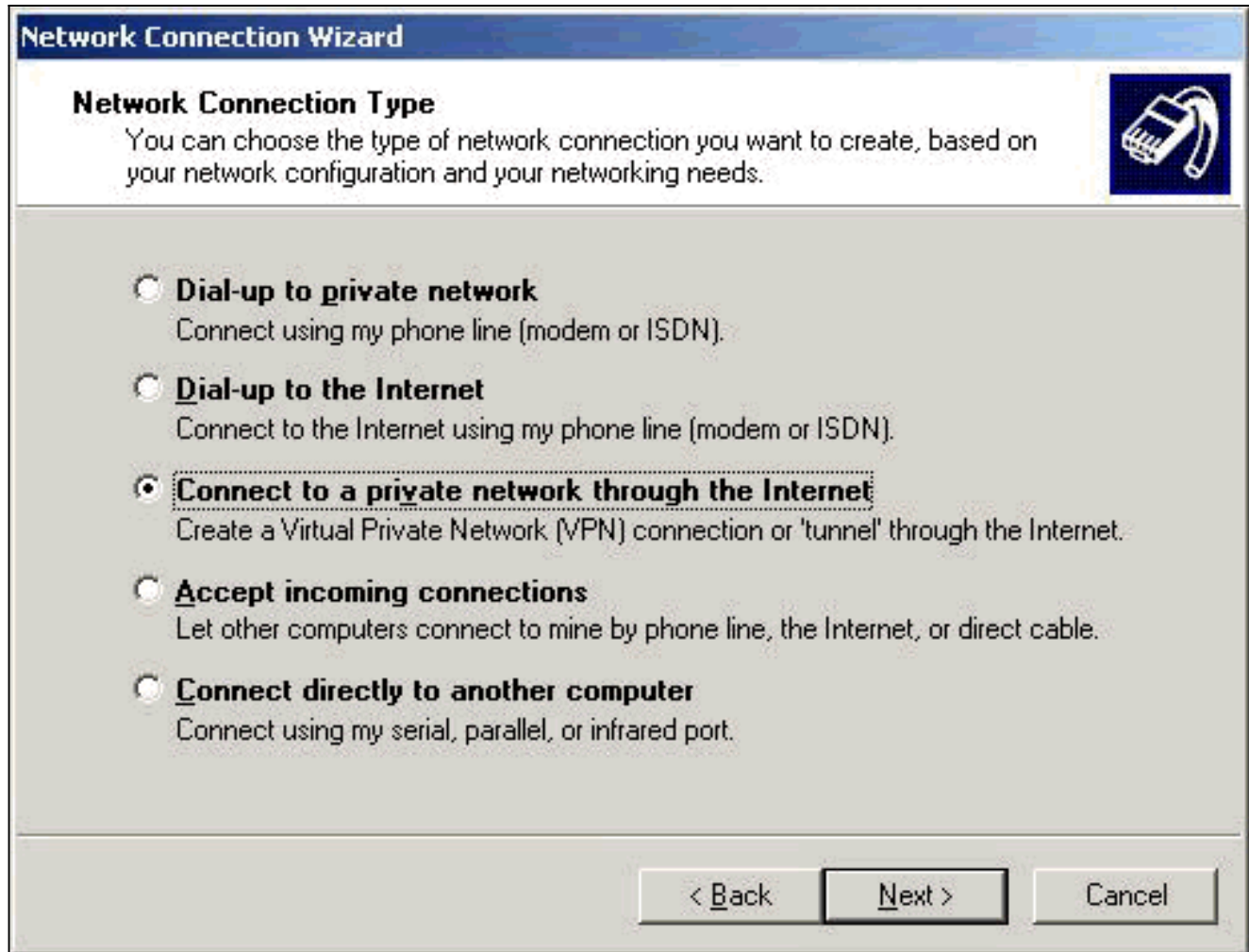
8. Als u uw clientcertificaat wilt weergeven, selecteert u **Start > Uitvoeren** en vervolgens voert u Microsoft Management Console (MMC) uit.
9. Klik op **console** en kies **Magnetisch toevoegen/verwijderen**.
10. Klik op **Add** en kies **Certificate** in de lijst.
11. Wanneer een venster verschijnt waarin u wordt gevraagd naar de reikwijdte van het certificaat, kiest u **Computeraccount**.
12. Controleer of het certificaat van de CA-server zich bevindt onder de Trusted Root-certificeringsinstanties. Controleer ook of u een certificaat hebt door **Console Root > Certificate (Local Computer) > Personal > Certificates** te selecteren, zoals in deze afbeelding wordt getoond.



[Een verbinding met VPN 3000 maken met de wizard Netwerkverbinding](#)

Voltooi deze procedure om een verbinding met VPN 3000 te maken met behulp van de wizard Netwerkverbinding:


1. Klik met de rechtermuisknop op **Mijn netwerklocaties**, kies **Eigenschappen** en klik op **Nieuwe verbinding maken**.
2. Kies in het venster Type netwerkverbinding de optie **Verbinding maken met een privaat netwerk via het internet** en klik vervolgens op **Volgende**.



3. Voer de hostnaam of het IP-adres van de openbare interface van de VPN Concentrator in en klik op **Volgende**.

Network Connection Wizard

Destination Address
What is the name or address of the destination?

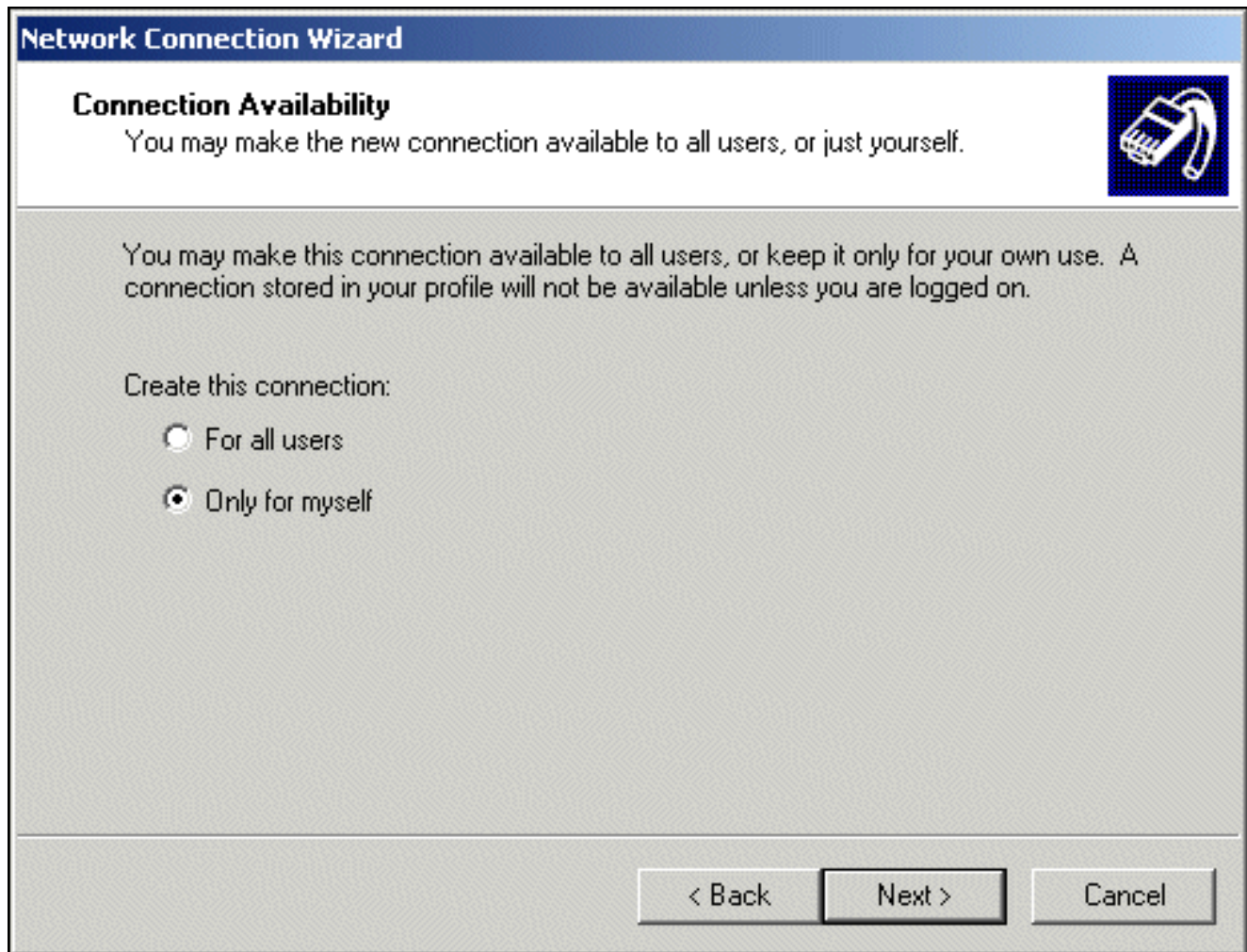


Type the host name or IP address of the computer or network to which you are connecting.

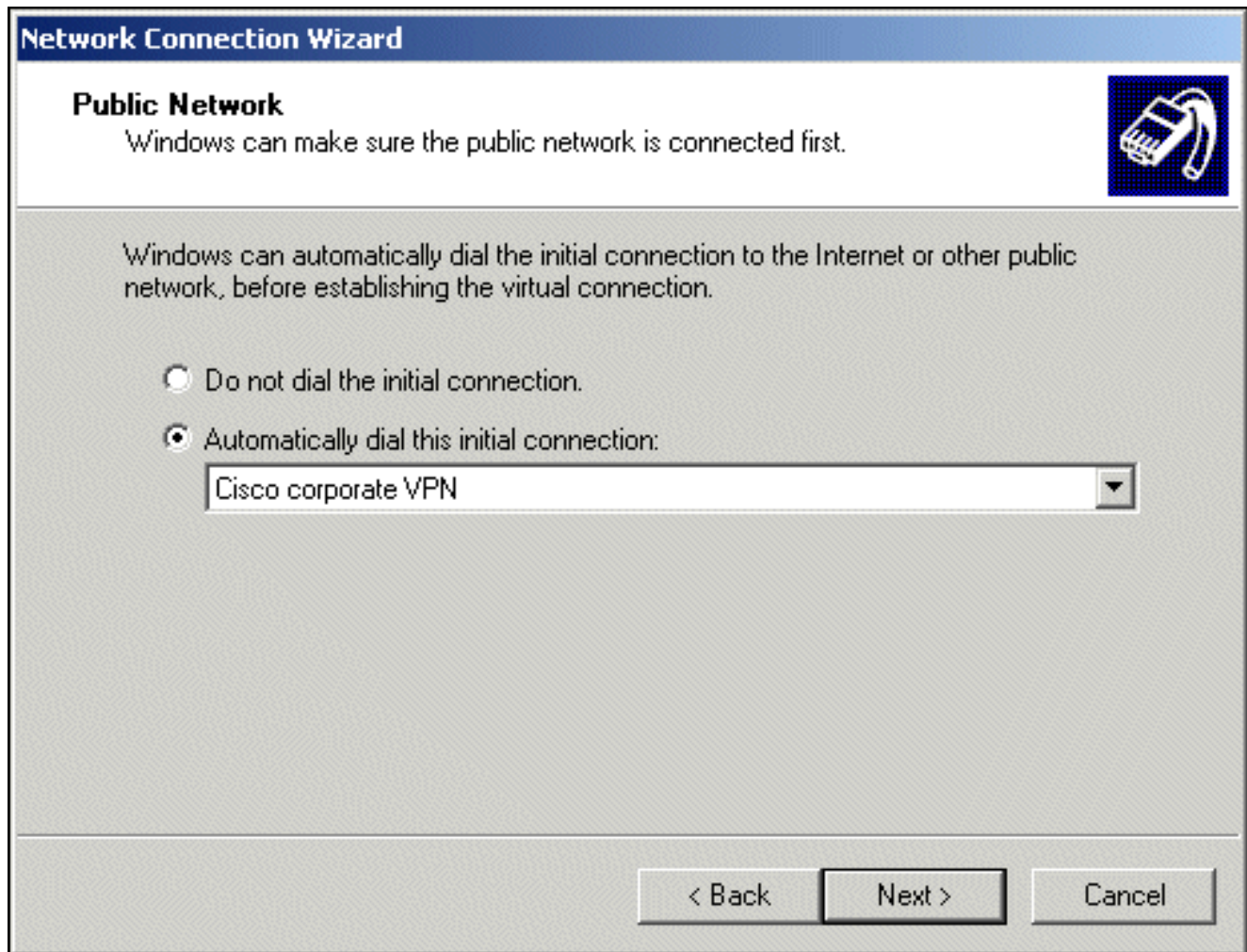
Host name or IP address (such as microsoft.com or 123.45.6.78):

< Back Next > Cancel

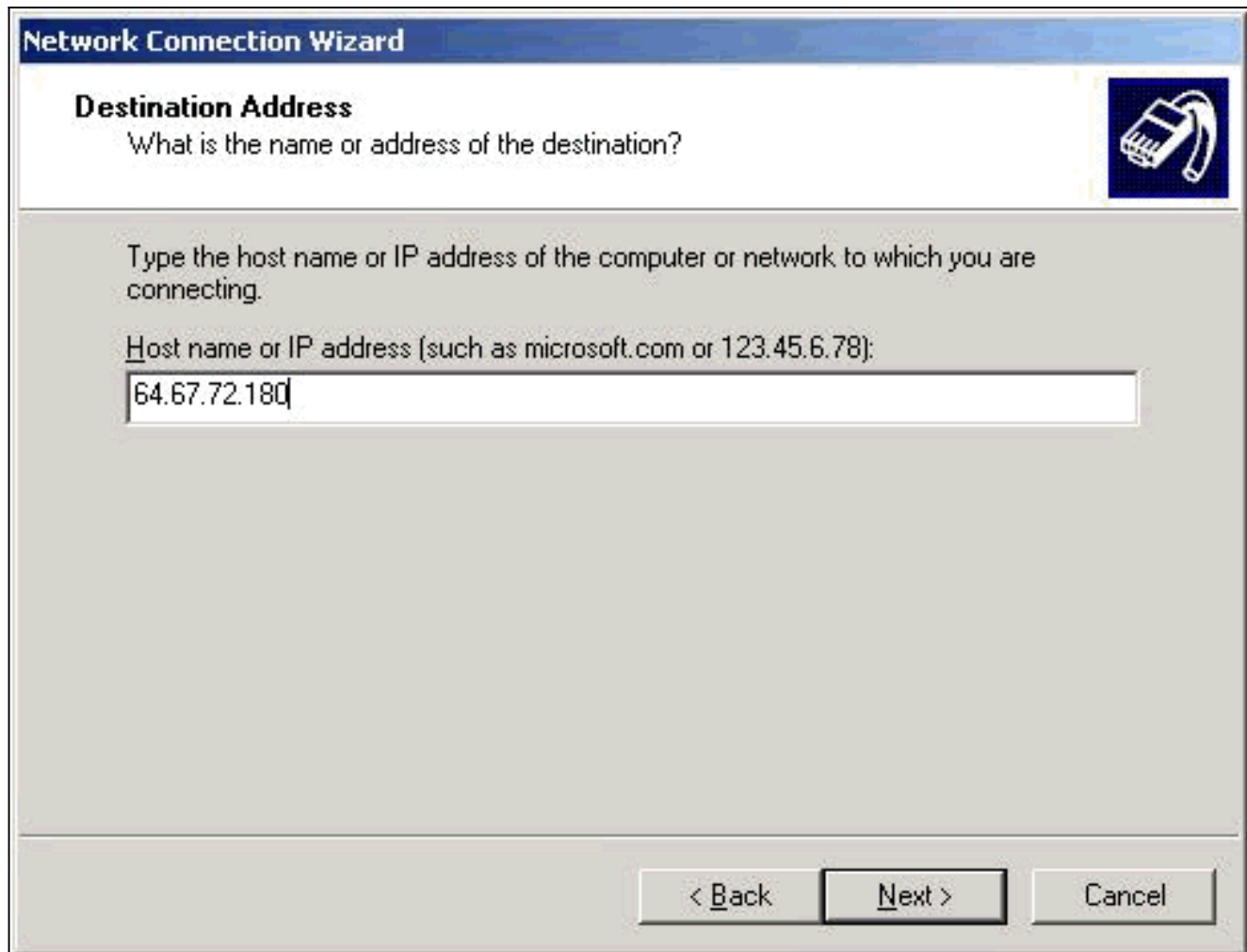
4. Selecteer in het venster Beschikbaarheid verbinding de optie **Alleen voor mezelf** en klik op **Volgende**.



5. Selecteer in het venster Openbaar netwerk of de eerste verbinding (de ISP-account) automatisch moet worden gedraaid.



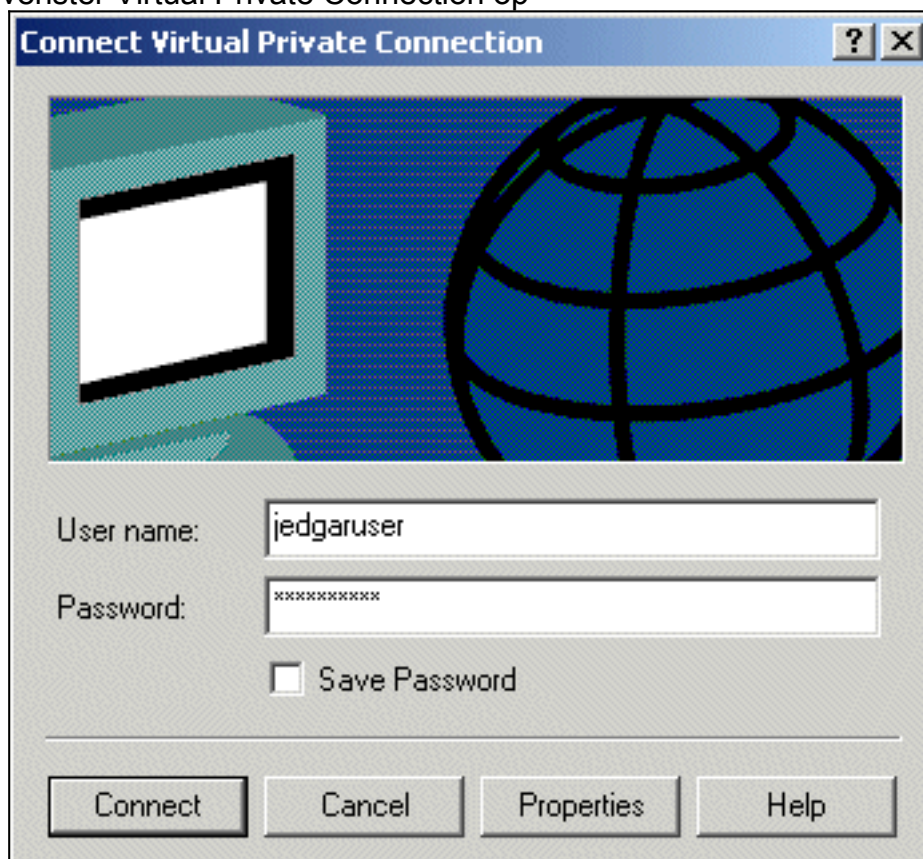
6. Voer in het scherm Doeladres de hostnaam of het IP-adres van de VPN 3000 Concentrator in en klik op **Volgende**.



7. Typ in het venster Wizard Netwerkverbinding een naam voor de verbinding en klik op **Voltoeien**. In dit voorbeeld wordt de verbinding "Cisco Corporate VPN" genoemd.



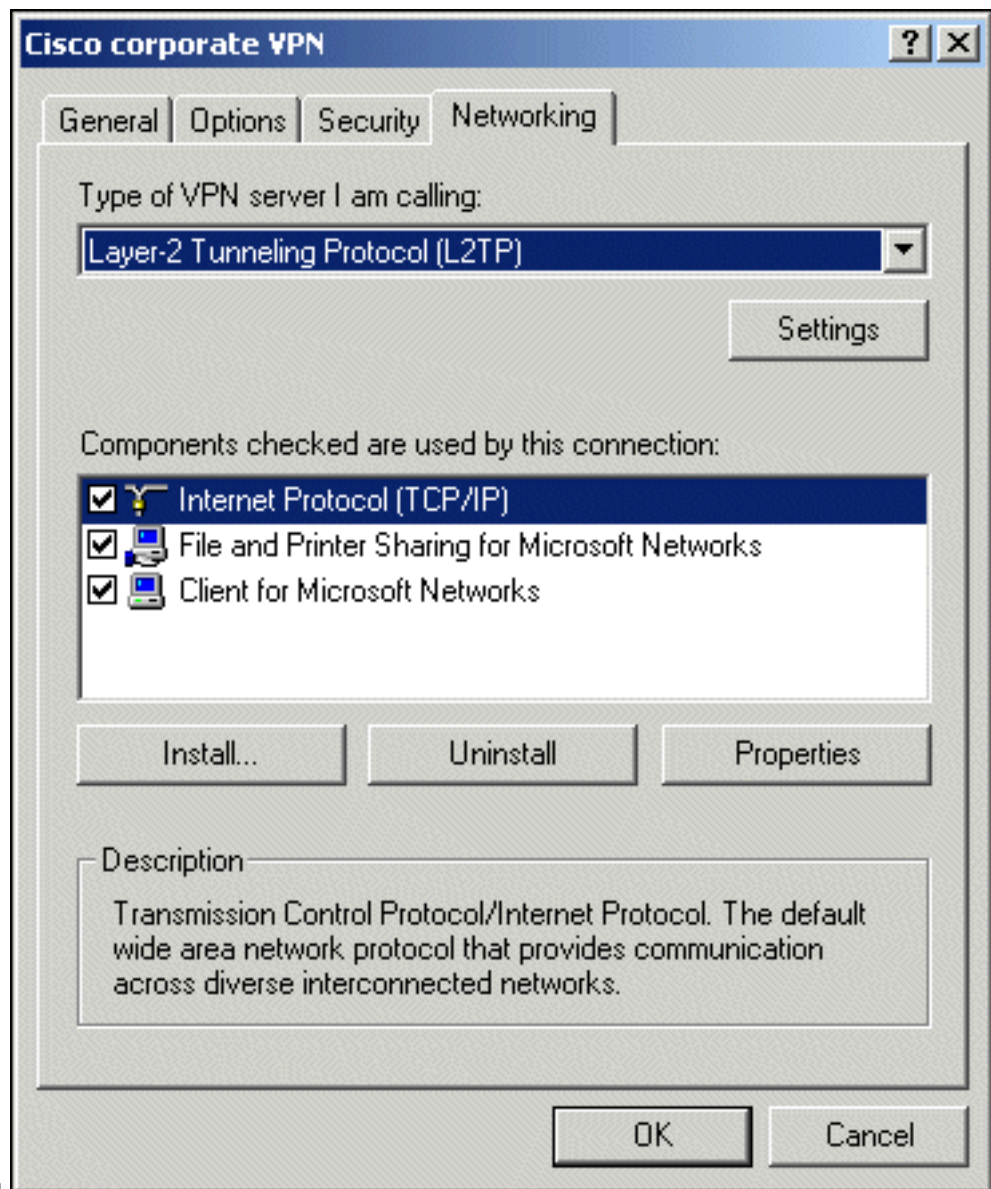
8. Klik in het venster Virtual Private Connection op



Properties.

9. Selecteer in het venster Eigenschappen het tabblad Netwerken.

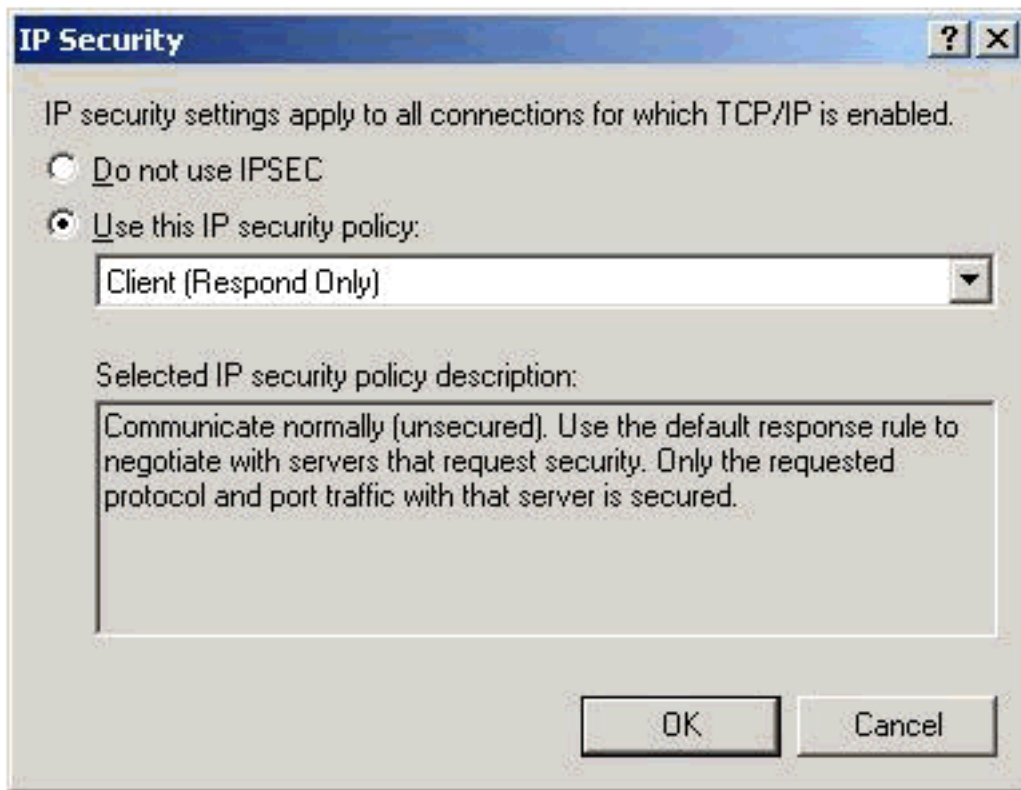
10. Kies onder Type VPN-server ik bel **L2TP** in het keuzemenu, markeer **Internet Protocol TCP/IP** en klik op



Eigenschappen.

11. Selecteer **Geavanceerd > Opties > Eigenschappen**.

12. Kies in het venster IP-beveiliging de optie **Dit IP-beveiligingsbeleid**



gebruiken.

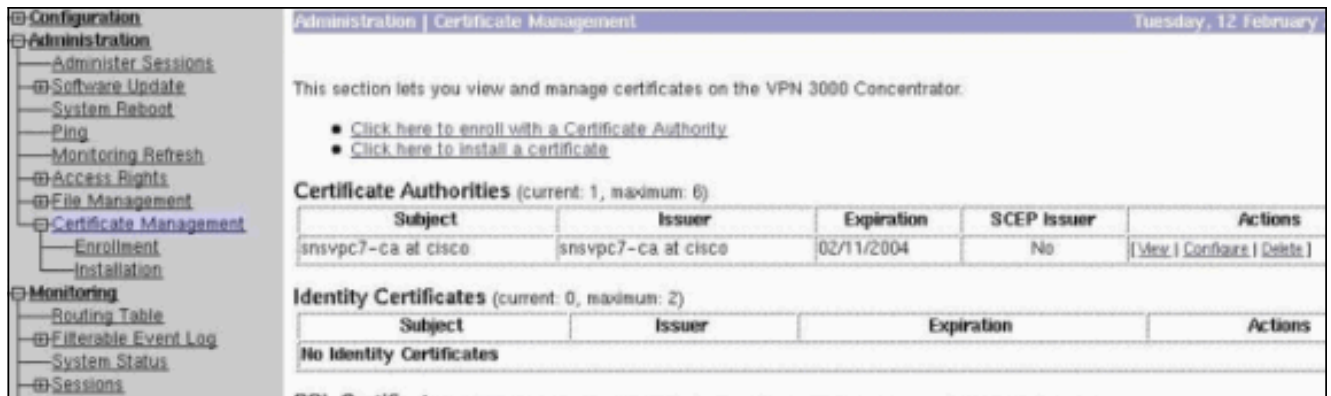
13. Kies het **clientbeleid (alleen antwoorden)** in het keuzemenu en klik meerdere malen op **OK** totdat u terugkeert naar het scherm **Verbinden**.
14. Om een verbinding te starten, voert u uw gebruikersnaam en wachtwoord in en klikt u op **Verbinden**.

[De VPN 3000 concentrator configureren](#)

[Verkrijg een basiscertificaat](#)

Voltooi deze stappen om een basiscertificaat te verkrijgen voor de VPN 3000 Concentrator:

1. Wijs uw browser naar uw CA (meestal iets zoals `http://ip_add_of_ca/certsrv/`), **haal het CA-certificaat of de lijst met certificaatherroeping op** en klik op **Volgende**.
2. Klik op **CA-certificaat downloaden** en sla het bestand ergens op uw lokale schijf op.
3. Op VPN 3000 Concentrator selecteert u **Beheer > Certificaatbeheer** en klikt u **hier om een certificaat te installeren en CA-certificaat te installeren**.
4. Klik op **Uploadbestand vanaf werkstation**.
5. Klik op **Bladeren** en selecteer het CA-certificaatbestand dat u zojuist hebt gedownload.
6. Markeer de bestandsnaam en klik op **Installeren**.



[Verkrijg een Identiteitscertificaat voor VPN 3000 Concentrator](#)

Voltooi deze stappen om een identiteitscertificaat voor de VPN 3000 Concentrator te verkrijgen:

1. Selecteer **ConfAdministration > Certificaatbeheer > Inschrijven > Identity Certificate** en klik vervolgens op **Inschrijven via PKCS10 request (Manual)**. Vul het formulier in zoals hier wordt getoond en klik op **Inschrijven**.

Er verschijnt een browservenster met de certificaataanvraag. Het moet tekst bevatten die vergelijkbaar is met deze uitvoer:

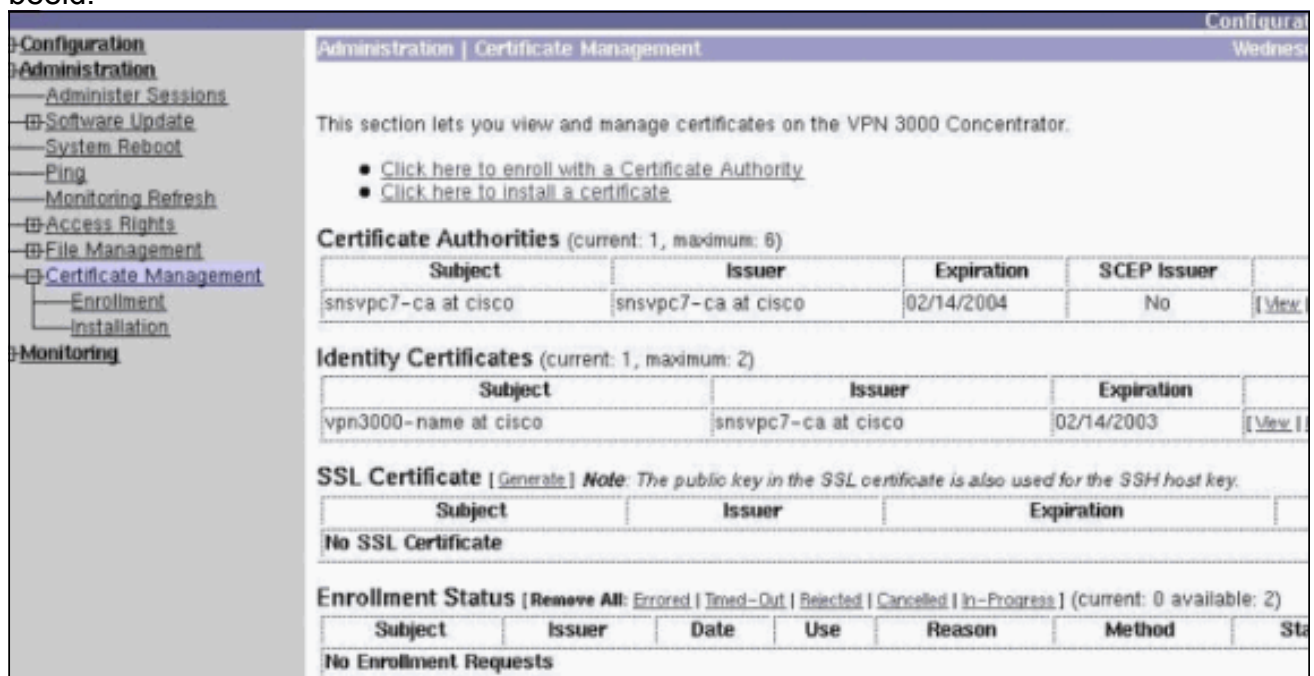
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY21zY28xMDEwLW5hbWUxMDEwLW5hbWUxMDEwLW5hbWUxMDEw
BgkqhkiG9w0BAQEFAANJADBGAkEAX7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJJDjElMCMwIQYDVR0RBowGIIWdnBuMzAwMCluYw11LmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBAbzCG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nFj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```

2. Wijs uw browser naar uw CA-server, controleer **Een certificaat aanvragen** en klik op **Volgende**.
3. Controleer **Geavanceerd verzoek**, klik op **Volgende** en selecteer **Een certificaatverzoek indienen met behulp van een base64 gecodeerd PKCS #10-bestand** of een **verlengingsverzoek met behulp van een base64 gecodeerd PKCS #7-bestand**.

4. Klik op **Next** (Volgende). Knijpt en plakt de tekst van de certificaataanvraag die eerder in het tekstgebied is weergegeven. Klik op **Verzenden**.
5. Gebaseerd op hoe de CA-server is geconfigureerd, kunt u op **CA-certificaat downloaden** klikken. Of zodra het certificaat is afgegeven door de CA, ga terug naar uw CA-server en controleer **een hangend certificaat**.
6. Klik op **Volgende**, selecteer uw verzoek en klik nogmaals op **Volgende**.
7. Klik op **CA-certificaat downloaden** en sla het bestand op de lokale schijf op.
8. Op VPN 3000 Concentrator selecteert u **Beheer > Certificaatbeheer > Installeren** en klikt u op **Certificaat installeren dat is verkregen via inschrijving**. Vervolgens ziet u uw verzoek in behandeling met de status "In uitvoering", zoals in deze afbeelding.



9. Klik op **Installeren**, gevolgd door **Upload File vanaf het werkstation**.
10. Klik op **Bladeren** en selecteer het bestand dat uw certificaat bevat dat is afgegeven door de CA.
11. Markeer de bestandsnaam en klik op **Installeren**.
12. Selecteer **Beheer > Certificaatbeheer**. Er verschijnt een scherm dat vergelijkbaar is met dit beeld.

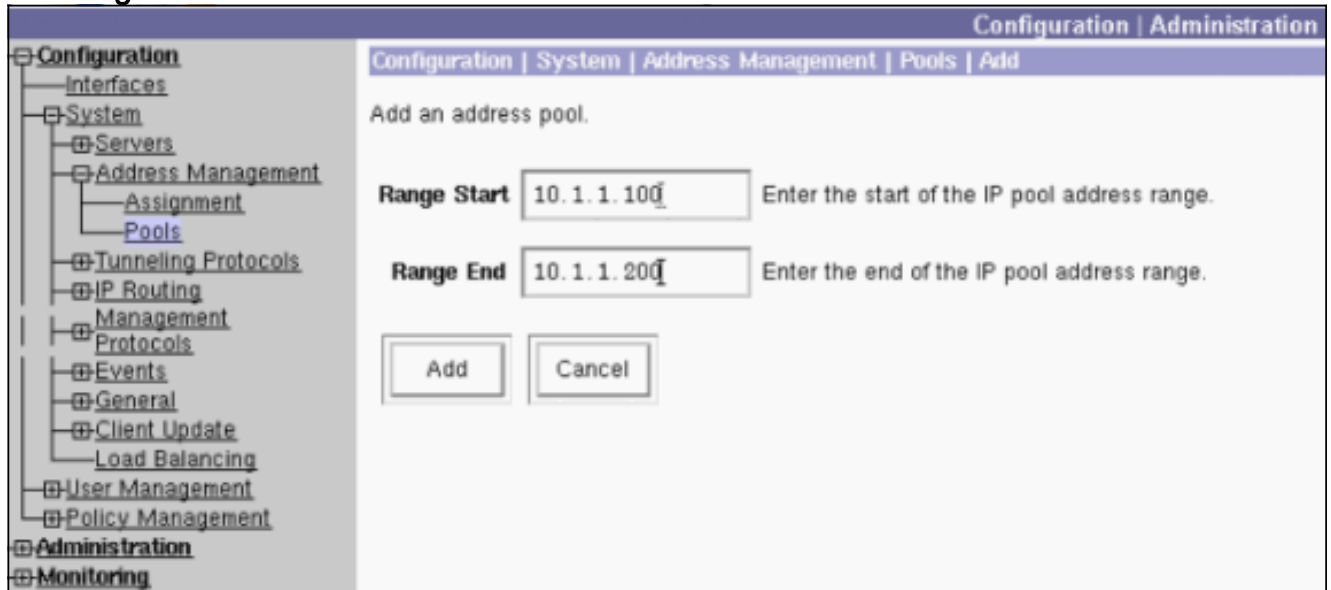


[Een pool voor de clients configureren](#)

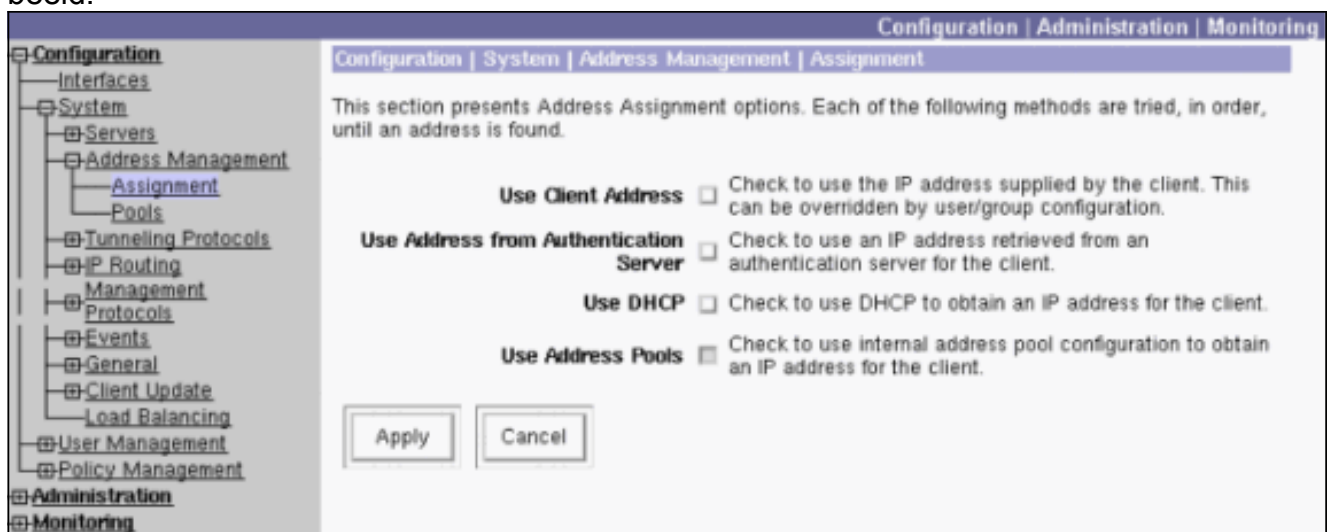
Voltooi deze procedure om een pool voor de cliënten te vormen:

1. Om een beschikbaar bereik van IP-adressen toe te wijzen, wijst u een browser naar de binnenkant van de interface van de VPN 3000 Concentrator en selecteert u **Configuratie > Systeem > Adresbeheer > Pools > Add**.

2. Specificeer een bereik van IP-adressen die niet conflicteren met andere apparaten in het binnennetwerk en klik op **Toevoegen**.



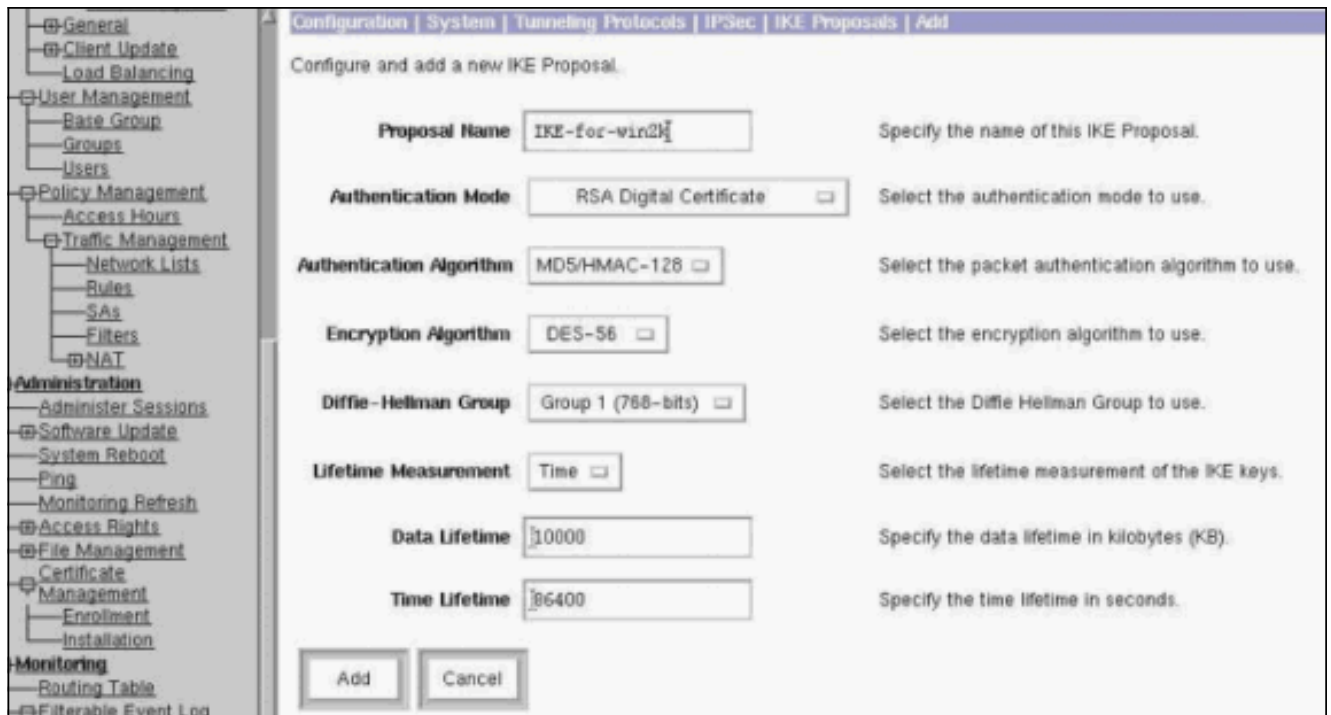
3. Om de VPN 3000 Concentrator te vertellen om de pool te gebruiken, selecteert u **Configuratie > Systeem > Adresbeheer > Toewijzing**, schakelt u het vakje **Adrespools gebruiken in** en klikt u op **Toepassen**, zoals in dit beeld.



[Een IKE-voorstel configureren](#)

Voltooi de volgende stappen om een IKE-voorstel te configureren:

1. Selecteer **Configuratie > Systeem > Tunneling Protocols > IPSec > IKE-voorstellen**, klik op **Add** en selecteer de parameters, zoals in deze afbeelding.



2. Klik op **Add**, markeer het nieuwe voorstel in de rechterkolom en klik op **Activeren**.

[De SA configureren](#)

Voltooi deze procedure om de Security Association (SA) te configureren:

1. Selecteer **Configuration > Policy Management > Traffic Management > SA** en klik op **ESP-L2TP-TRANSPORT**. Als deze SA niet beschikbaar is of als u deze gebruikt voor een ander doel, maak een nieuwe SA vergelijkbaar met deze. Verschillende instellingen voor de SA zijn acceptabel. Verander deze parameter op basis van uw beveiligingsbeleid.
2. Selecteer het digitale certificaat dat u eerder hebt geconfigureerd onder het keuzemenu **Digitaal certificaat**. Selecteer het voorstel **IKE-for-win2k** Internet Key Exchange (IKE). **Opmerking:** dit is niet verplicht. Wanneer de L2TP/IPSec-client verbinding maakt met de VPN Concentrator, worden alle IKE-voorstellen die zijn geconfigureerd onder de actieve kolom van de pagina **Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen** in volgorde geprobeerd. Dit beeld toont de configuratie die nodig is voor de SA:



[De groep en gebruiker configureren](#)

Voltooi deze procedure om de Groep en de Gebruiker te configureren:

1. Selecteer **Configuratie > Gebruikersbeheer > Basisgroep**.
2. Zorg dat op het tabblad Algemeen **L2TP via IPsec** is ingeschakeld.
3. Selecteer onder het tabblad IPsec de **ESP-L2TP-TRANSPORT SA**.
4. Schakel onder het tabblad PPTP/L2TP alle opties voor **L2TP-encryptie uit**.
5. Selecteer **Configuratie > Gebruikersbeheer > Gebruikers** en klik op **Toevoegen**.
6. Voer de naam en het wachtwoord in waarmee u verbinding wilt maken vanuit uw Windows 2000-client. Zorg ervoor dat u **basisgroep** selecteert onder de groepsselectie.
7. Controleer op het tabblad Algemeen het **L2TP via IPsec-tunnelprotocol**.
8. Selecteer onder het tabblad IPsec de **ESP-L2TP-TRANSPORT SA**.
9. Schakel onder het tabblad PPTP/L2TP alle opties voor **L2TP-encryptie uit** en klik op **Add**. U kunt nu verbinding maken met behulp van de L2TP/IPsec Windows 2000-client. **Opmerking:** u hebt ervoor gekozen de basisgroep te configureren om de externe L2TP/IPsec-verbinding te accepteren. Het is ook mogelijk om een groep te configureren die overeenkomt met het veld Organisatie-eenheid (OU) van de SA om de inkomende verbinding te accepteren. De configuratie is identiek.

[Debuginformatie](#)

```
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 constructing 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

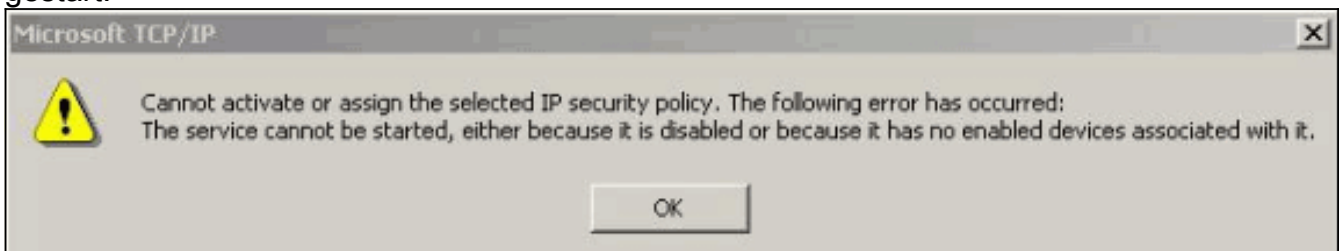
524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0

```

Informatie over probleemoplossing

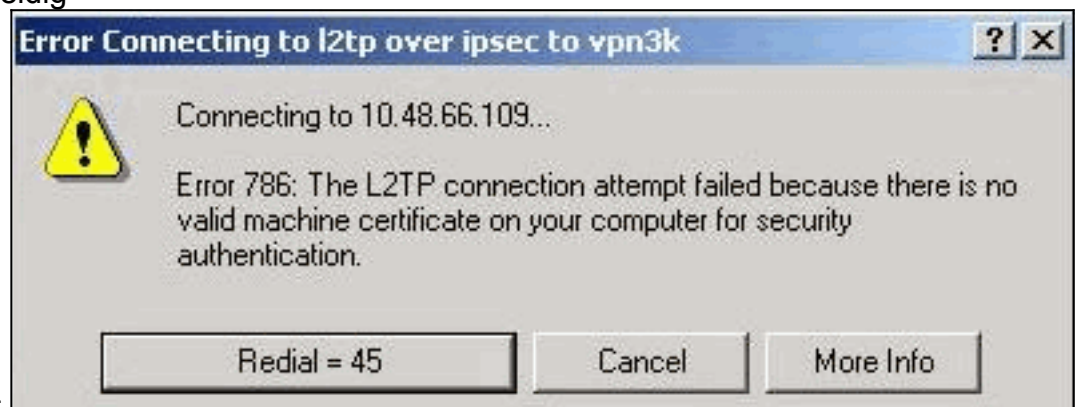
Deze sectie illustreert enkele veelvoorkomende problemen en de probleemoplossingsmethoden voor elk probleem.

- De server kan niet worden gestart.



Waarschijnlijk is de IPSec-service niet gestart. Selecteer **Start > Programma's > Beheergereedschappen > Service** en zorg ervoor dat de **IPSec-service** is ingeschakeld.

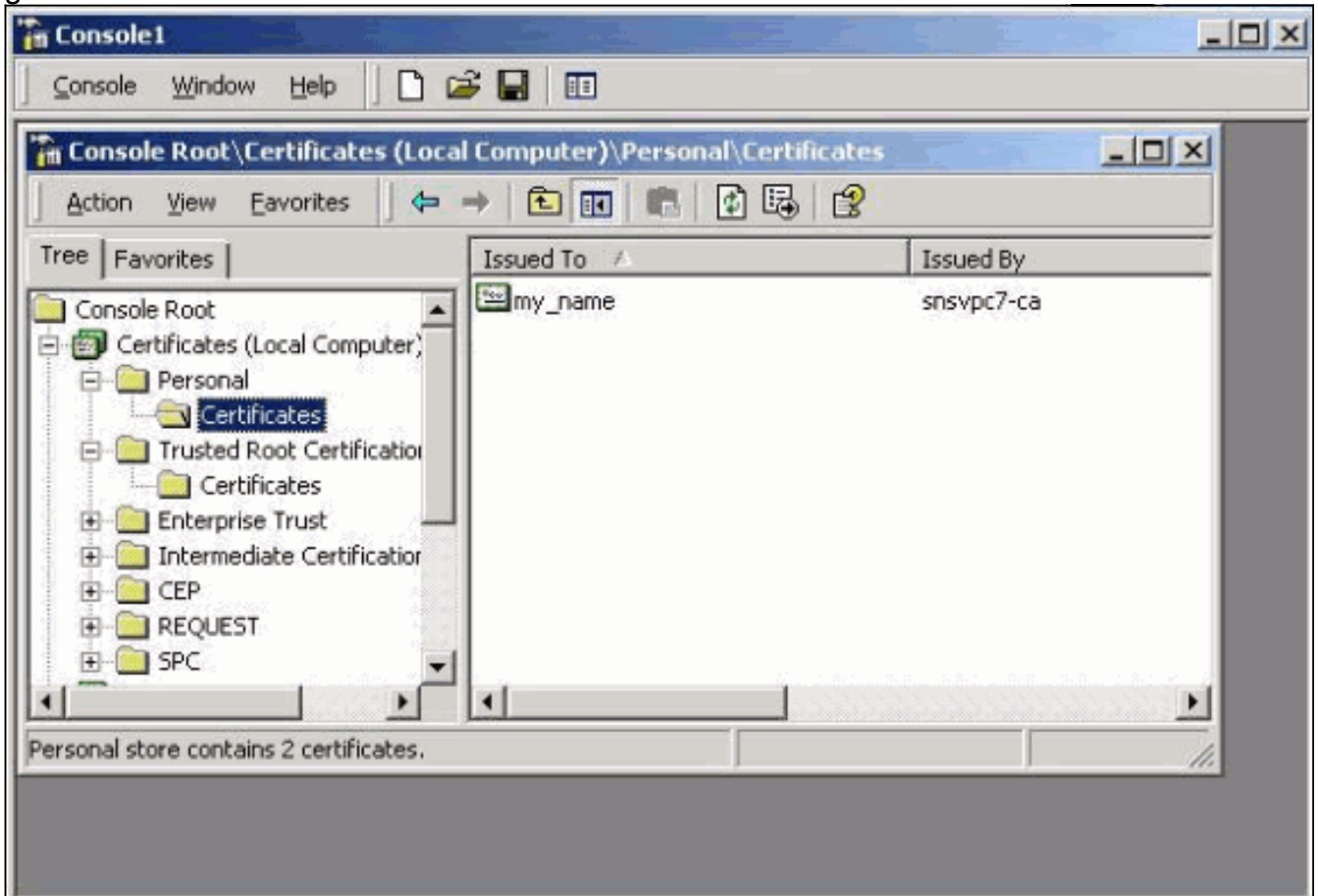
- Error 786: Geen geldig



machinecertificaat.

Deze fout geeft een probleem aan met het certificaat op de lokale machine. Selecteer **Start > Uitvoeren** om eenvoudig naar uw certificaat te kijken en voer MMC uit. Klik op **console** en kies **Magnetisch toevoegen/verwijderen**. Klik op **Add** en kies **Certificate** in de lijst. Wanneer een venster verschijnt waarin u wordt gevraagd naar de reikwijdte van het certificaat, kiest u **Computeraccount**. U kunt nu controleren of het certificaat van de CA-server zich bevindt onder de **Trusted Root-certificeringsinstanties**. U kunt ook controleren of u een certificaat hebt door

Console Root > Certificate (Local Computer) > Personal > Certificates te selecteren, zoals in deze afbeelding wordt getoond.

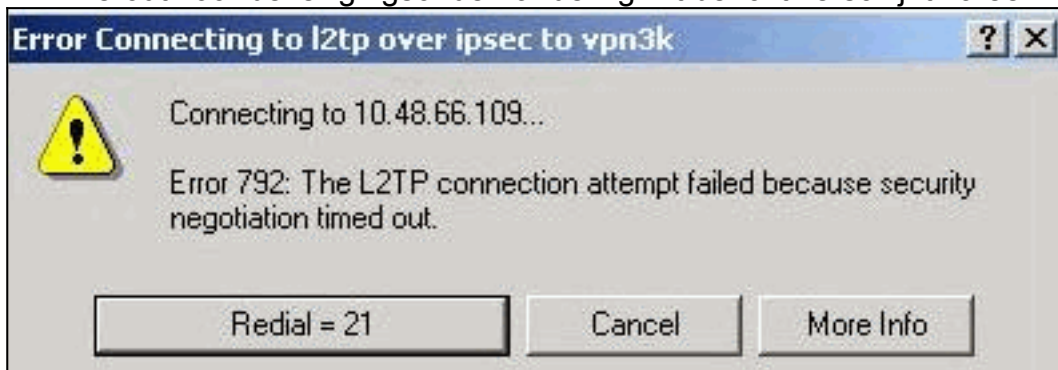


Klik op het **certificaat**. Controleer of alles klopt. In dit voorbeeld, is er een privé sleutel verbonden aan het certificaat. Dit certificaat is echter verlopen. Dat is de oorzaak van het



probleem.

- Error 792: Time-out voor beveiligingsonderhandeling. Dit bericht verschijnt na een lange



periode.

Zet de

relevante debugs aan zoals uitgelegd in de [veelgestelde vragen](#) over [Cisco VPN 3000 Concentrator](#). Lees ze door. Je moet iets zien dat lijkt op dit resultaat:

```
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:

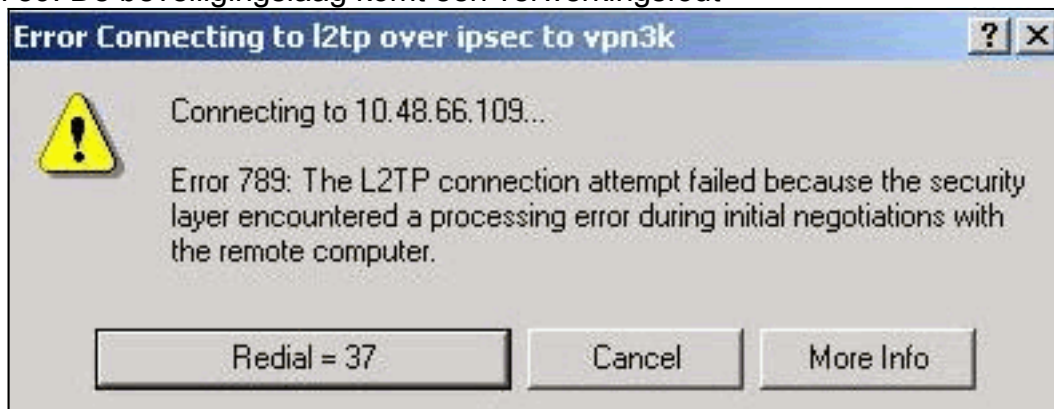
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007

sending delete message

Dit geeft aan dat het IKE-voorstel niet goed is geconfigureerd. Controleer de informatie in het gedeelte [IKE-voorstel configureren](#) van dit document.

- Error 789: De beveiligingslaag komt een verwerkingsfout



tegen. Zet de relevante debugs aan zoals uitgelegd in de [veelgestelde vragen](#) over [Cisco VPN 3000 Concentrator](#). Lees ze door. Je moet iets zien dat lijkt op dit resultaat:

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!

- **Gebruikte versie** Selecteer **Monitoring > System Status** om deze uitvoer te bekijken:

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

Gerelateerde informatie

- [Productondersteuning van IPSec-onderhandeling/IKE-protocollen](#)
- [Technische ondersteuning – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.