SSL VPN-client (SVC) op IOS met Configuratievoorbeeld

Inhoud

Inleiding

De SSL VPN Client (SVC) biedt een volledige tunnel voor veilige communicatie naar het interne netwerk van het bedrijf. U kunt de toegang op een gebruikersbasis configureren of u kunt verschillende WebVPN-contexten maken waarin u een of meer gebruikers plaatst.

SSL VPN of WebVPN technologie wordt ondersteund op deze IOS routerplatforms:

- 870, 1811, 1841, 2801, 2811, 2821, 2851
- 3725, 3745, 3825, 3845, 7200 en 7301

U kunt SSL VPN-technologie op deze modi configureren:

- **Clientless SSL VPN (WebVPN)** - Biedt een externe client die een SSL-enabled Web browser vereist om toegang te krijgen tot HTTP of HTTPS Web servers op een lokaal netwerk (LAN). Daarnaast heeft clientloze SSL VPN toegang tot Windows-bestand dat doorbladert door het

Protocol Common Internet File System (CIFS). Outlook Web Access (OWA) is een voorbeeld van HTTP-toegang.Raadpleeg Clientless SSL VPN (WebVPN) op Cisco IOS met het Voorbeeld van de Configuration om meer te weten te komen over de Clientless SSL VPN.

- **Thin-Client SSL VPN (Port Forwarding)** — Biedt een externe client die een kleine Java-gebaseerde applicatie downloads en maakt beveiligde toegang mogelijk voor TCP-toepassingen (Transmission Control Protocol) die statische poortnummers gebruiken. Point of Presence (POP3), Simple Mail Transfer Protocol (MTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) en Telnet zijn voorbeelden van beveiligde toegang. Omdat bestanden op de lokale machine-wijziging moeten worden gewijzigd, moeten gebruikers lokale beheerrechten hebben om deze methode te kunnen gebruiken. Deze methode van SSL VPN werkt niet met toepassingen die dynamische port opdrachten, zoals sommige FTP-toepassingen (File Transfer Protocol) gebruiken.Raadpleeg Thin-Client SSL VPN (WebVPN) IOS Configuration Voorbeeld met DSM om meer te weten te komen over Thin-Client SSL VPN.**Opmerking:** User Datagram Protocol (UDP) wordt niet ondersteund.
- **SSL VPN-client (SVC volledige tunnelmodus)** - downloads een kleine client naar het externe werkstation en bieden volledige beveiligde toegang tot resources op een intern bedrijfsnetwerk. U kunt de SVC permanent naar een extern werkstation downloaden, of u kunt de client verwijderen wanneer de beveiligde sessie is gesloten.

Dit document demonstreert de configuratie van een Cisco IOS router voor gebruik door een SSL VPN-client.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Microsoft Windows 2000 of XP
- Web browser met SUN JRE 1.4 of hoger of een door ActiveX gecontroleerde browser
- Plaatselijke administratieve rechten op de cliënt
- Een van de routers die in de Inleiding worden vermeld met een geavanceerde security afbeelding (12.4(6)T of hoger)
- Cisco Security apparaat Manager (DSM) versie 2.3Als Cisco DSM niet reeds op uw router is geladen, kunt u een gratis exemplaar van de software verkrijgen van de Software Download (geregistreerde klanten slechts). U moet een CCO-account met een servicecontract hebben. Raadpleeg voor gedetailleerde informatie over de installatie en configuratie van het SDM de router en de veiligheidsapparaat Manager van Cisco.
- Een digitaal certificaat op de routerOm aan deze eis te voldoen, kunt u een certificaat of een externe certificeringsinstantie (CA) gebruiken. Raadpleeg voor meer informatie over aanhoudende zelf-ondertekende certificaten de aanhoudende zelf-ondertekende certificaten.

Gebruikte componenten

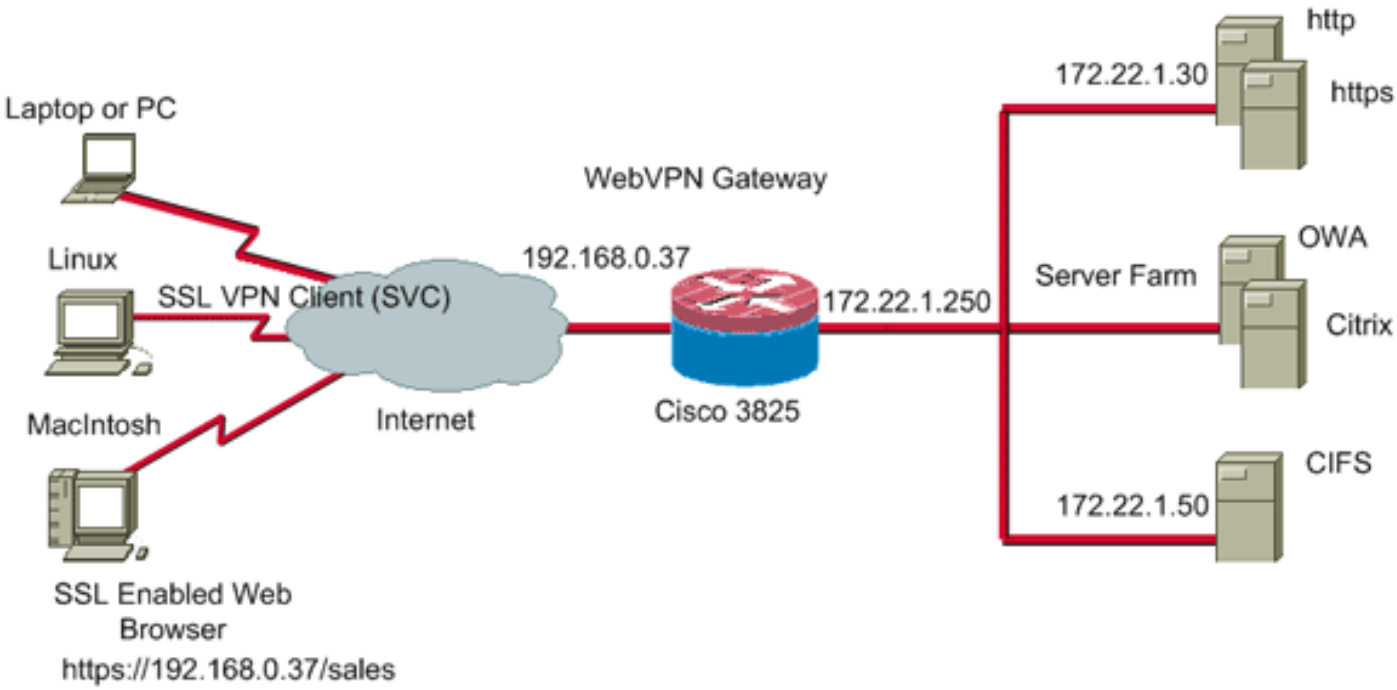
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-router 3825 Series met 12.4(9)T
- Security Devices Manager (DSM) versie 2.3.1

Opmerking: de informatie in dit document is gemaakt van apparatuur in een specifieke labomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Preconfiguratie van taken

1. Configureer de router voor DSM. (optioneel)De routers met de juiste vergunning van de veiligheidsbundel hebben reeds de toepassing sdm in flitser geladen. Raadpleeg het downloaden en installeren van Cisco Router en Security apparaat Manager (DSM) om de software te verkrijgen en te configureren.
2. Download een exemplaar van de SVC aan uw beheerpc.U kunt bij Software Download een exemplaar van het SVC-pakketbestand verkrijgen: Cisco SSL VPN-client (alleen geregistreerde klanten). U moet een geldige CCO-account met een servicecontract hebben.
3. Stel de juiste datum, tijd en tijdzone in en stel vervolgens een digitaal certificaat op de router in.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

SVC wordt aanvankelijk geladen op de WebVPN gateway router. Elke keer dat de client verbinding maakt, wordt er dynamisch een kopie van de SVC gedownload op de PC. Om dit gedrag te veranderen, moet u de router configureren om de software permanent op de clientcomputer te laten blijven.

SVC op IOS configureren

In deze sectie wordt u voorgesteld met de stappen die nodig zijn om de functies te configureren die in dit document worden beschreven. Deze voorbeeldconfiguratie gebruikt de Wizard SVC om de bediening van SVC op de IOS router toe te staan.

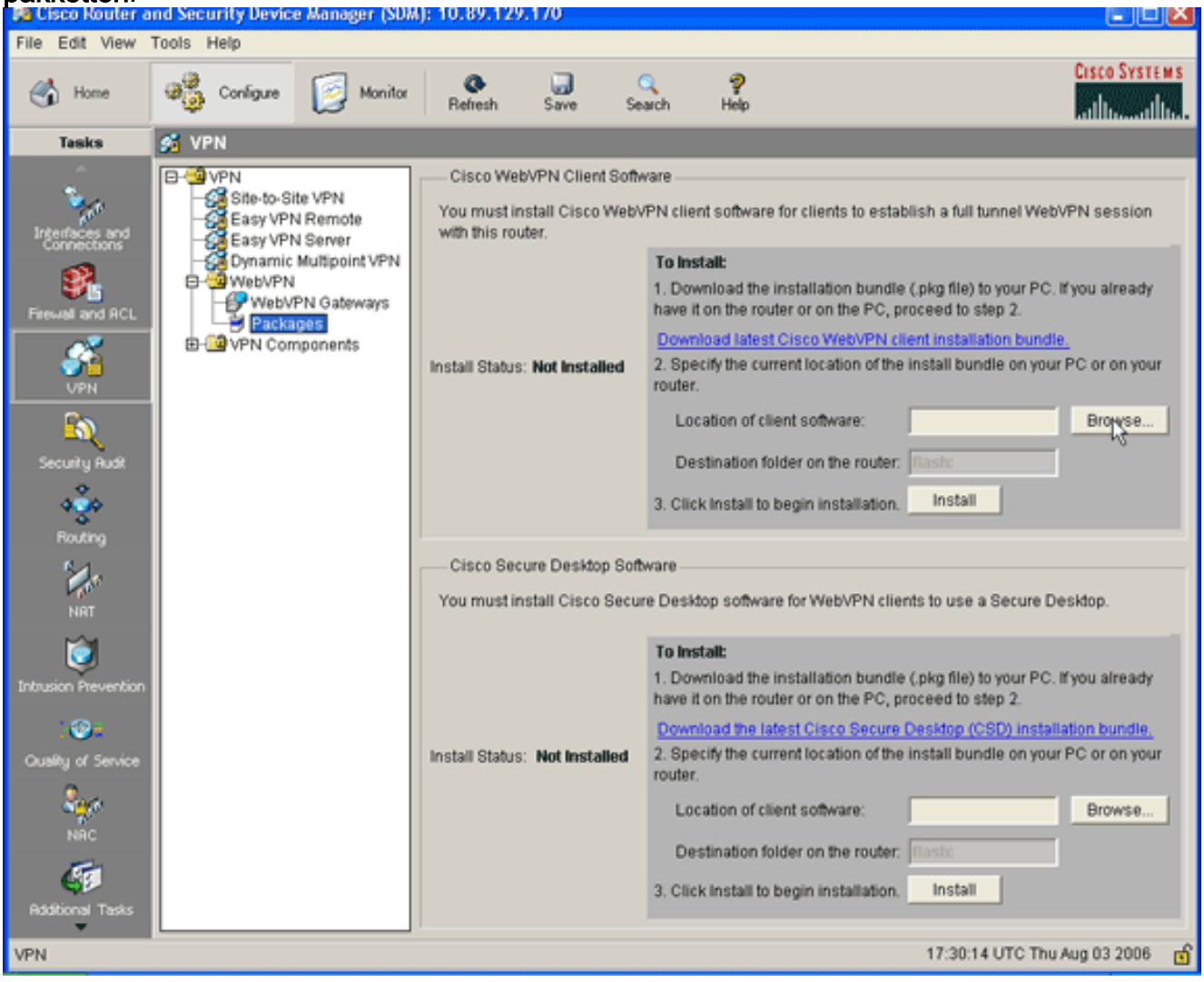
Voltooi deze stappen om SVC op de IOS-router te configureren:

1. Installeer en schakel de SVC-software op de IOS-router in
2. Configureer een WebVPN-context en gateway voor Webex met de wizard
3. De gebruikersdatabase voor SVC-gebruikers configureren
4. Configureer de bronnen om deze aan gebruikers bloot te stellen

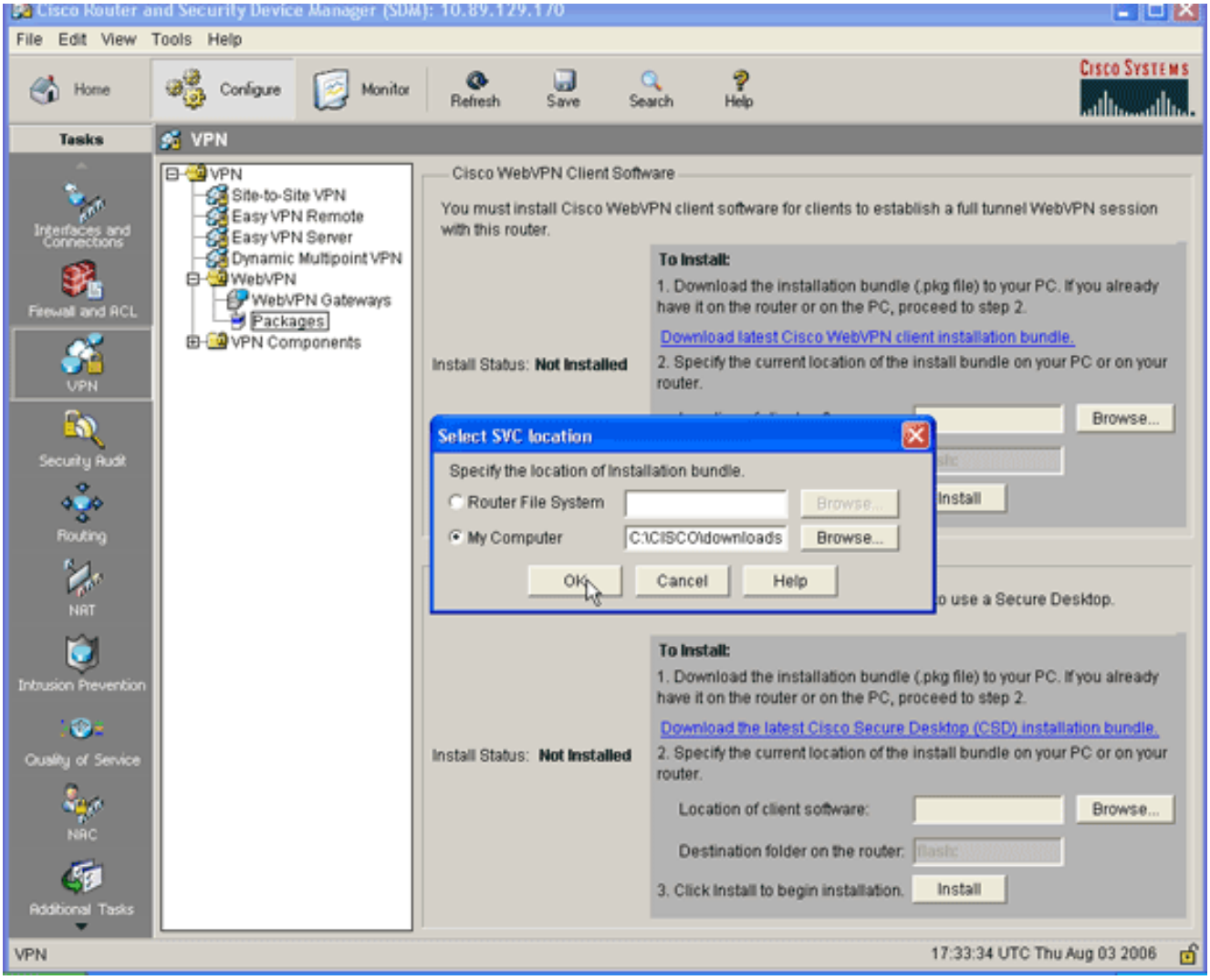
Stap 1. Installeer en schakel de SVC-software op de IOS-router in.

Voltooi deze stappen om de SVC-software op de IOS-router te installeren en inschakelen:

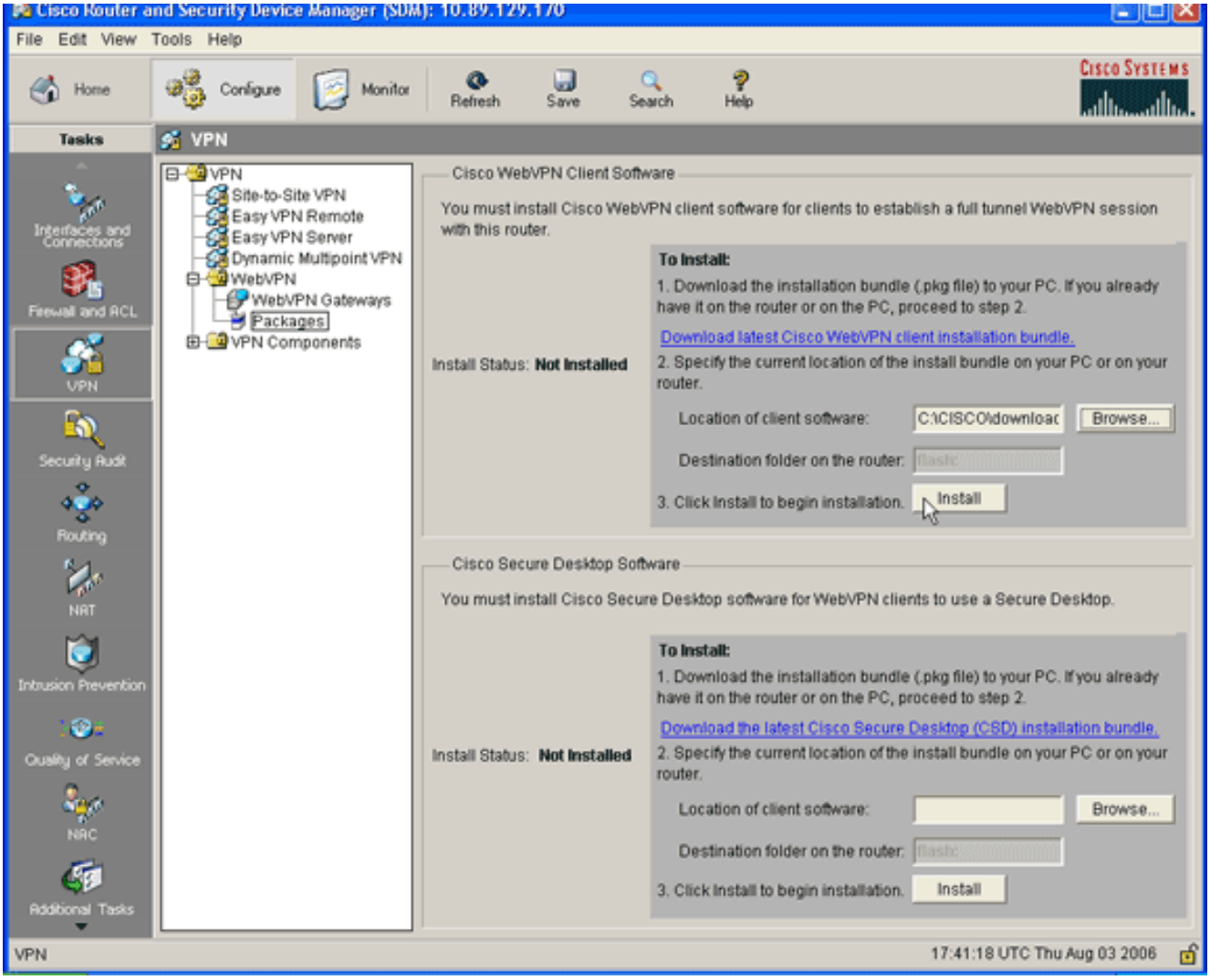
1. Open de toepassing sdm, klik **Configureren** en klik vervolgens op **VPN**.
2. Vul **WebVPN** uit en kies **pakketten**.



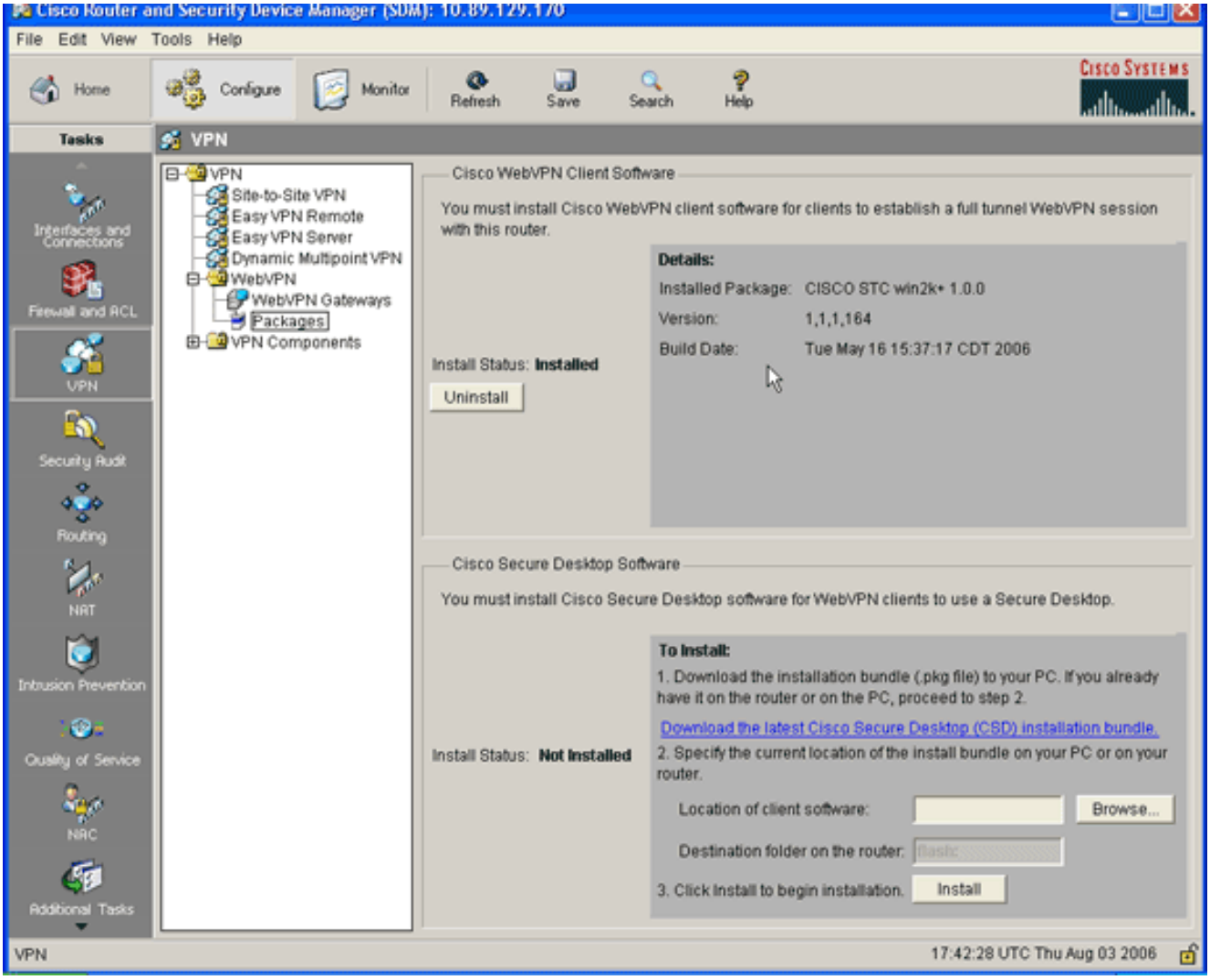
3. Klik in het gebied Cisco WebVPN Client Software op de knop **Bladeren**.Het dialoogvenster Zoeken naar SVC-locatie verschijnt.



4. Klik op de knop **Deze computer** en klik vervolgens op **Bladeren** om het SVC-pakket op uw beheerpc te vinden.
5. Klik op **OK** en vervolgens op de knop **Installeer**.



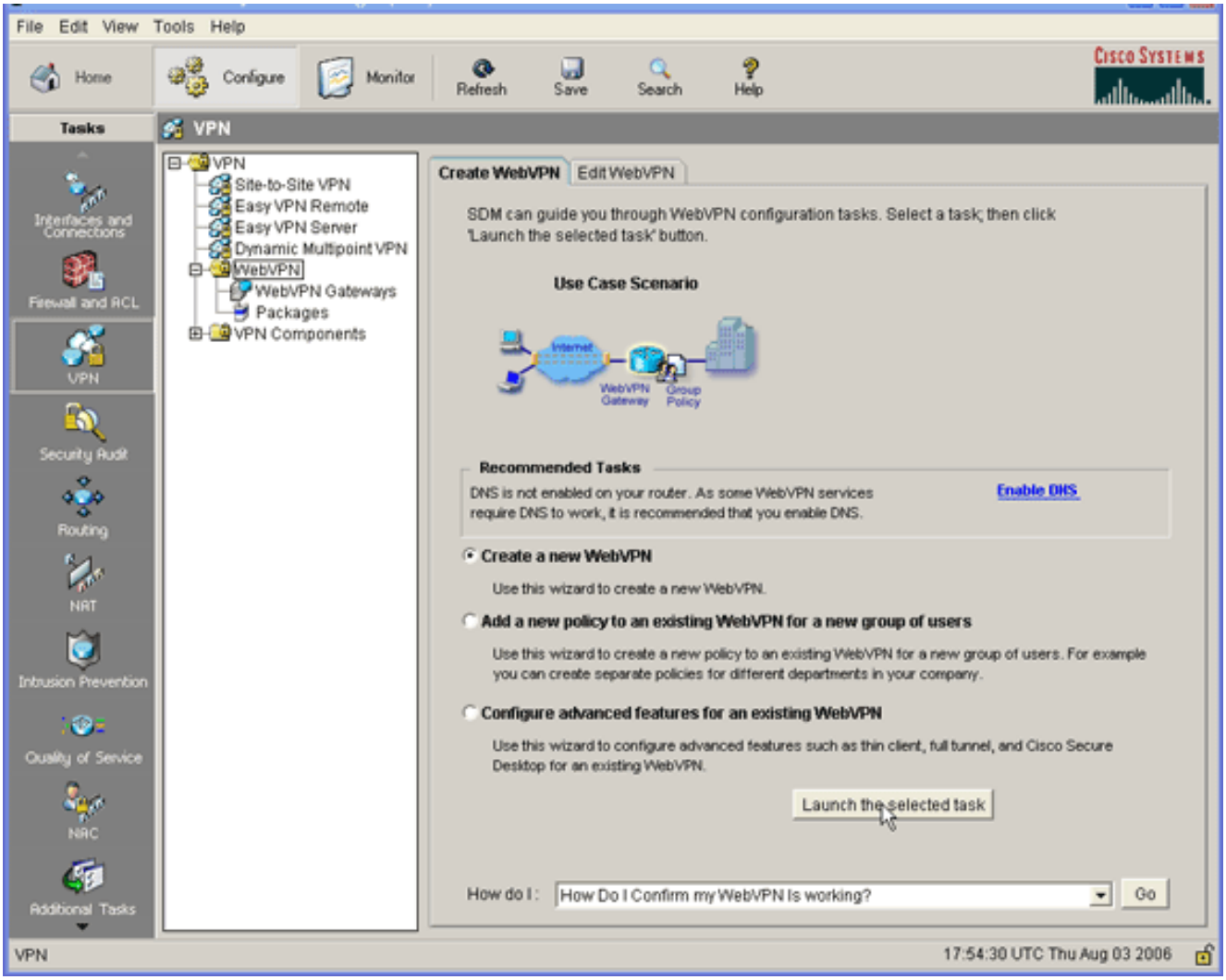
6. Klik op **Ja** en vervolgens op **OK**.Een geslaagde installatie van het SVC-pakket wordt in deze afbeelding
   weergegeven:



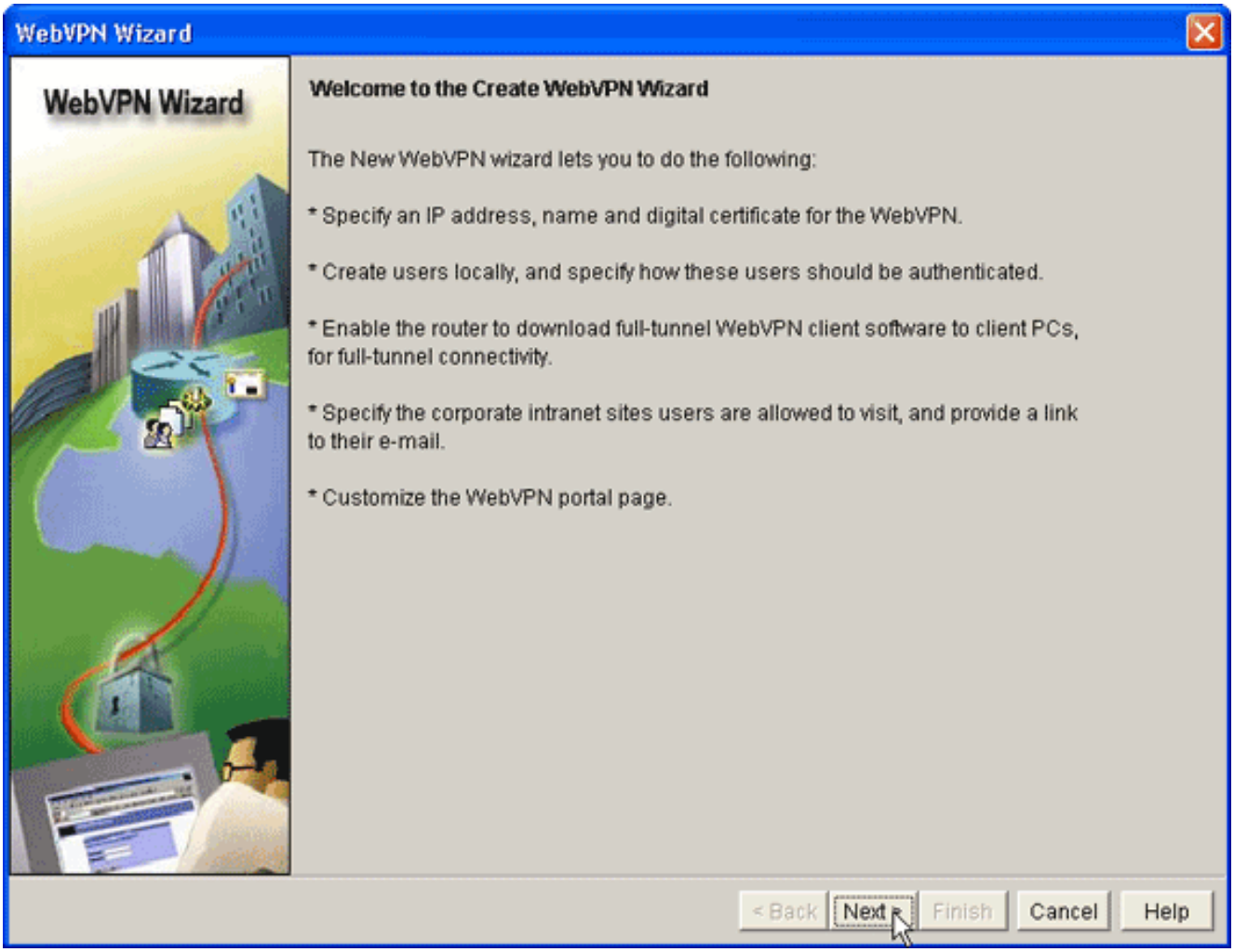
Stap 2. Configureer een WebVPN-context en gateway voor Webex met de wizard

Voltooi deze stappen om een WebVPN-context en een WebVPN-gateway te configureren:

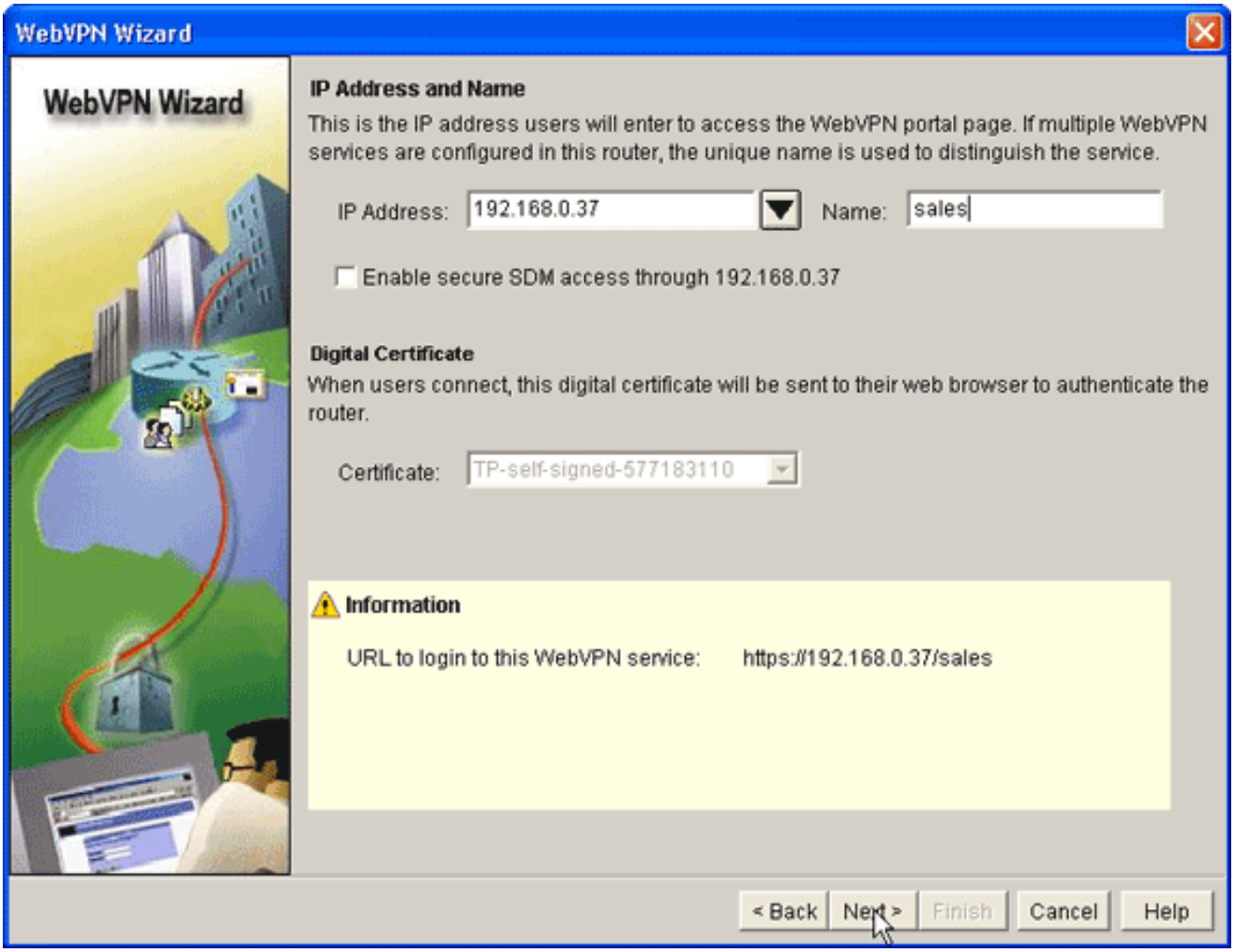
1. Nadat de SVC op de router is geïnstalleerd, klikt u op **Configureren** en vervolgens klikt u op **VPN**.
2. Klik op **WebVPN** en klik op het tabblad **WebVPN maken**.



3. Controleer de radioknop **Nieuw WebVPN** en klik vervolgens op **Start de geselecteerde taak**.Het dialoogvenster Wizard Webex verschijnt.



4. Klik op **Volgende**.



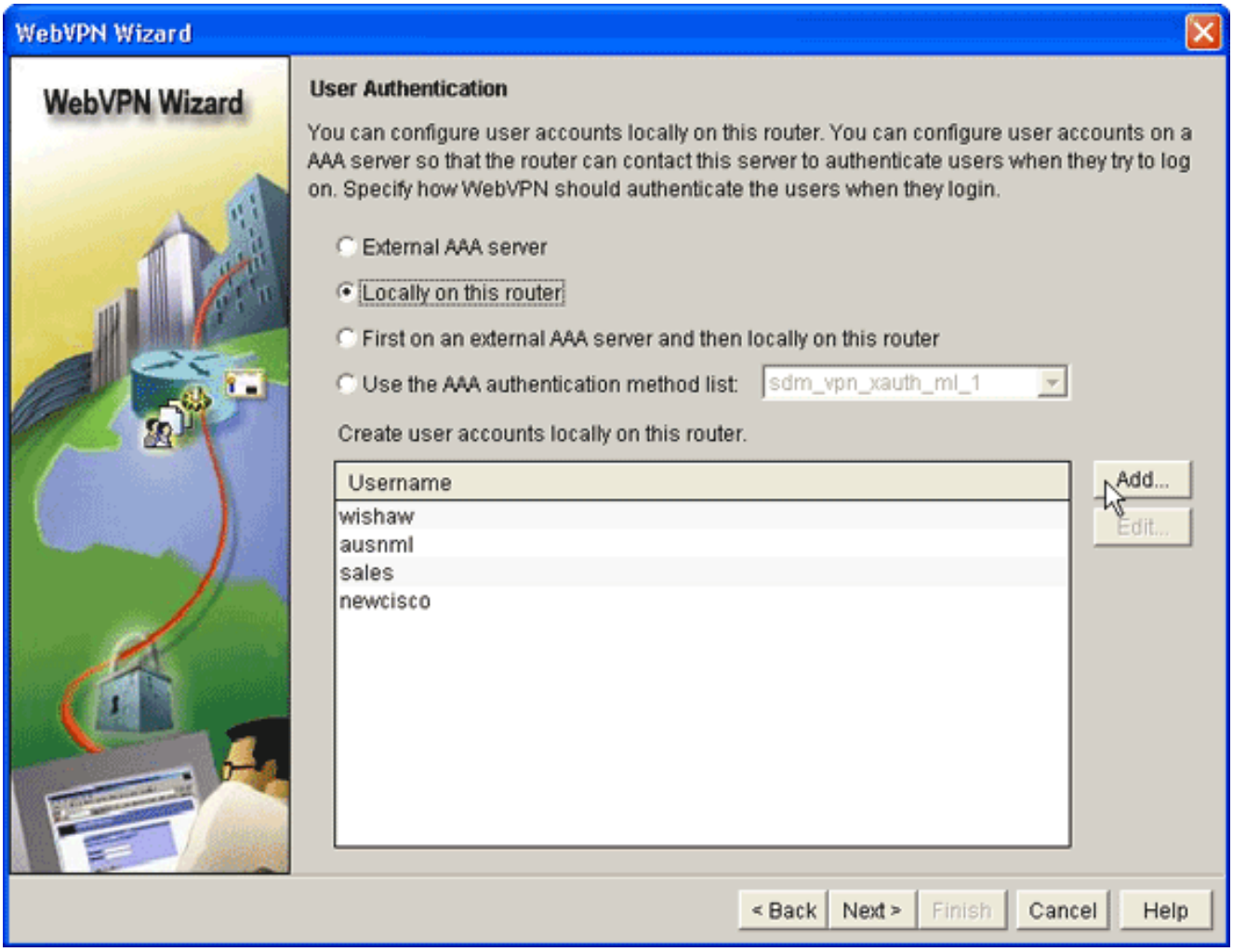
5. Voer het IP-adres van de nieuwe WebVPN-gateway in en voer een unieke naam voor deze WebVPN-context in.U kunt verschillende WebVPN-contexten maken voor hetzelfde IP-adres (WebVPN-gateway), maar elke naam moet uniek zijn. Dit voorbeeld gebruikt dit IP-adres: *https://192.168.0.37/sales*
6. Klik op **Volgende** en ga verder naar Stap 3.

Stap 3. Configureer de gebruikersdatabase voor SVC-gebruikers

Voor verificatie kunt u een AAA-server, lokale gebruikers of beide gebruiken. Dit configuratievoorbeeld gebruikt lokaal gemaakte gebruikers voor authenticatie.

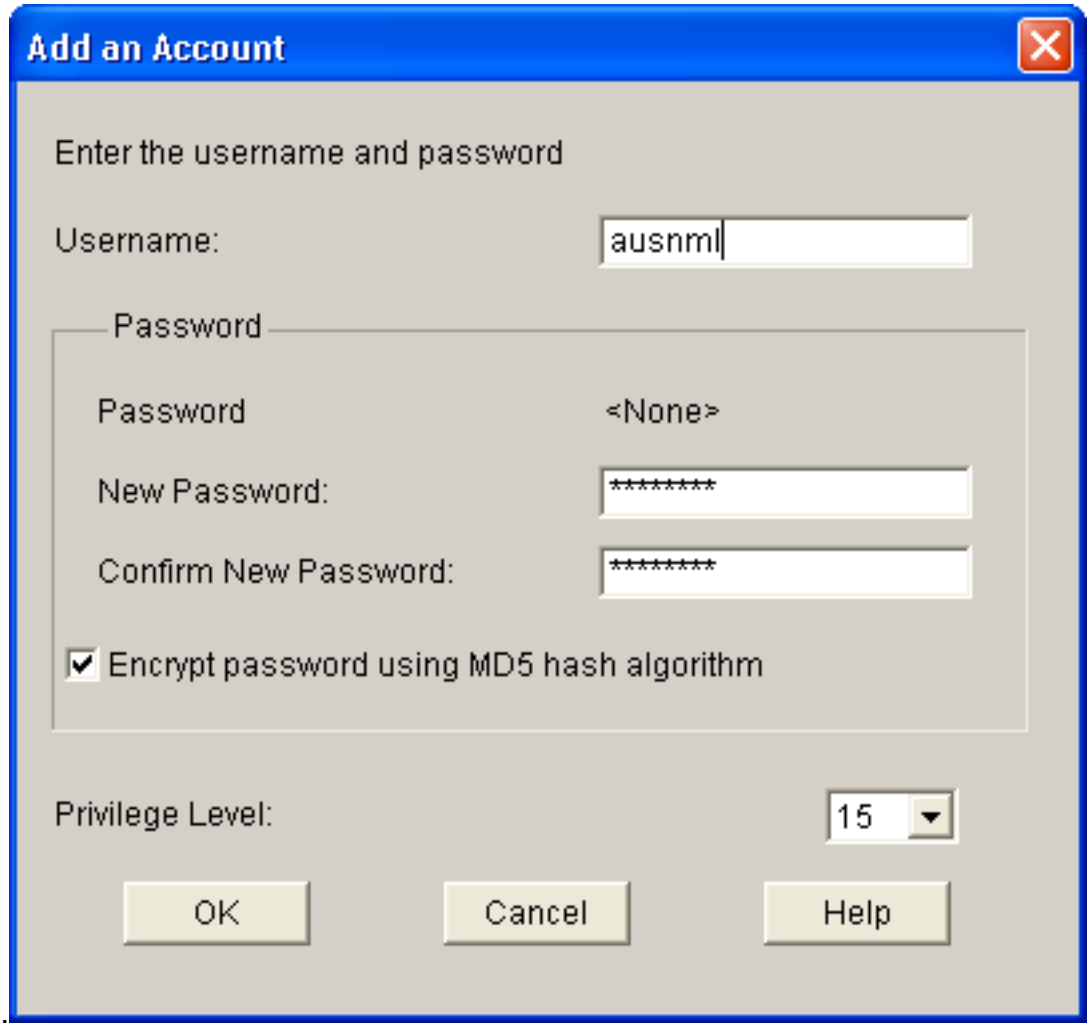
Volg deze stappen om de gebruikersdatabase voor SVC-gebruikers te configureren:

1. Nadat u Stap 2 hebt voltooid, klikt u **op het** selectieknop **Locally op deze router** in het dialoogvenster WEBVPN Wizard Gebruikersverificatie.



In dit dialoogvenster kunt u gebruikers aan de lokale database toevoegen.

2. Klik op **Add** en voer gebruikersinformatie



in.

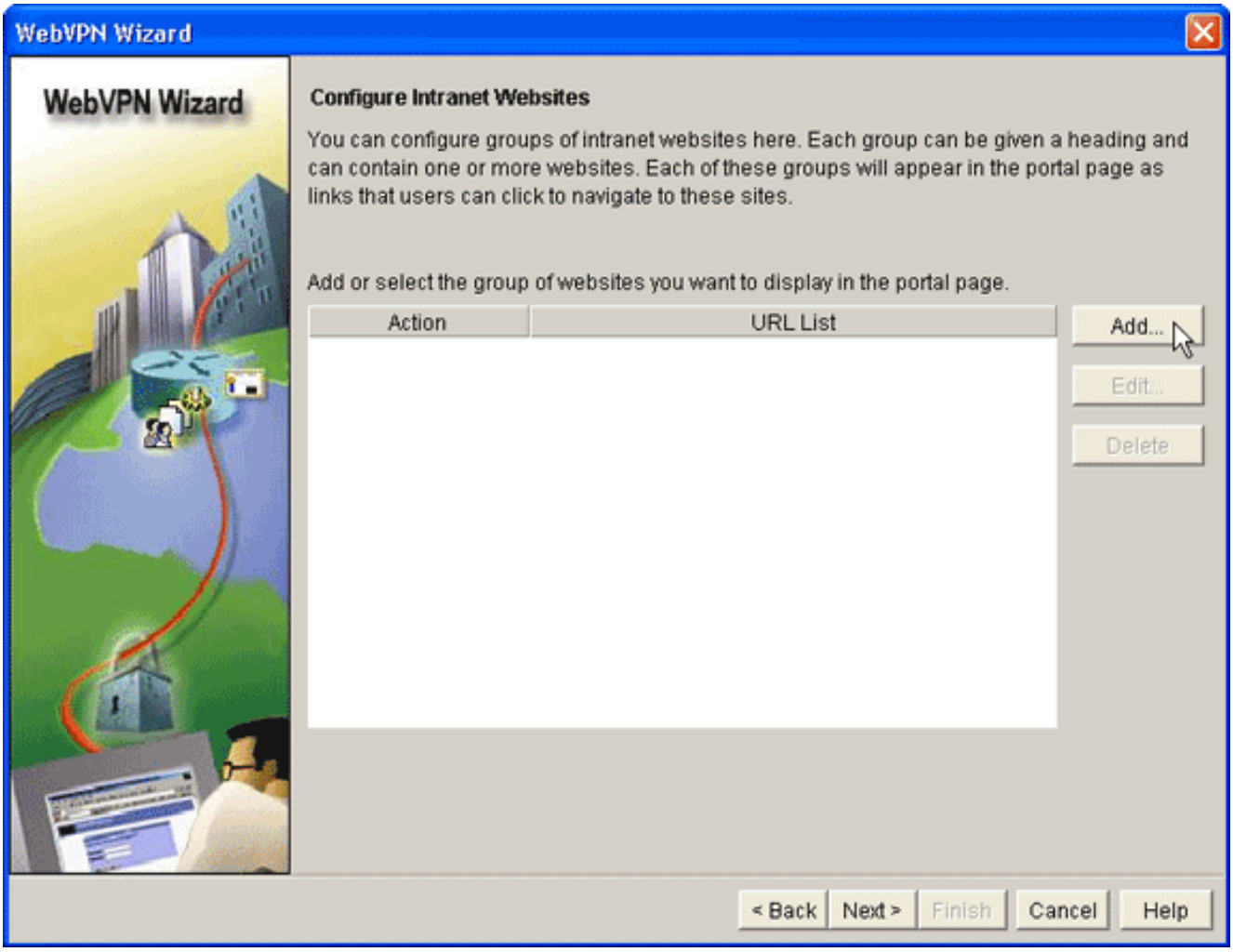
3. Klik op **OK** en voeg indien nodig extra gebruikers toe.
4. Nadat u de benodigde gebruikers hebt toegevoegd, klikt u op **Volgende** en vervolgens gaat u verder naar Stap 4.

Stap 4. Configureer de bronnen om deze aan gebruikers bloot te stellen

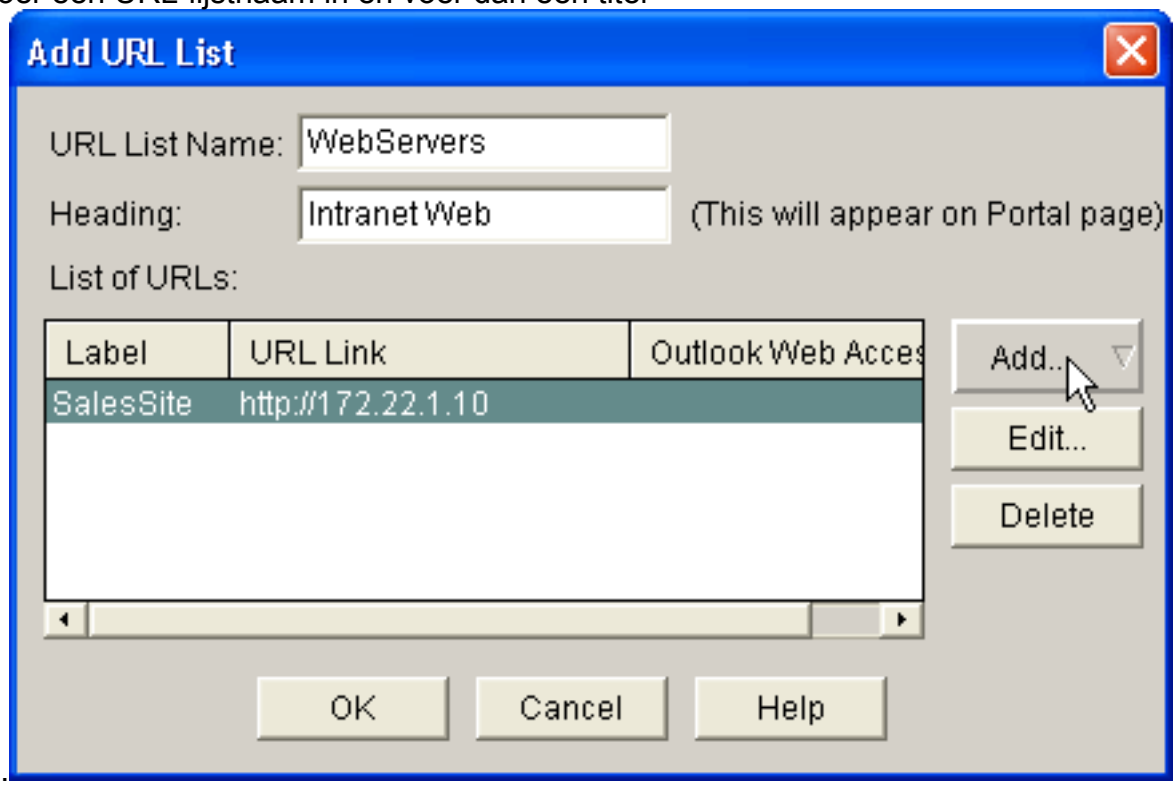
Met het dialoogvenster Intranet Websites WebVPN configureren kunt u de intranetbronnen selecteren die u aan uw SVC-clients wilt blootstellen.

Voltooi deze stappen om de bronnen aan te passen om gebruikers bloot te stellen:

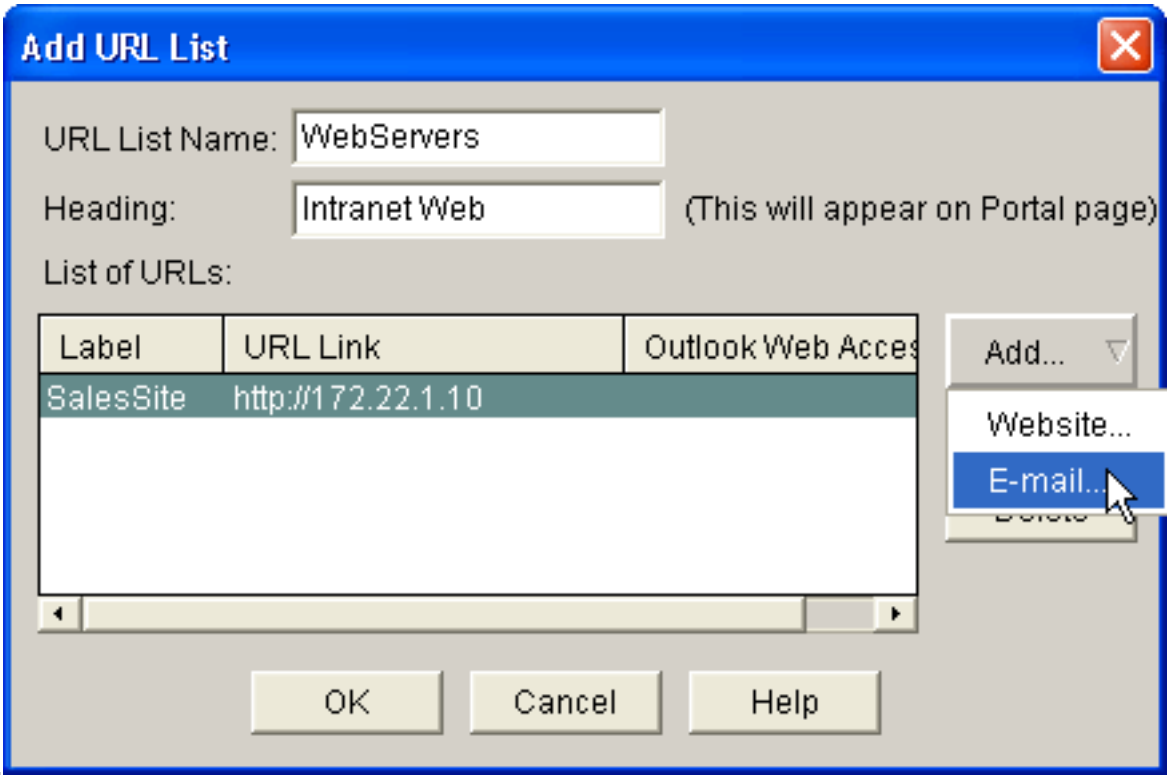
1. Nadat u Stap 3 hebt voltooid, klikt u op de knop **Add** in het dialoogvenster Intranet websites.



2. Voer een URL-lijstnaam in en voer dan een titel in.

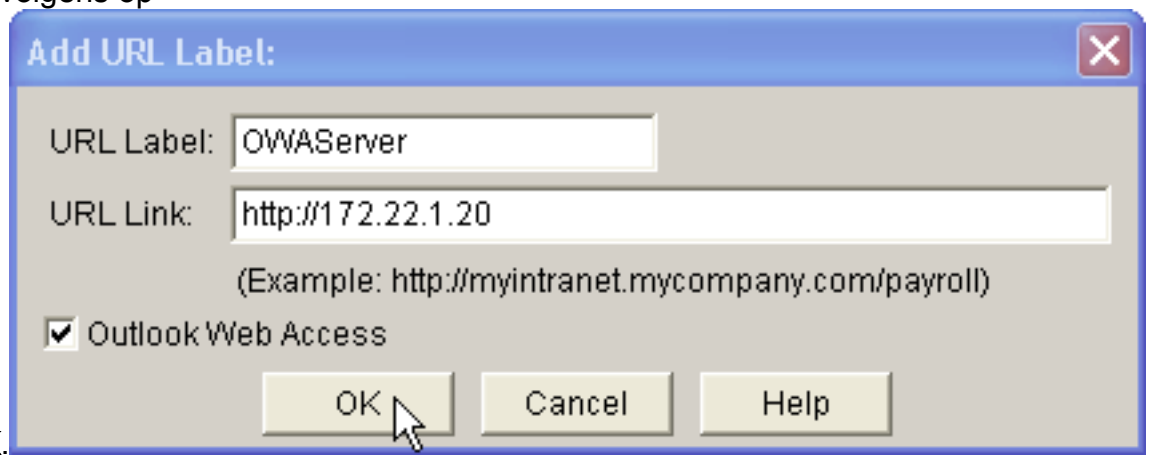


3. Klik op **Add** en kies **Website** om de websites toe te voegen die u aan deze client wilt blootstellen.
4. Voer URL en link informatie in en klik vervolgens op **OK**.
5. Als u toegang tot andere WO-uitwisselingsservers wilt toevoegen, klikt u op **Toevoegen** en vervolgens kiest u **e-**



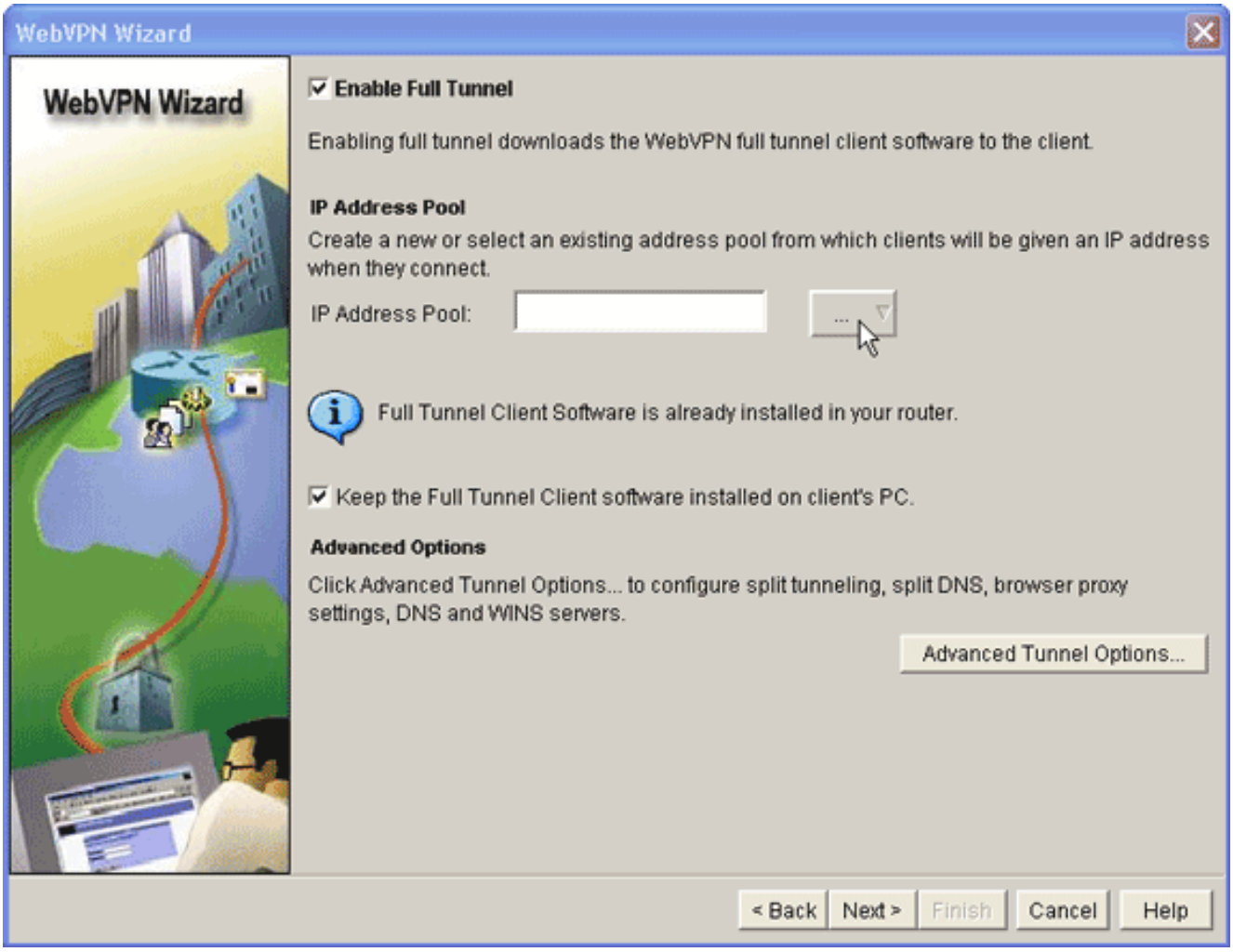
mail.

6. Controleer het aanvinkvakje **Outlook Web Access**, voer het URL-label en de link in en klik vervolgens op

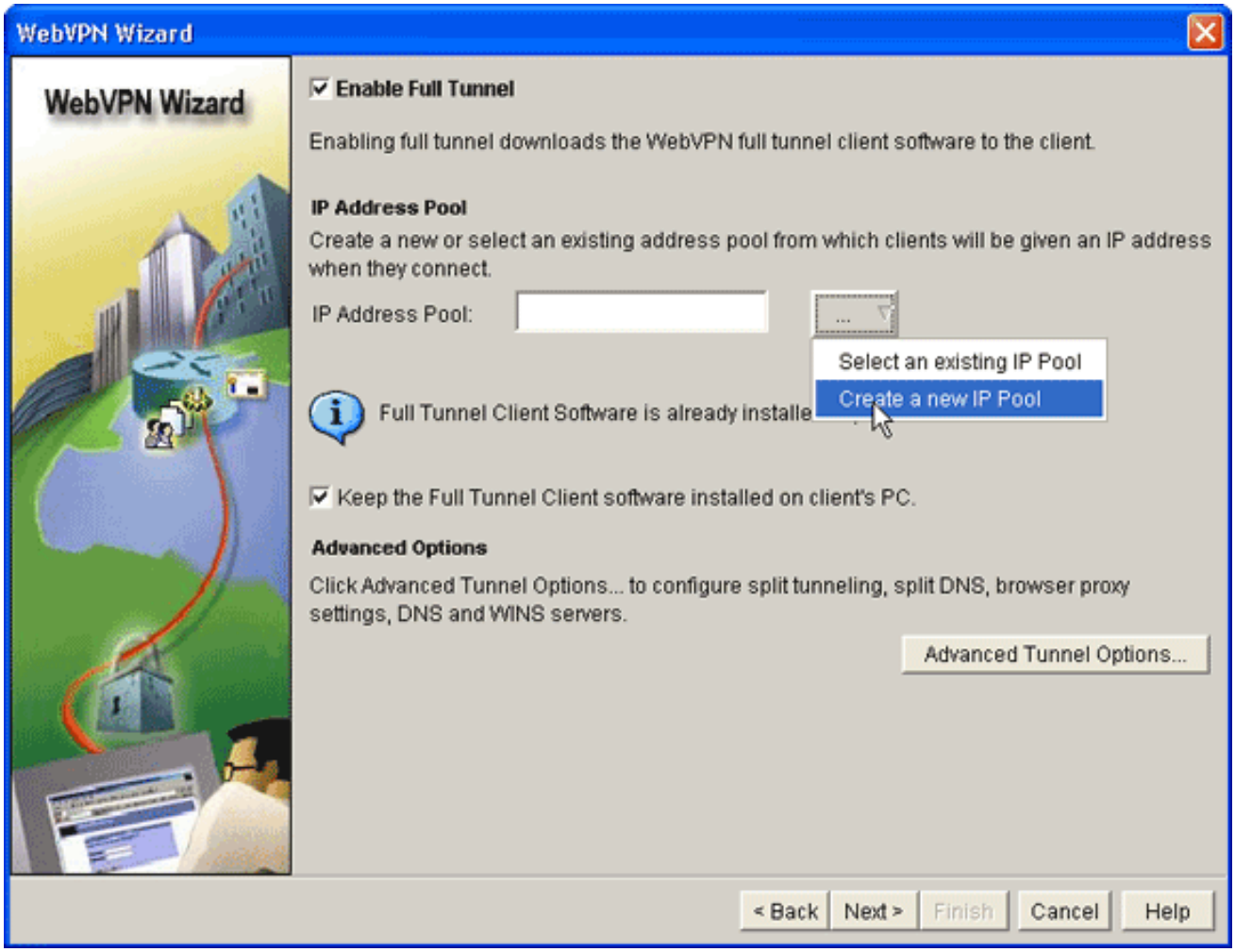


OK.

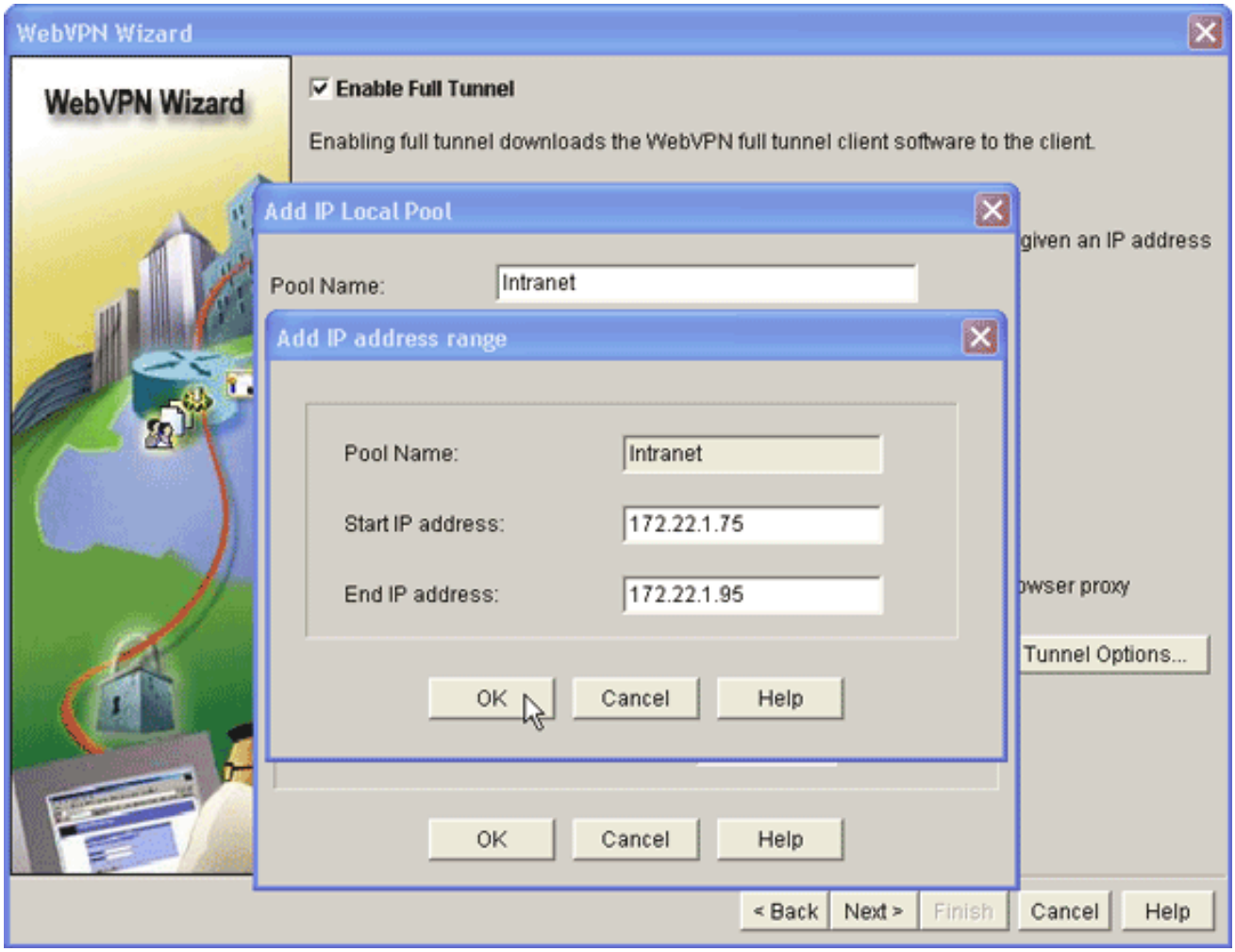
7. Nadat u de gewenste bronnen hebt toegevoegd, klikt u op **OK** en vervolgens klikt u op **Volgende**.Het volledige venster van de Wizard WebVPN verschijnt.



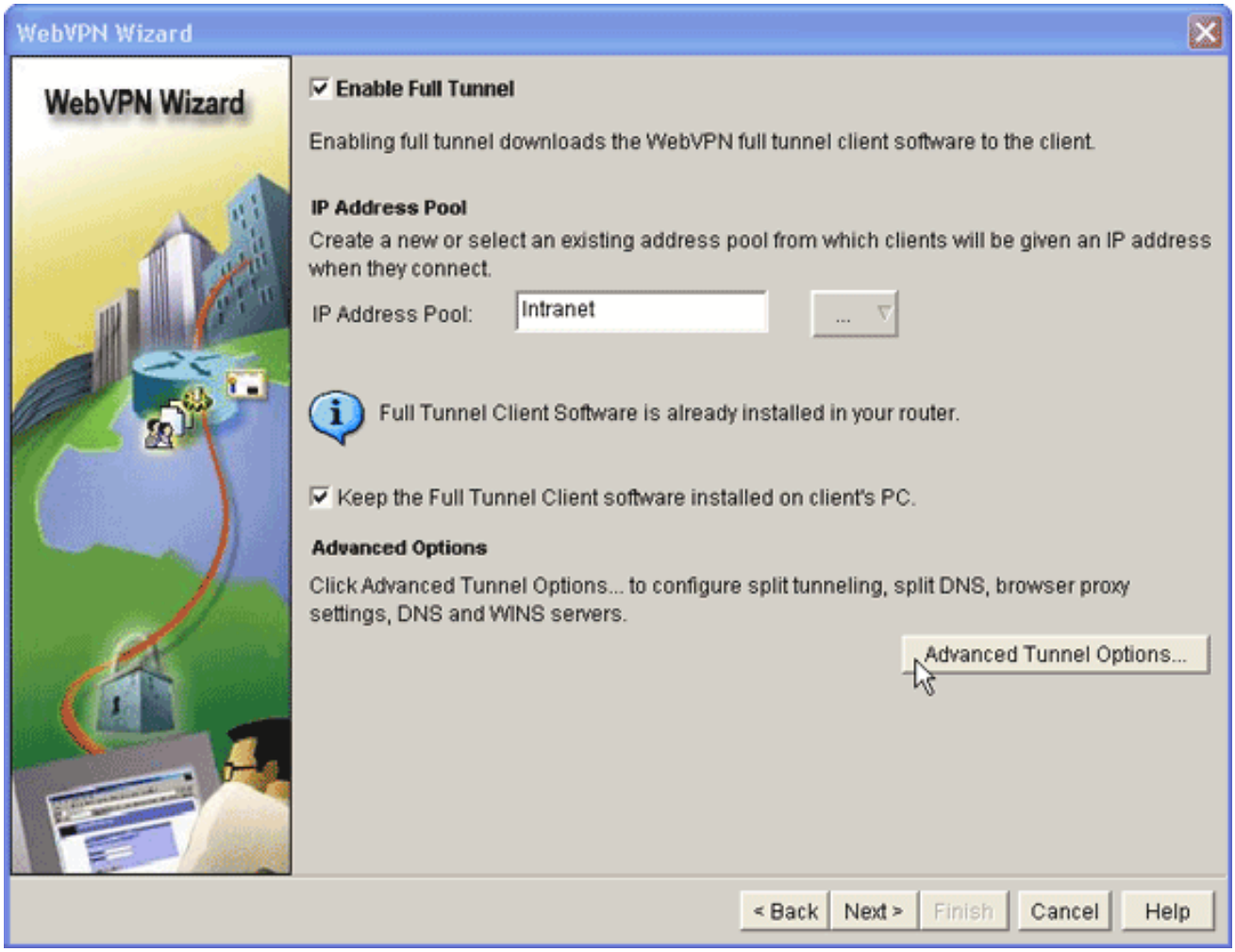
8. Controleer of het vakje **Full Tunnel inschakelen** is ingeschakeld.
9. Maak een pool van IP adressen die klanten van deze WebVPN context kunnen gebruiken. Het adressenbestand moet overeenkomen met de adressen die beschikbaar en routeerbaar zijn op uw intranet.
10. Klik op de ellips (**...**) naast het veld IP-adresgroep en kies **Een nieuwe IP-pool maken**.



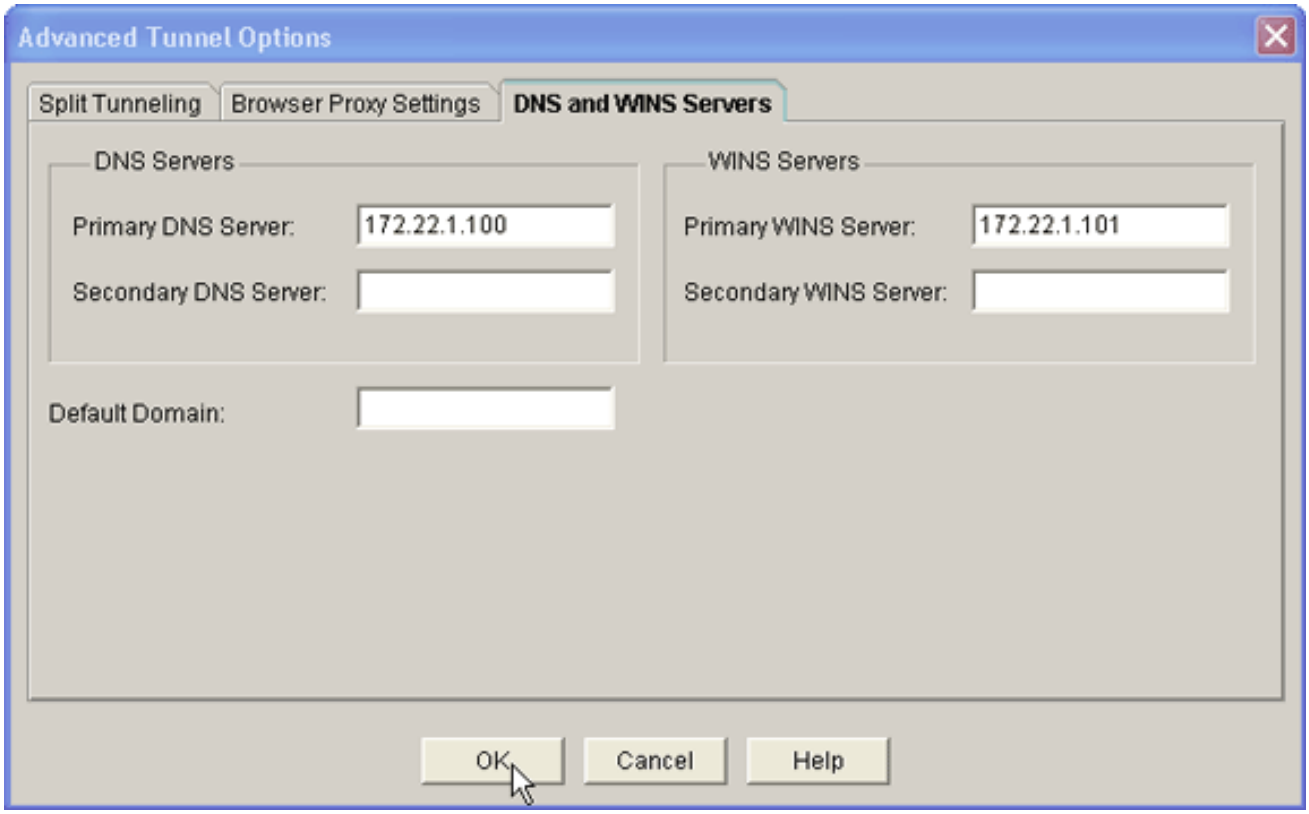
11. Typ in het dialoogvenster Local Pool toevoegen een naam voor de pool en klik op **Add**.



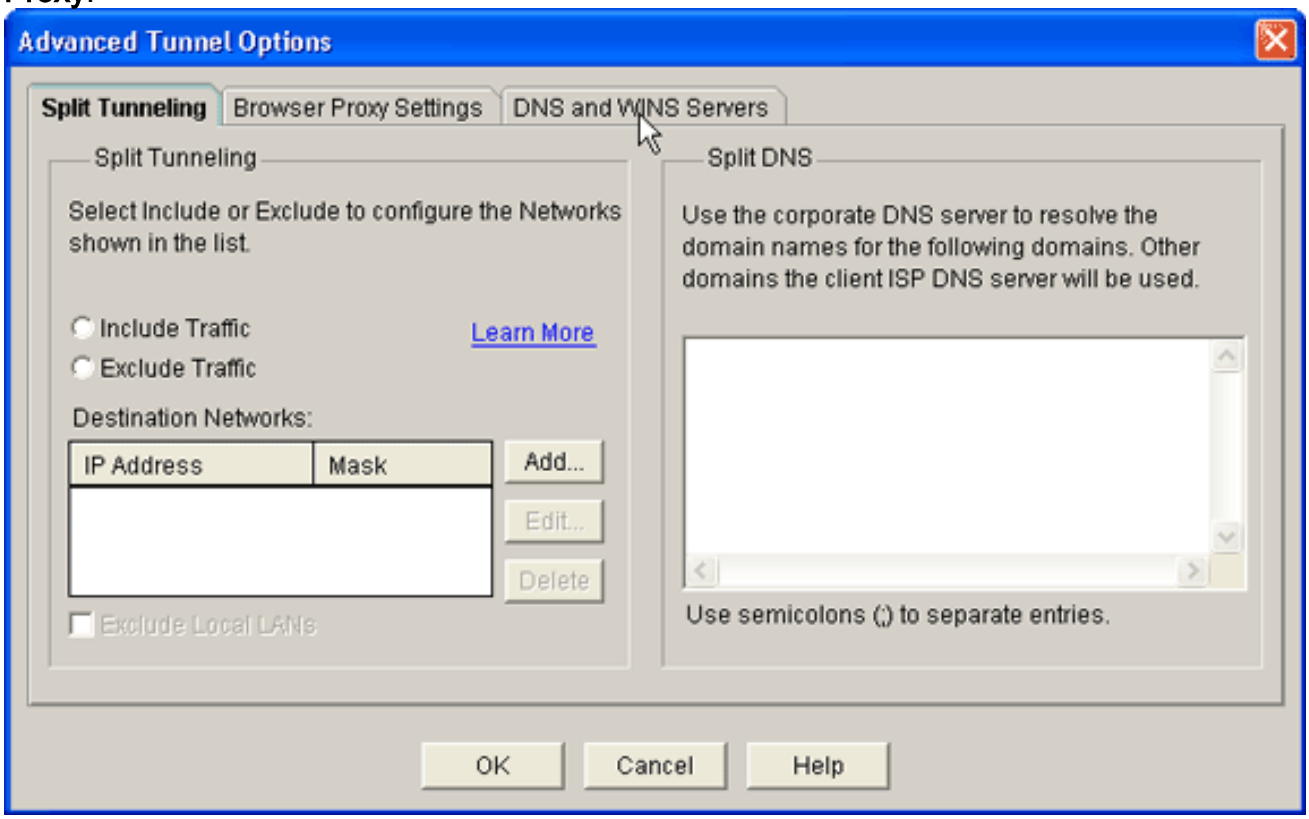
12. In het dialoogvenster IP-adresbereik toevoegen specificeert u het bereik van de adrespool voor de SVC-clients en vervolgens klikt u op **OK**.**Opmerking:** Het IP-adresbestand moet in een bereik van een interface zijn die rechtstreeks op de router is aangesloten. Als u een ander poolbereik wilt gebruiken, kunt u een loopback-adres maken dat aan uw nieuwe pool is gekoppeld om aan deze eis te voldoen.
13. Klik op
    OK.



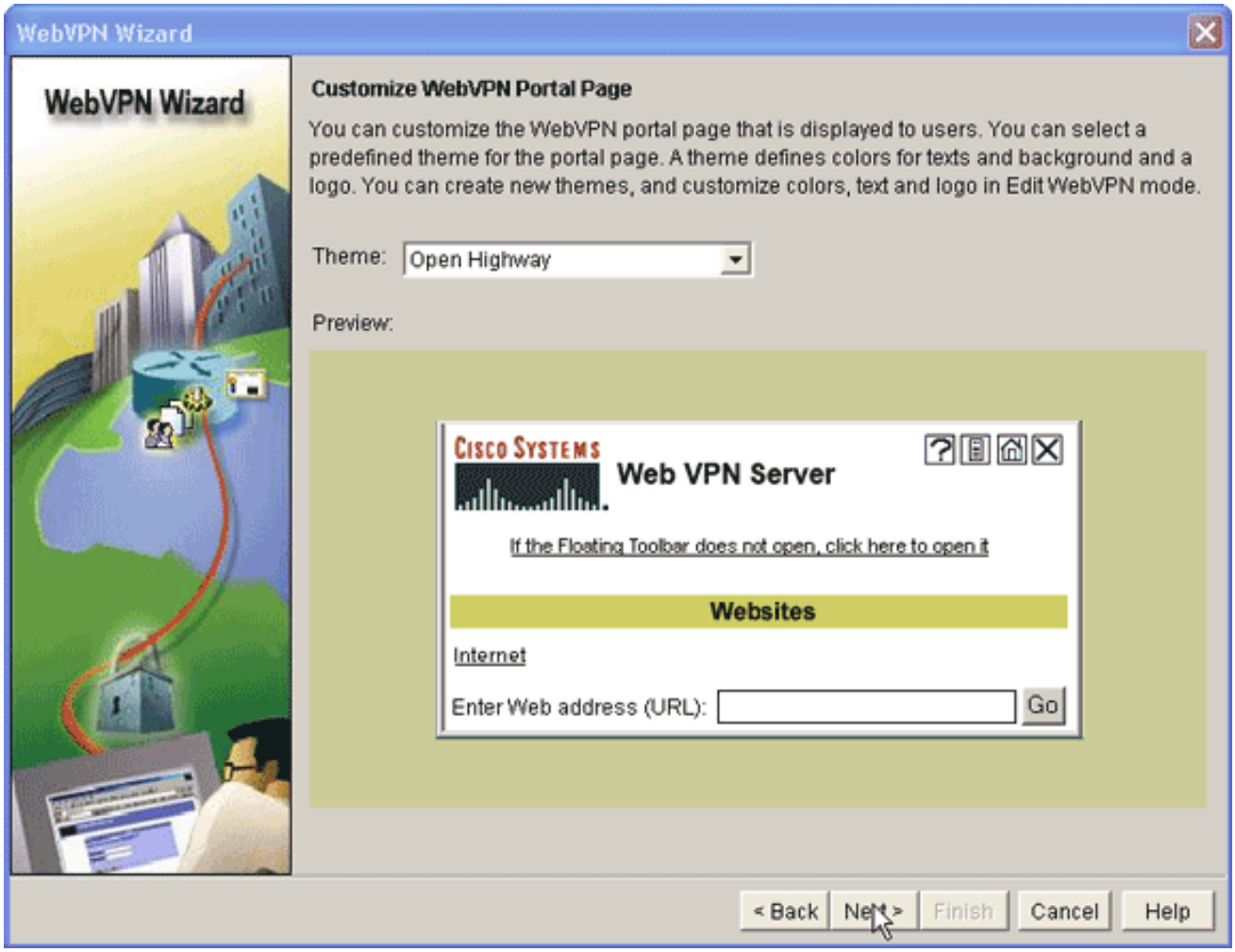
14. Als u wilt dat uw externe clients een kopie van de SVC permanent opslaan, klikt u op het aanvinkvakje **De volledige tunnelclientsoftware** die **op de PC van de client is geïnstalleerd**. Schakel deze optie uit om van de client te eisen dat u de SVC-software downloaden telkens wanneer een client aansluit.
15. Configureer geavanceerde tunnelopties, zoals gesplitste tunneling, gesplitste DNS, browser proxy-instellingen en DNS- en WNS-servers. Cisco raadt u aan ten minste DNS- en WINS-servers te configureren.Voltooi de volgende stappen om geavanceerde tunnelopties te configureren:Klik op de knop **Geavanceerde tunnelopties**.



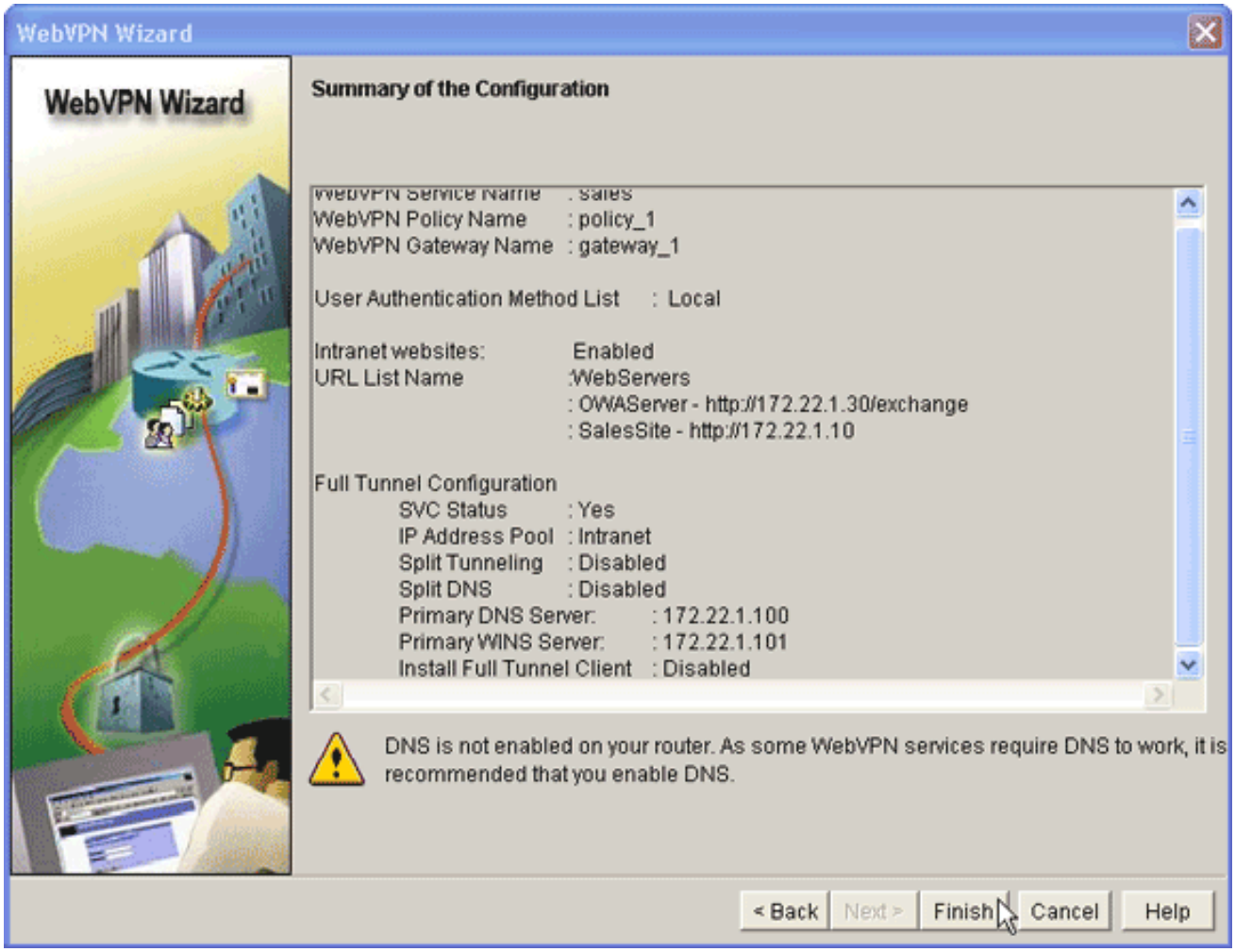
Klik op het tabblad **DNS en WINS Server** en voer de primaire IP-adressen in voor de DNS- en WINS-servers.Om gesplitste tunneling en browser proxy instellingen te configureren klikt u op het tabblad **Split Tunneling** of **browser Proxy**.



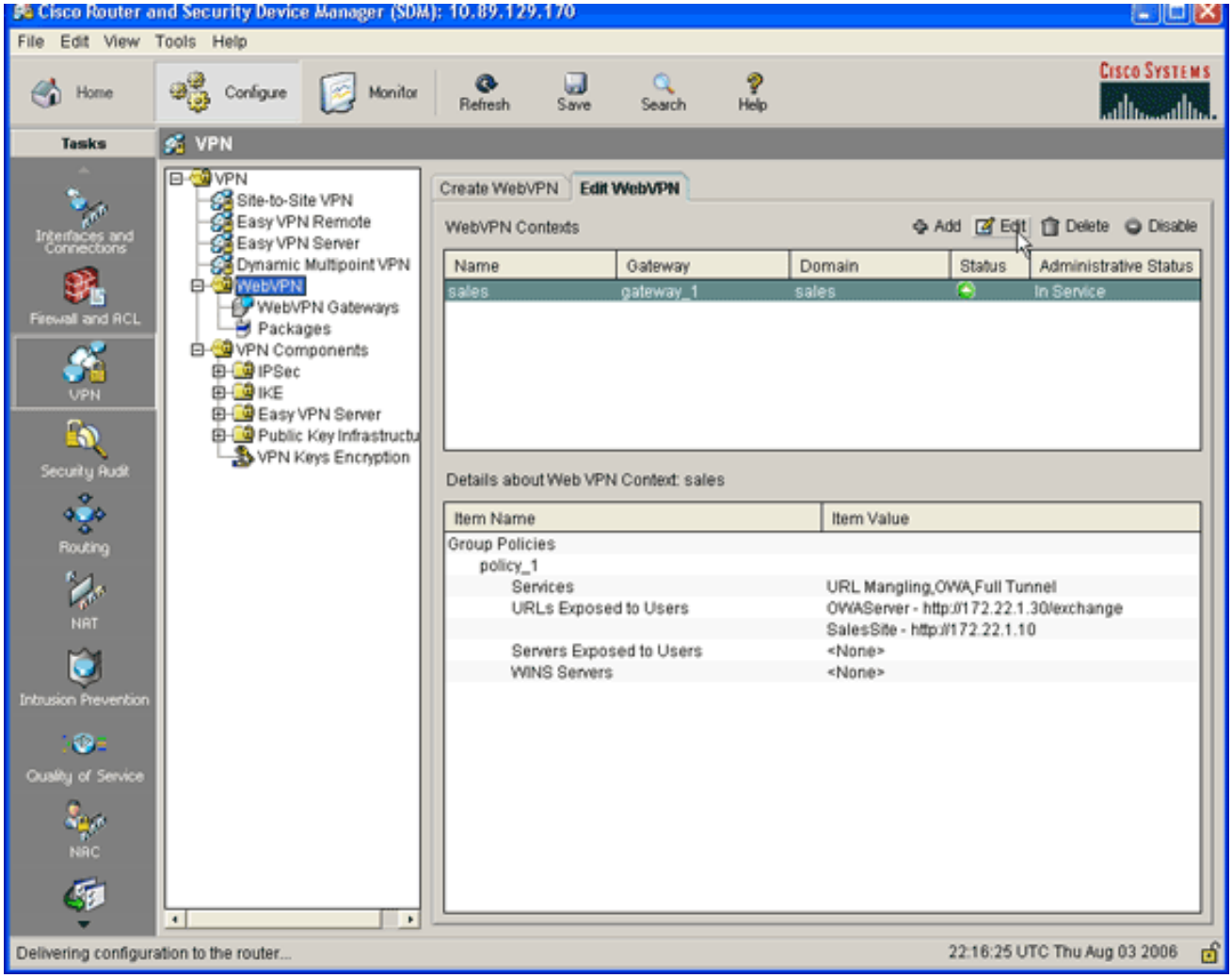
16. Nadat u de gewenste opties hebt ingesteld, klikt u op **Volgende**.
17. Pas de WebVPN Portal Pagina aan of selecteer de standaardwaarden.Met de Portal Pagina's van WebVPN aanpassen kunt u uw klanten aanpassen hoe de WebVPN-portal-pagina wordt
weergegeven.



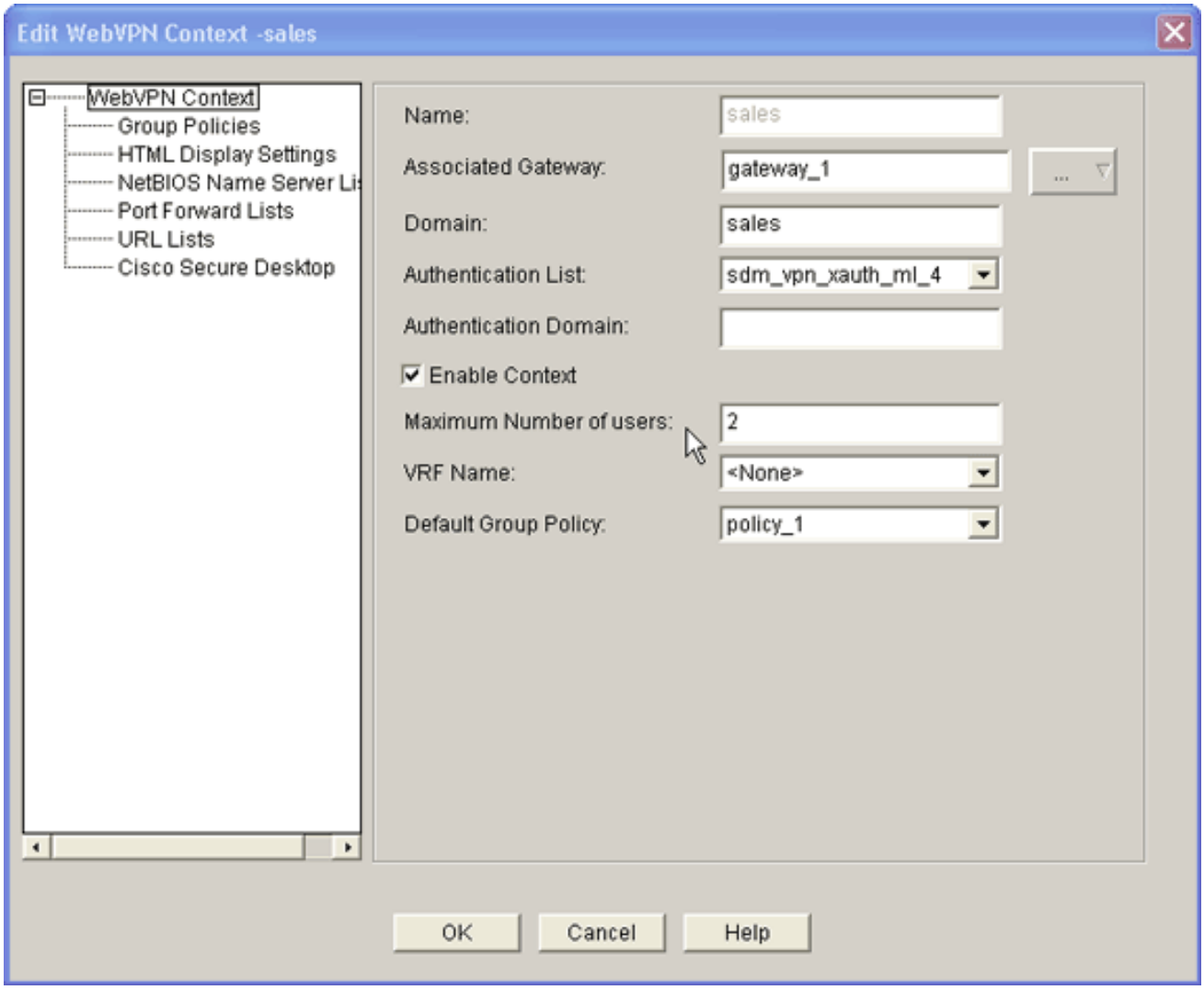
18. Nadat u de WebVPN Portal pagina hebt configureren klikt u op **Volgende**, klikt u op **Voltooien** en vervolgens klikt u op **OK**.De wizard van WebVPN geeft tour opdrachten door aan de router.
19. Klik op **OK** om de configuratie op te slaan.**N.B.:** Als u een foutbericht ontvangt, is de WebVPN-licentie mogelijk onjuist. In deze afbeelding wordt een foutmelding weergegeven:



Voltooi de volgende stappen om een licentieafgifte te corrigeren:Klik op **Configureren** en vervolgens op **VPN**.Vul **WebVPN** uit en klik op het tabblad **WebVPN bewerken**.



Markeer de nieuwe context en klik op de knop **Bewerken**.



Typ in het veld Maximum aantal gebruikers het juiste aantal gebruikers voor uw licentie.Klik op **OK** en vervolgens op **OK**.Uw opdrachten worden naar het configuratiebestand geschreven.Klik op **Opslaan** en vervolgens op **Ja** om de wijzigingen te aanvaarden.

Resultaten

ASDM maakt deze opdrachtregel-configuraties:

ausnml-3825-01

```
ausnml-3825-01#show run
Building configuration...

Current configuration : 4393 bytes
!
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
```

```
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
!
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server ip http timeout-policy idle 600 life 86400
requests 100 ! control-plane ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
```

```
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Procedure

Om uw configuratie te testen, voer *http://192.168.0.37/sales* in in een SSL-enabled browser van het clientWeb.

Opdrachten

Verschillende **tonen** opdrachten worden geassocieerd met WebVPN. U kunt deze opdrachten uitvoeren op de opdrachtregel-interface (CLI) om statistieken en andere informatie weer te geven. Raadpleeg voor gedetailleerde informatie over opdrachten **voor het** weergeven van de configuratie van WebVPN.

Opmerking: Uitvoer Tolk (alleen geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

SSL-connectiviteitsprobleem

Probleem: SSL VPN-clients zijn niet in staat de router aan te sluiten.

Oplossing: Onvoldoende IP-adressen in de IP-adrespool kunnen dit probleem veroorzaken. Vergroot het aantal IP adressen in het pool van IP adressen op de router om dit probleem op te lossen.

Opdrachten voor troubleshooting

Verschillende **heldere** opdrachten worden geassocieerd met WebVPN. Raadpleeg voor gedetailleerde informatie over deze opdrachten de optie Opdrachten wissen via WebVPN.

Meerdere **debug** opdrachten zijn gekoppeld aan WebVPN. Raadpleeg voor gedetailleerde informatie over deze opdrachten het gebruik van Debug Commands van WebVPN.

Opmerking: het gebruik van **debug-**opdrachten kan een negatieve invloed hebben op uw Cisco-apparaat. Voordat u **debug**-opdrachten gebruikt, raadpleegt u Belangrijke informatie over Debug Commands.

Gerelateerde informatie

- Cisco IOS VPN-SLVPN
- SSL VPN - WebVPN
- Clientloze SSL VPN (WebexVPN) op Cisco IOS met het Configuratievoorbeeld van DHCP
- Thin-Client SSL VPN (WebVPN) IOS Configuration-voorbeeld met DSM
- Implementatiegids voor Webex en DMVPN-conversie
- Technische ondersteuning en documentatie – Cisco Systems