Configuratie van Thin-Client SSL VPN (WebVPN) Cisco IOS met DSM

Inhoud

Inleiding

Thin-Client SSL VPN-technologie kan worden gebruikt om beveiligde toegang toe te staan voor toepassingen die statische poorten gebruiken. Voorbeelden hiervan zijn telnet (23), SSH (22), POP3 (110), IMAP4 (143) en MTP (25). De Thin-Client kan door een gebruiker worden aangestuurd, of beide. De toegang kan per gebruiker worden ingesteld of groepsbeleid kan worden gemaakt dat een of meer gebruikers omvat. SSL VPN-technologie kan in drie hoofdmodi worden geconfigureerd: Clientloze SSL VPN (WebVPN), Thin-Client SSL VPN (Port Forwarding) en SSL VPN-client (SVC-Full Tunnel Mode).

1. Clientless SSL VPN (WebVPN):

Een externe client heeft alleen een SSL-enabled webbrowser nodig om toegang te krijgen tot http- of https-enabled-webservers op het LAN. Er is ook toegang beschikbaar om door te bladeren voor Windows-bestanden met het Common Internet File System (CIFS). Een goed voorbeeld van http toegang is de Outlook Web Access (OWA) client.

Verwijs naar Clientless SSL VPN (WebVPN) op Cisco IOS die het Voorbeeld van de Configuratie van het Configuratie SDM gebruikt om meer over Clientless SSL VPN te leren.

2. Thin-Client SSL VPN (Port Forwarding)

Een externe client moet een kleine, op Java gebaseerde applicatie downloaden voor beveiligde toegang tot TCP-toepassingen waarin statische poortnummers worden gebruikt. UDP wordt niet ondersteund. Tot de voorbeelden behoren toegang tot POP3, MTP, IMAP, SSH, en Telnet. De gebruiker heeft lokale beheerrechten nodig omdat de wijzigingen in bestanden op de lokale machine worden aangebracht. Deze methode van SSL VPN werkt niet met toepassingen die dynamische port opdrachten gebruiken, bijvoorbeeld, verscheidene FTP toepassingen.

3. SSL VPN-client (SVC-volledige tunnelmodus):

De SSL VPN-client downloads een kleine client naar het externe werkstation en biedt volledige en beveiligde toegang tot de resources op het interne bedrijfsnetwerk. De SVC kan permanent naar het externe station worden gedownload, of kan na de beveiligde sessie worden verwijderd.

Raadpleeg SSL VPN Client (SVC) op IOS die het Voorbeeld van de Configuration gebruiken om meer te weten te komen over de SSL VPN-client.

Dit document demonstreert een eenvoudige configuratie voor Thin-Client SSL VPN op een Cisco IOS® router. Het Thin-Client SSL VPN loopt op deze Cisco IOS-routers:

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

Voorwaarden

Vereisten

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

Vereisten voor de Cisco IOS-router

- Een van de vermelde routers die met DSM zijn geladen en een geavanceerde afbeelding van IOS versie 12.4(6)T of hoger
- Een beheerstation geladen met middel van een dmCisco vervoert nieuwe routers met een voorgeïnstalleerd exemplaar van PDM. Als uw router geen installeert heeft, kunt u de software bij Software downloaden-Cisco het apparaat van het Veiligheidsapparaat Manager verkrijgen. U moet een CCO-account met een servicecontract hebben. Raadpleeg het configureren van uw router met Security Devices Manager voor gedetailleerde instructies.

Eisen voor clientcomputers

- Afstandsklanten dienen lokale administratieve rechten te hebben; het is niet nodig , maar het is zeer gesuggereerd .
- Afstandsklanten moeten beschikken over Java Runtime Environment (JRE) versie 1.4 of hoger.
- Afstandsbrowsers: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 of Firefox 1.0
- Gebruikte koekjes en populaties toegestaan op externe klanten

Gebruikte componenten

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

- Cisco Advanced Enterprise-softwarerelease 12.4(9)T
- Cisco 3825 geïntegreerde services router
- Cisco Router en Security apparaat Manager (DSM) versie 2.3.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een gewiste (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen. De IP adressen die voor deze configuratie gebruikt worden komen van de RFC 1918 adresruimte. Ze zijn niet legaal op het internet.

Conventies

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

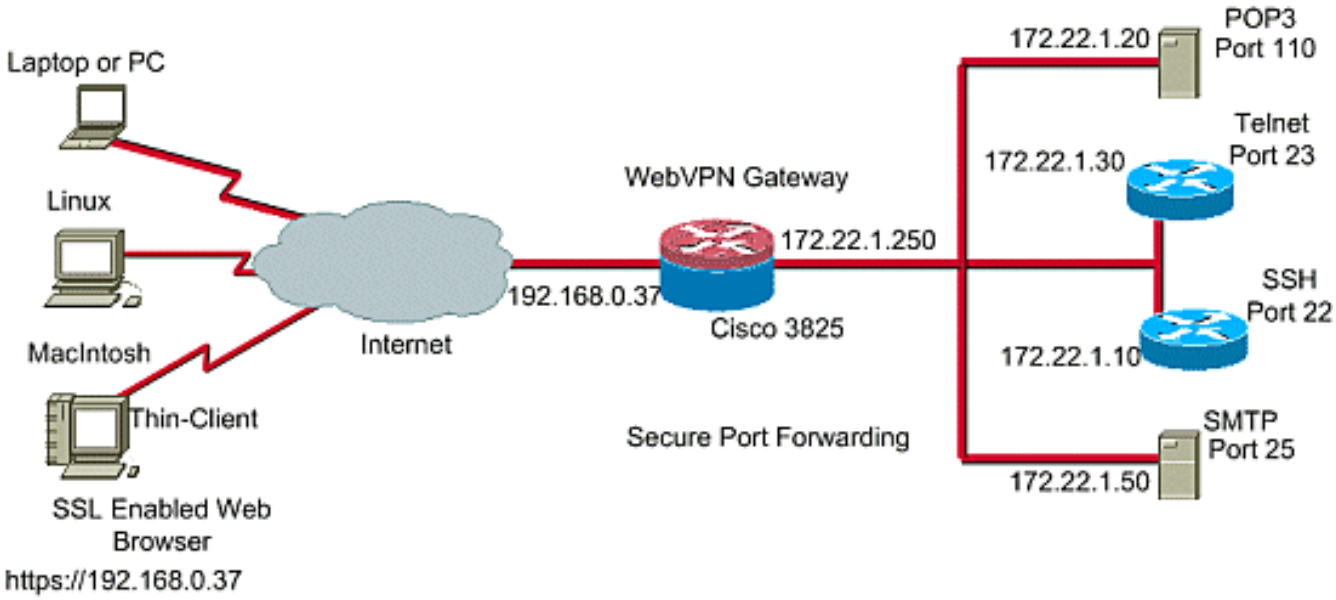
Configureren

Taak

Deze sectie bevat de informatie die nodig is om de functies te configureren die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

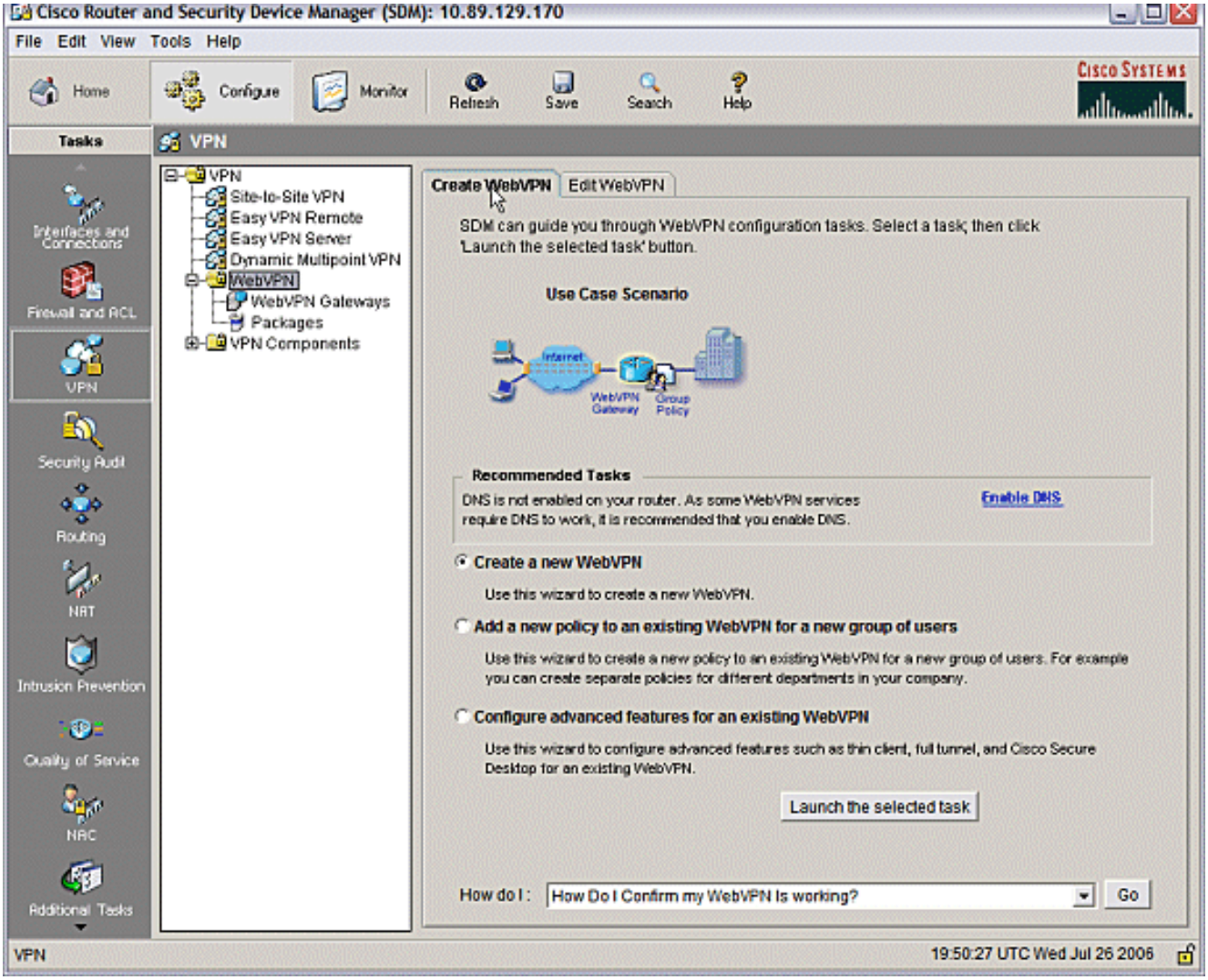


Het Thin-Client SSL VPN configureren

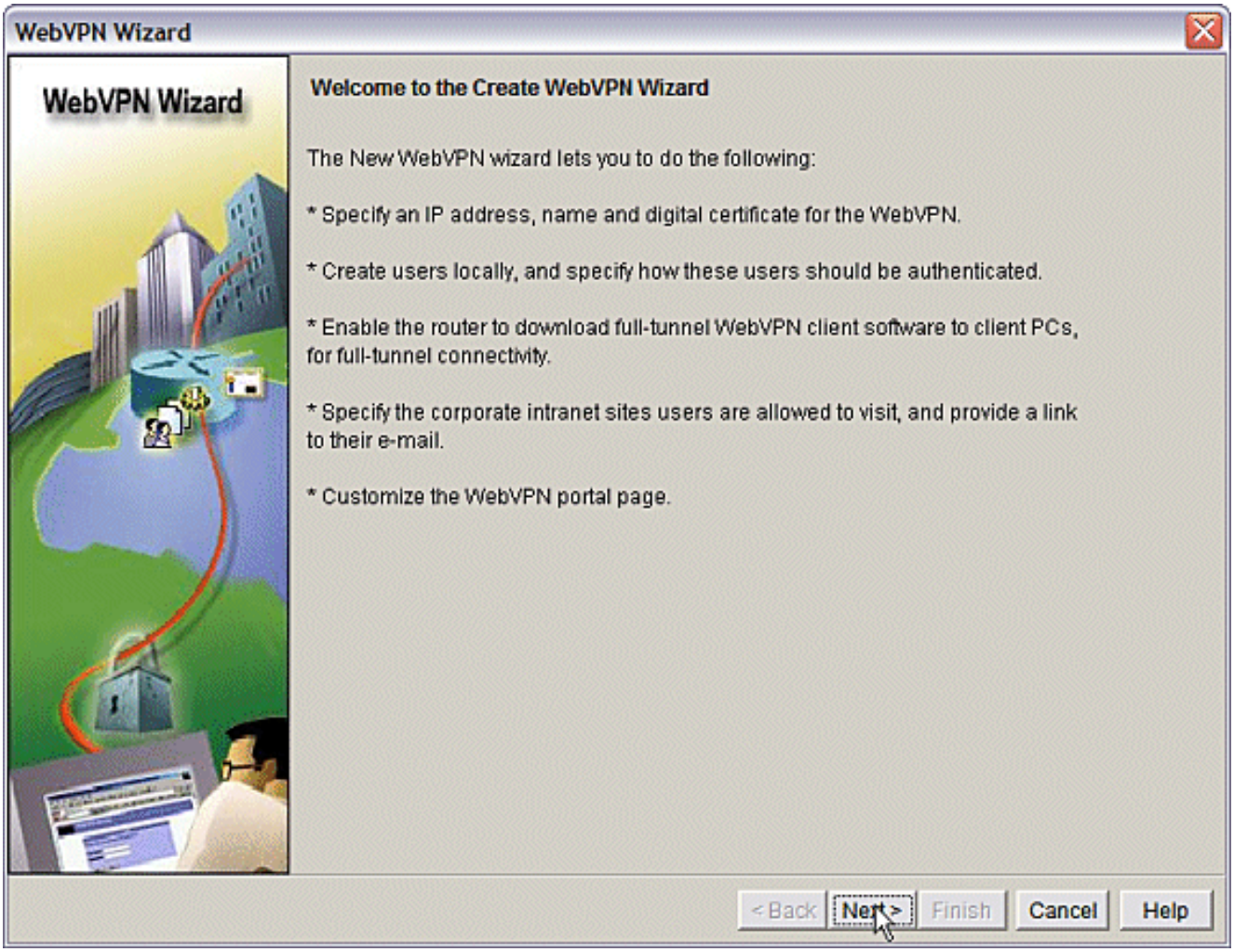
Gebruik de Wizard die in de interface Security Devices Manager (DSM) wordt meegeleverd om het Thin-Client SSL VPN op Cisco IOS te configureren of het op de Opdrachtlijn Interface (CLI) of handmatig in de DNS-toepassing te configureren. Dit voorbeeld gebruikt de Wizard.

1. Kies het tabblad **Configureren**.Kies in het navigatiedeelvenster **VPN > WebVPN**.Klik op het tabblad **WebVPN maken**.Klik op de radioknop naast **Create a new WebVPN**.Klik op de knop **De geselecteerde taak**

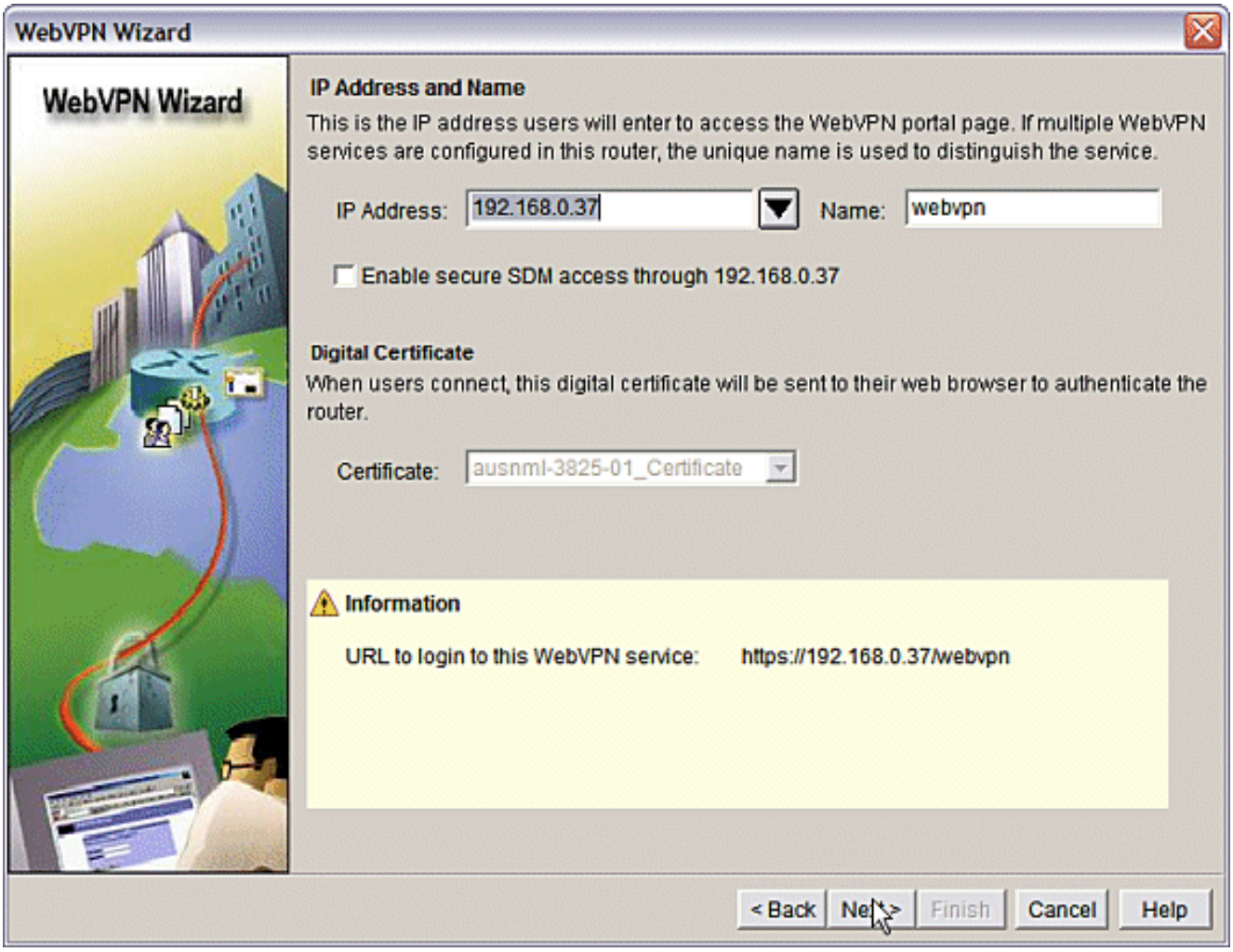
starten.



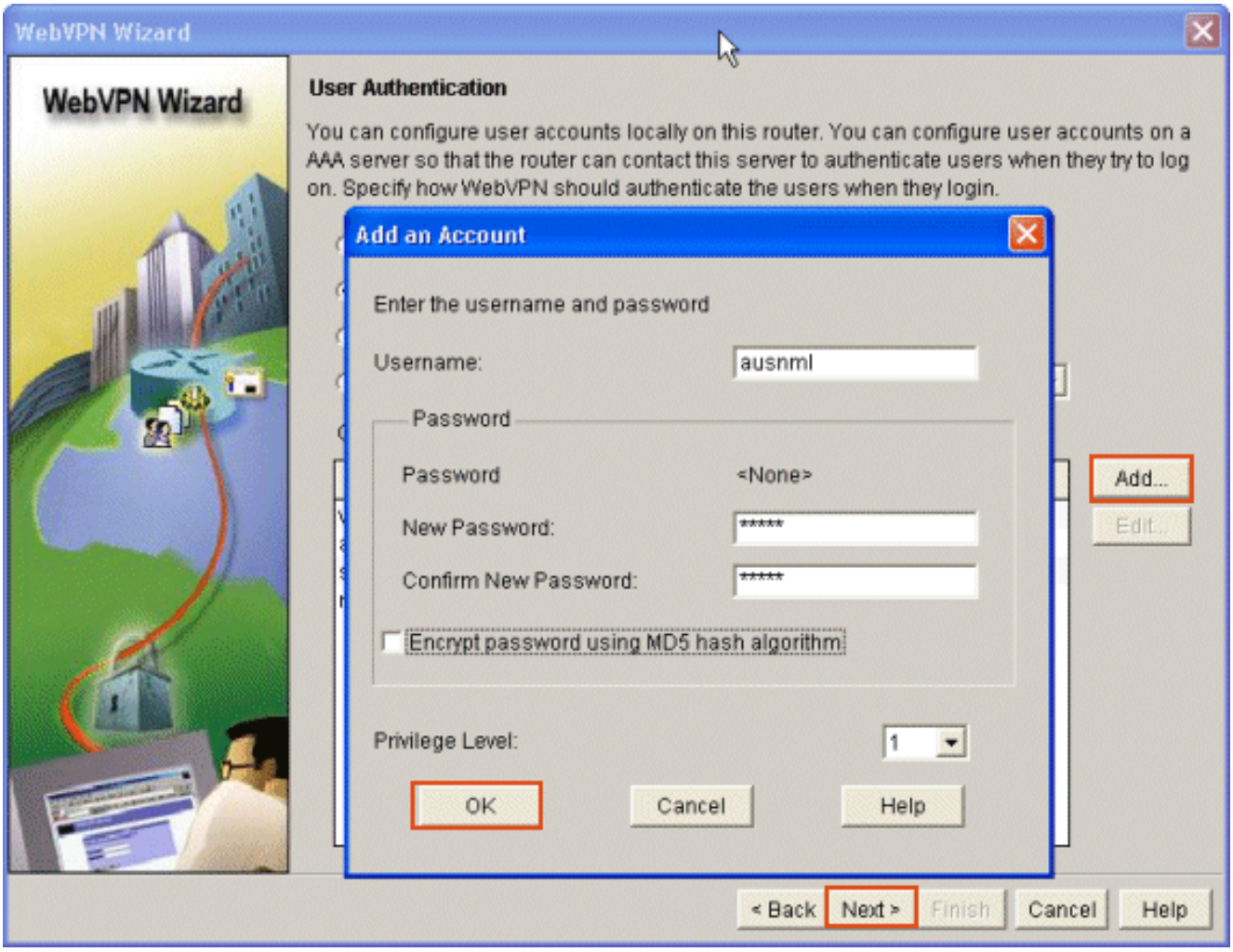
2. De Wizard WebVPN start. Klik op **Volgende**.



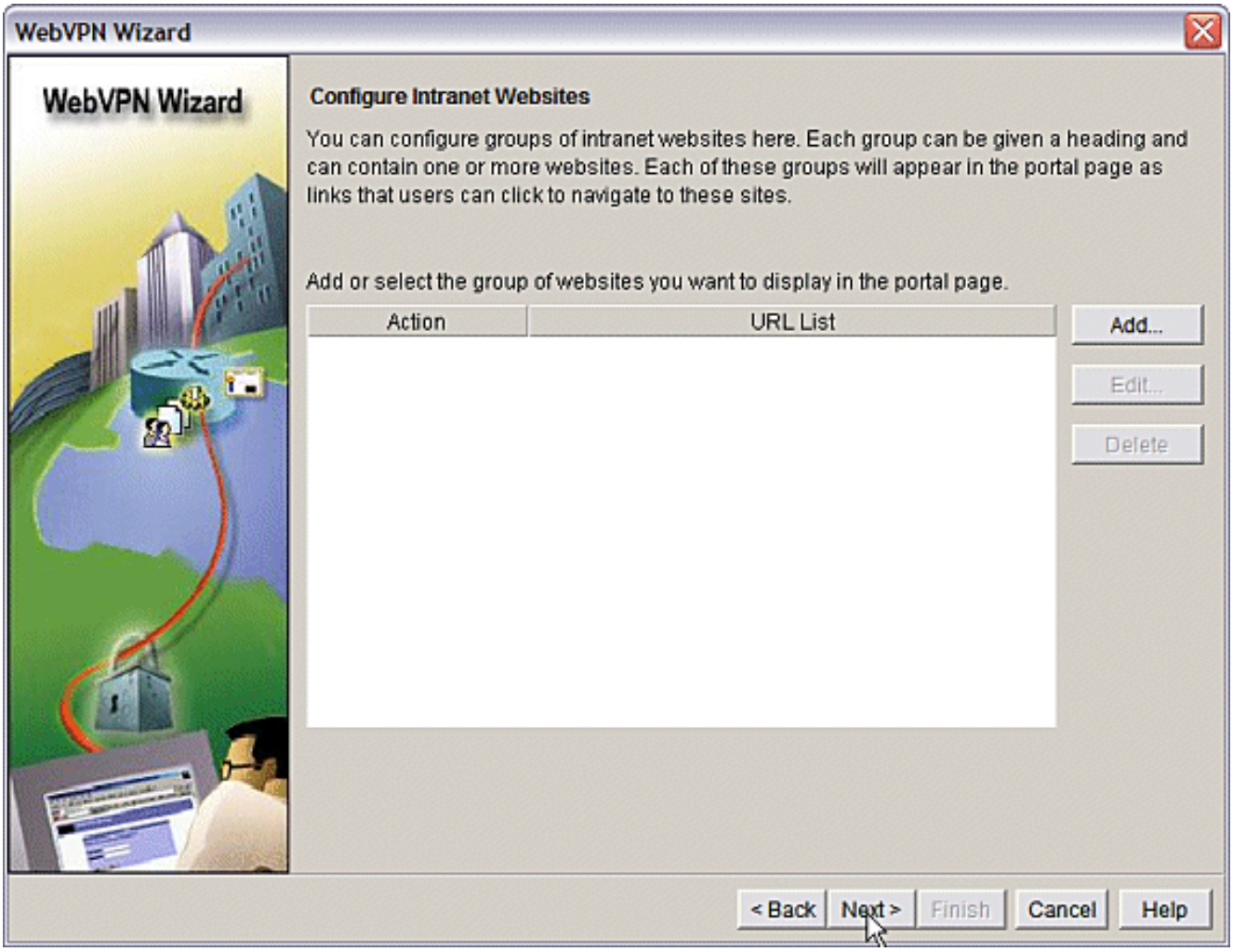
Voer het IP-adres in en een unieke naam voor deze WebVPN-gateway. Klik op **Volgende**.



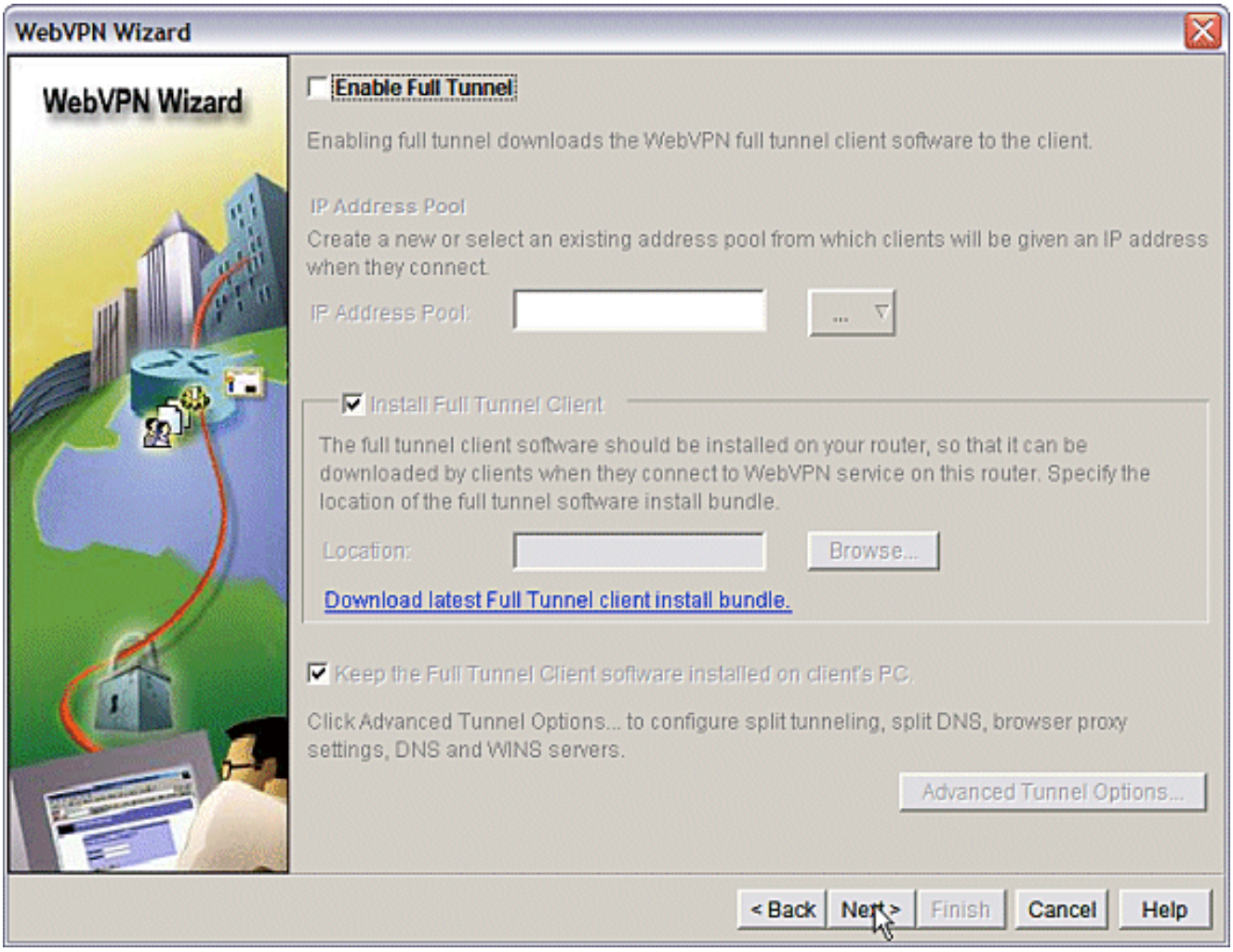
3. Het gebruikersverificatiescherm biedt de mogelijkheid om te voorzien in de verificatie van gebruikers. Deze configuratie gebruikt een account die lokaal op de router is gemaakt. U kunt ook een AAA-server (verificatie, autorisatie en accounting) gebruiken.Als u een gebruiker wilt toevoegen, klikt u op **Toevoegen**.Voer de gebruikersinformatie in op het scherm Toevoegen en klik op **OK**.Klik op **Volgende** op het scherm Gebruikersverificatie.



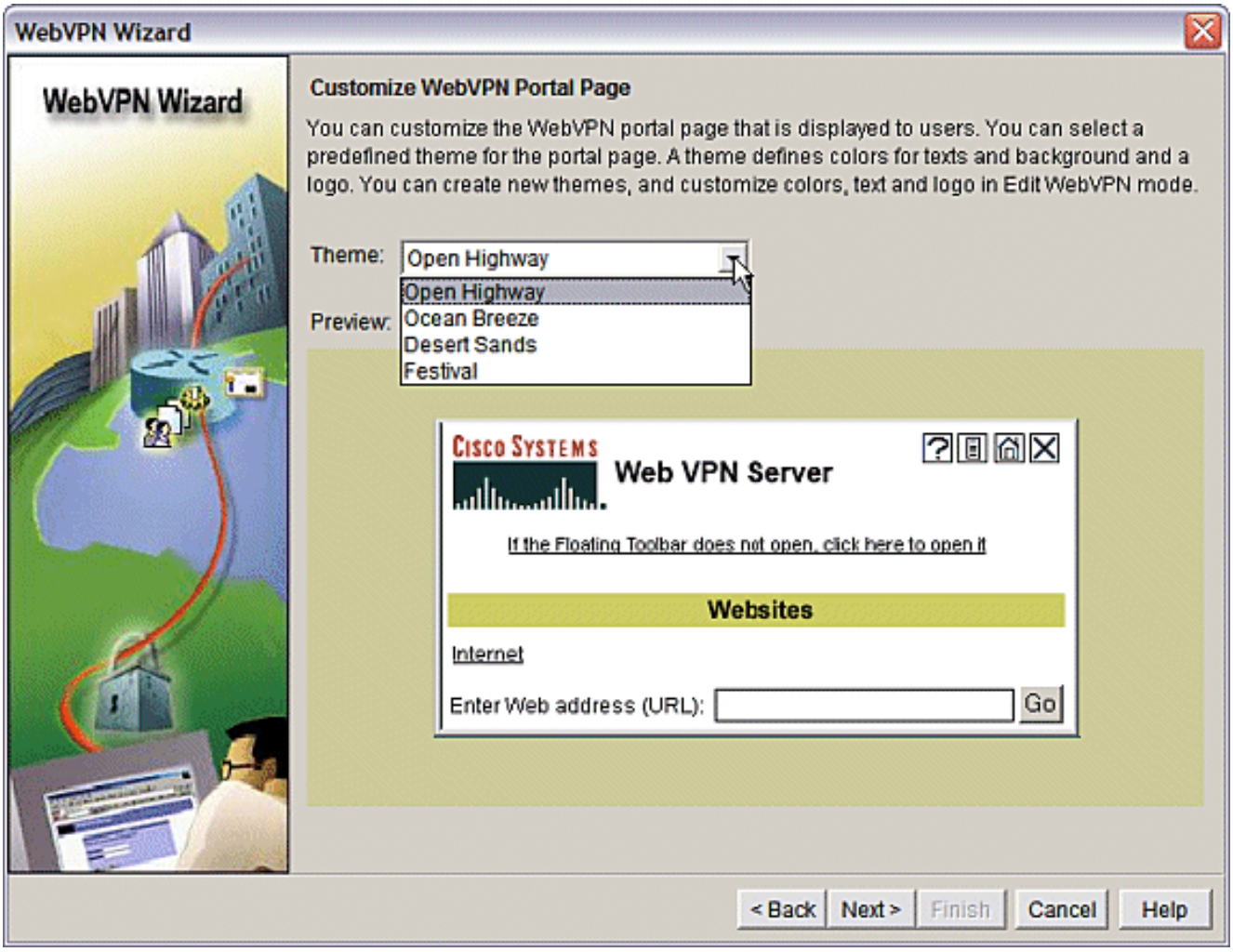
Het scherm van de Wizard WebVPN staat voor de configuratie van Intranet websites toe, maar deze stap wordt weggelaten omdat Port-Forwarding voor deze toepassingstoegang wordt gebruikt. Als u toegang tot websites wilt toestaan, gebruikt u de Clientless of Full Client SSL VPN-configuraties, die niet binnen het toepassingsgebied van dit document vallen.



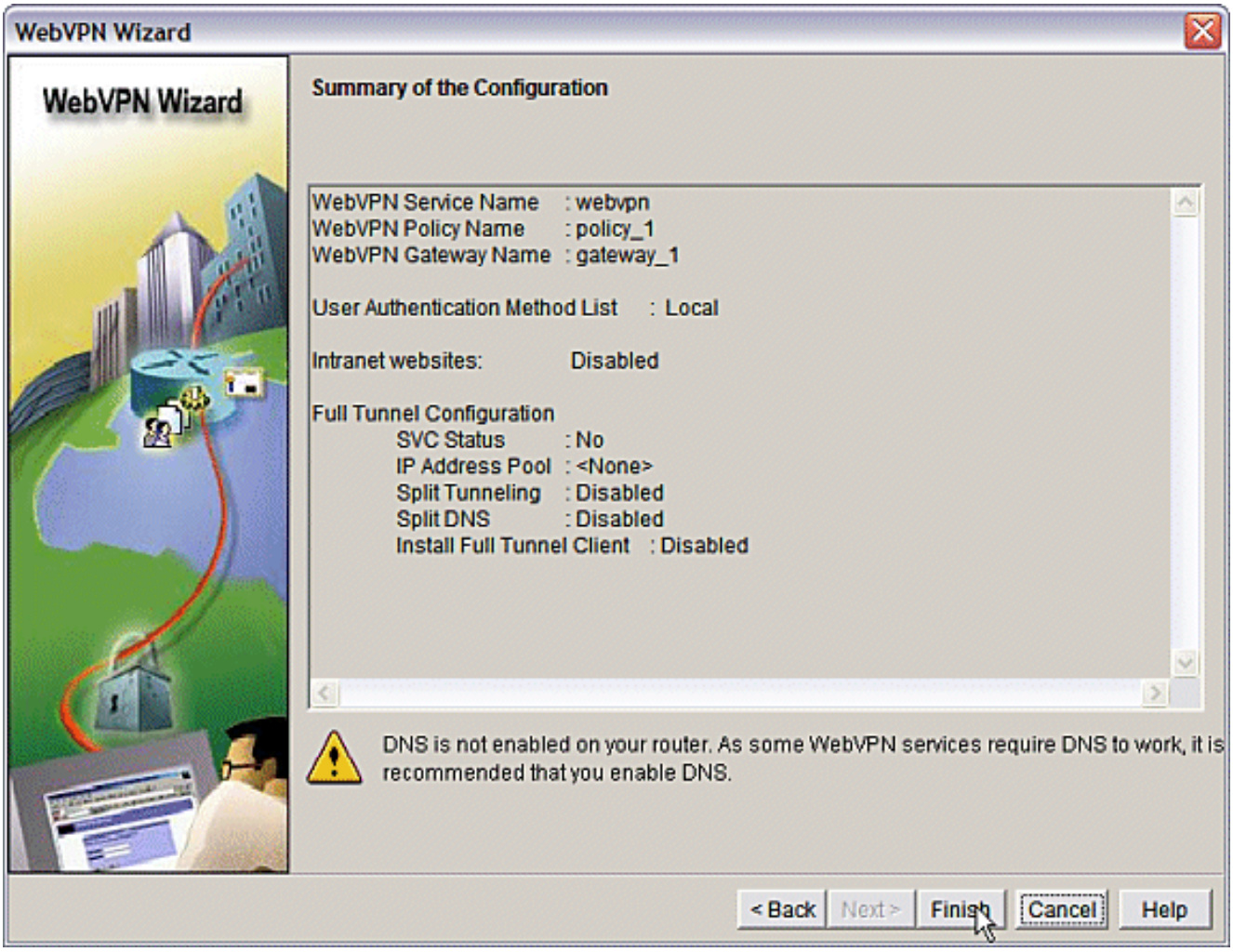
Klik op **Volgende**. De wizard geeft een scherm weer dat de volledige tunnelclient kan configureren. Dit is niet van toepassing op het Thin-Client SSL VPN (Port Forwarding).Schakel **de volledige tunnelverbinding uit**. Klik op **Volgende**.



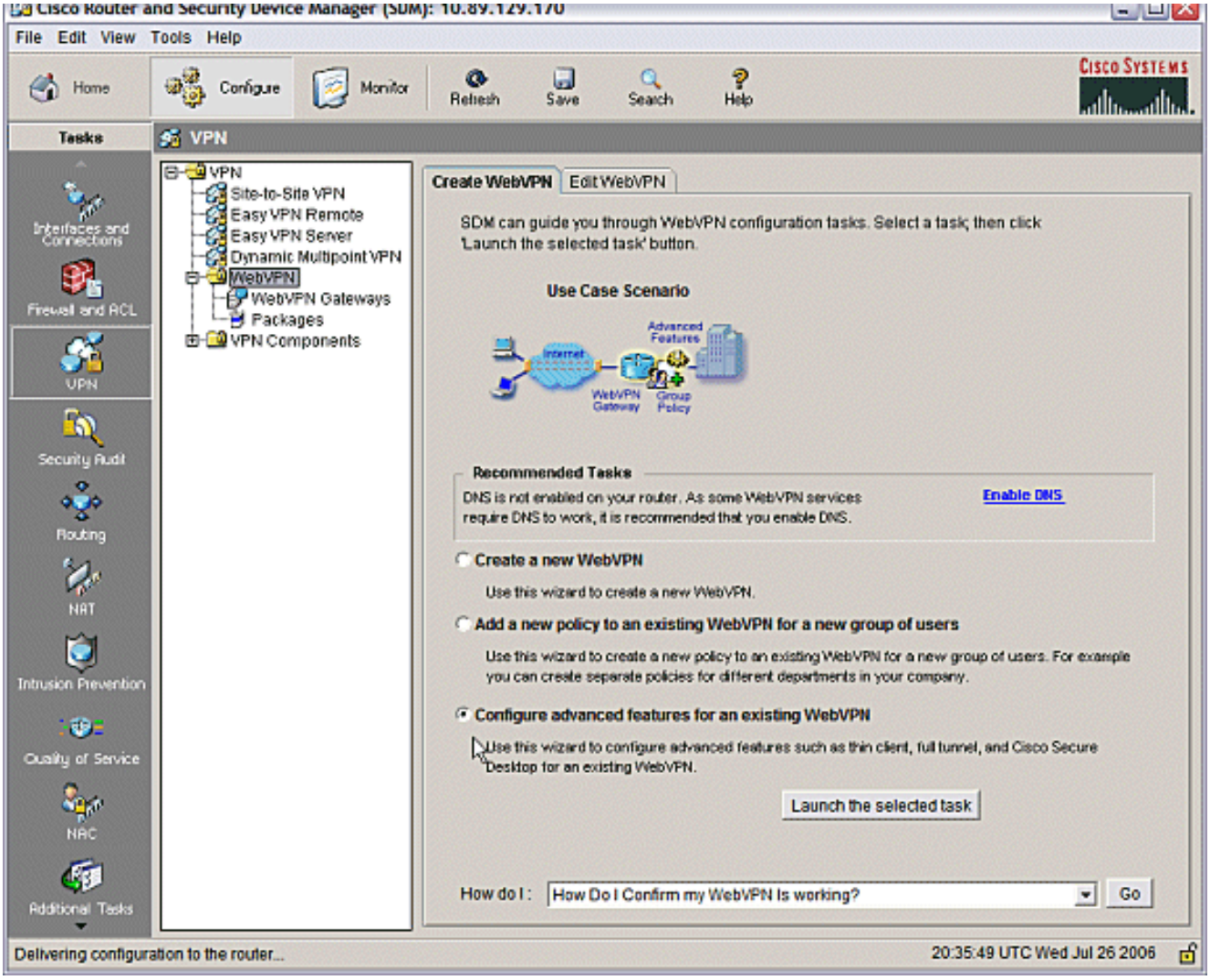
4. Pas de weergave van de webpoortpagina aan of accepteer de standaardweergave.Klik op **Volgende**.



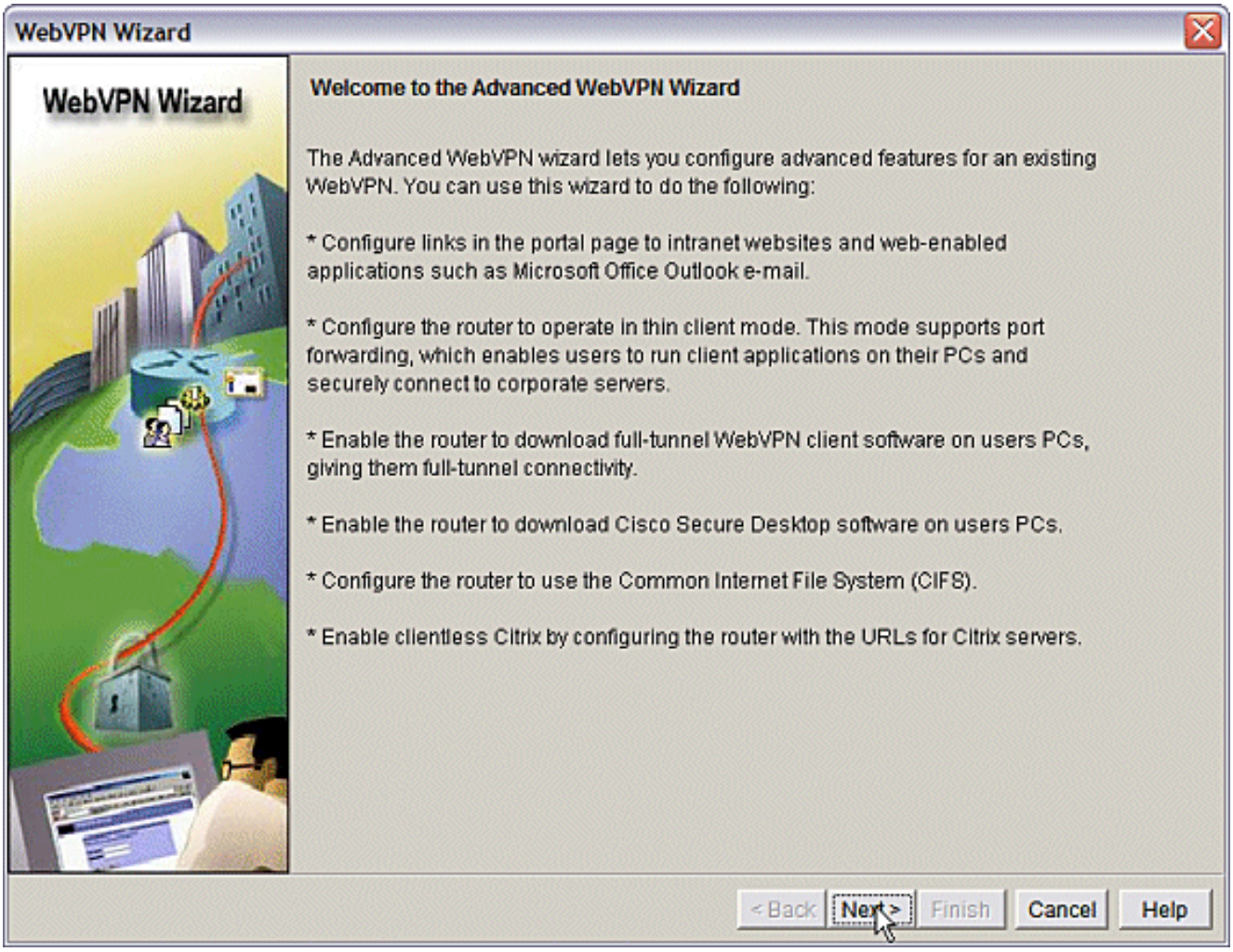
Bekijk de samenvatting van de configuratie en klik op **Voltooien > Opslaan**.



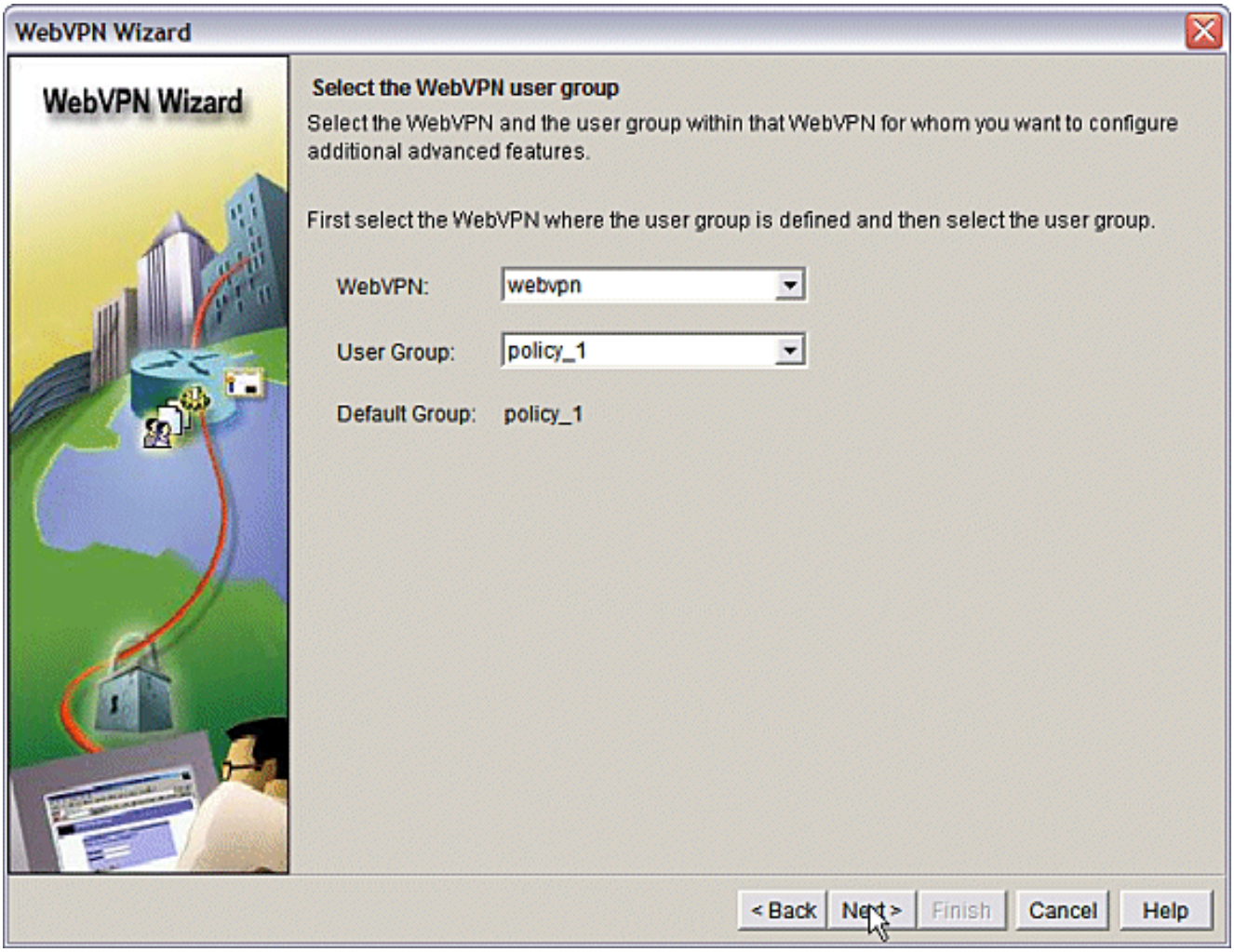
5. U hebt een WebVPN Gateway en een WebVPN Context met een gekoppeld groepsbeleid gemaakt. Configureer de thin-Client-poorten die beschikbaar worden gesteld wanneer clients verbinding maken met WebVPN.Kies **instellen**.Kies **VPN > WebVPN**.Kies **WebVPN maken**.Kies de radioknop **Geavanceerde functies voor een bestaand WebVPN configureren** en klik op **Start de geselecteerde taak**.



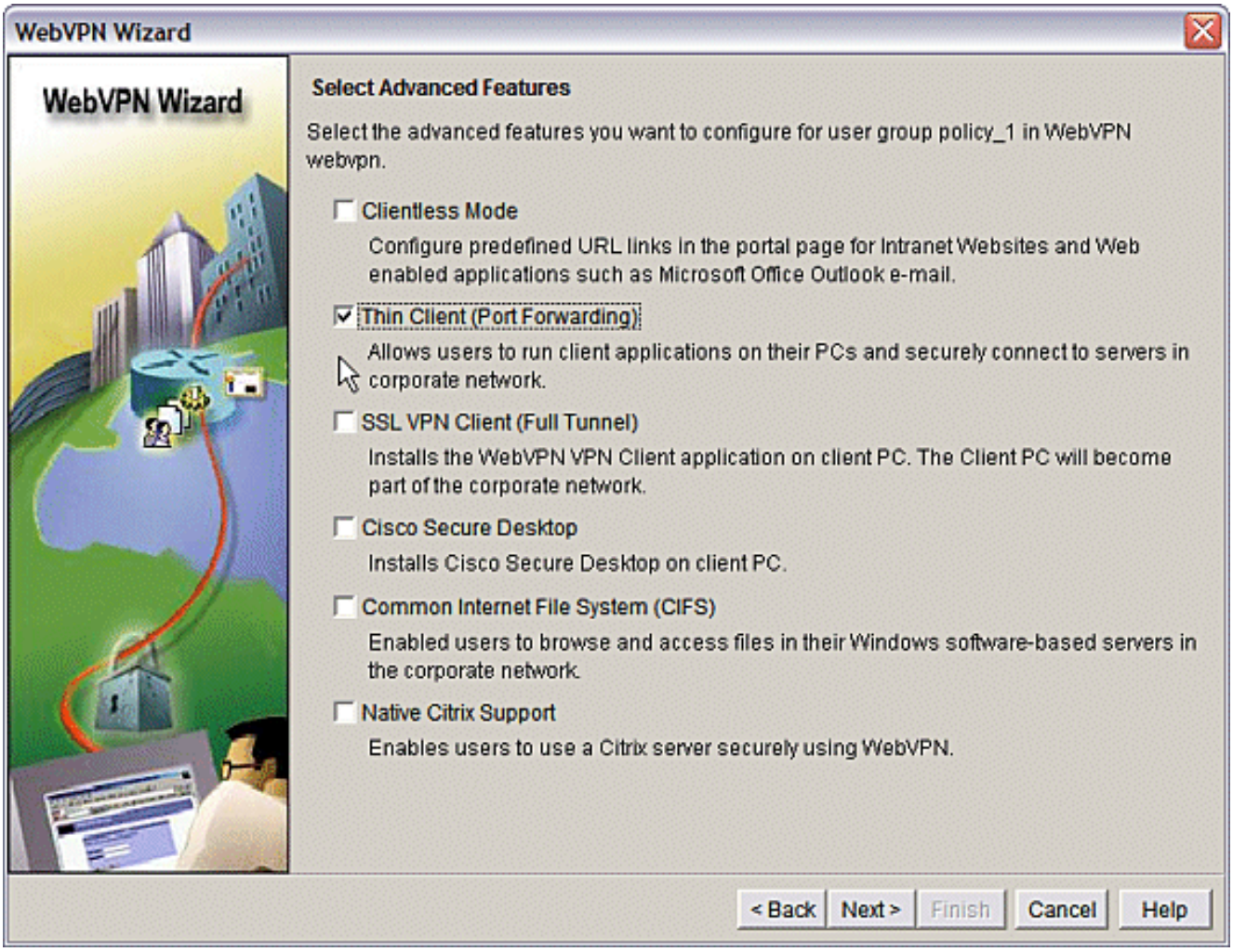
Het welkomstscherm biedt hoogtepunten van de mogelijkheden van de Wizard. Klik op **Volgende**.



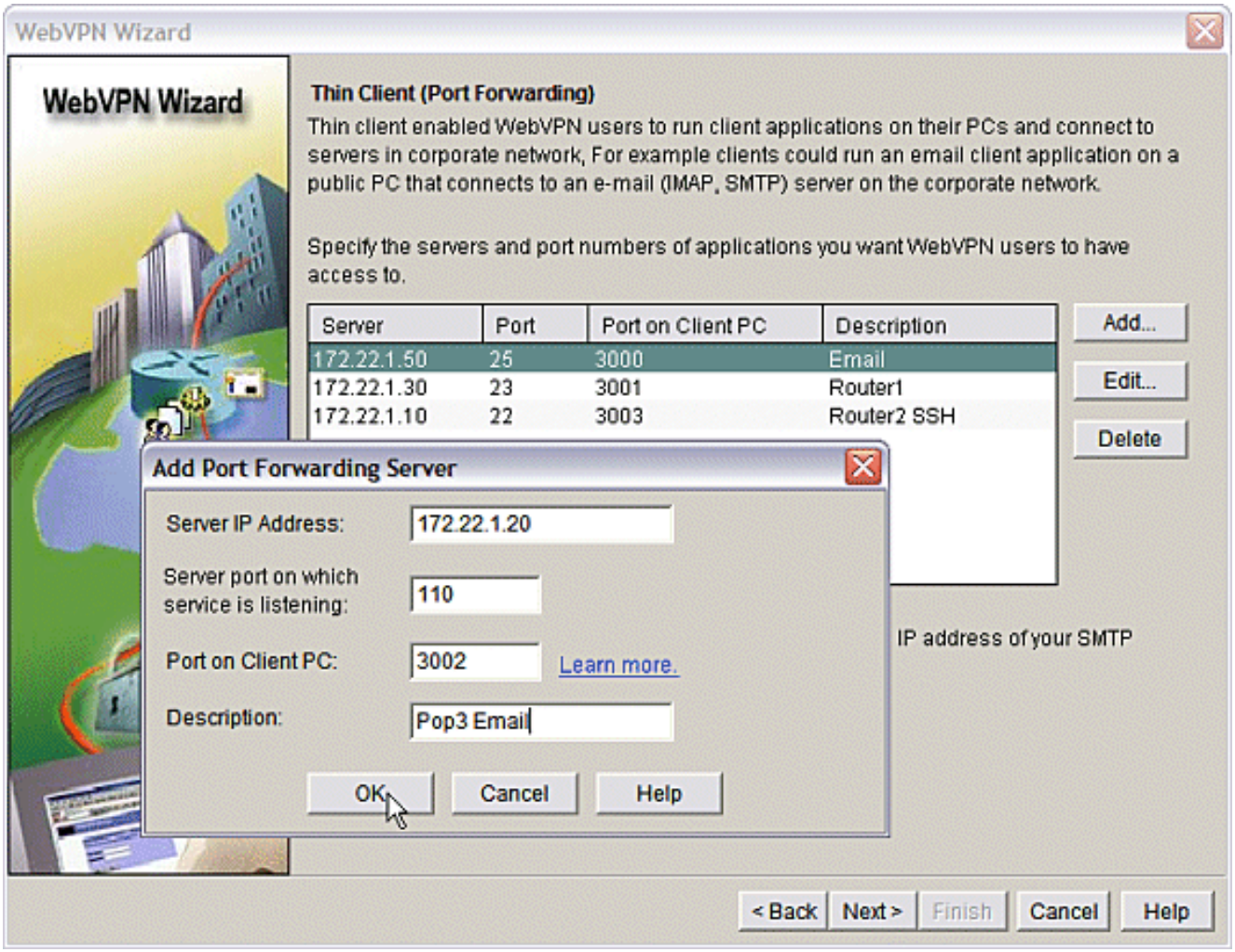
Kies de Webex-context en de gebruikersgroep in de vervolgkeuzemenu's. Klik op **Volgende**.



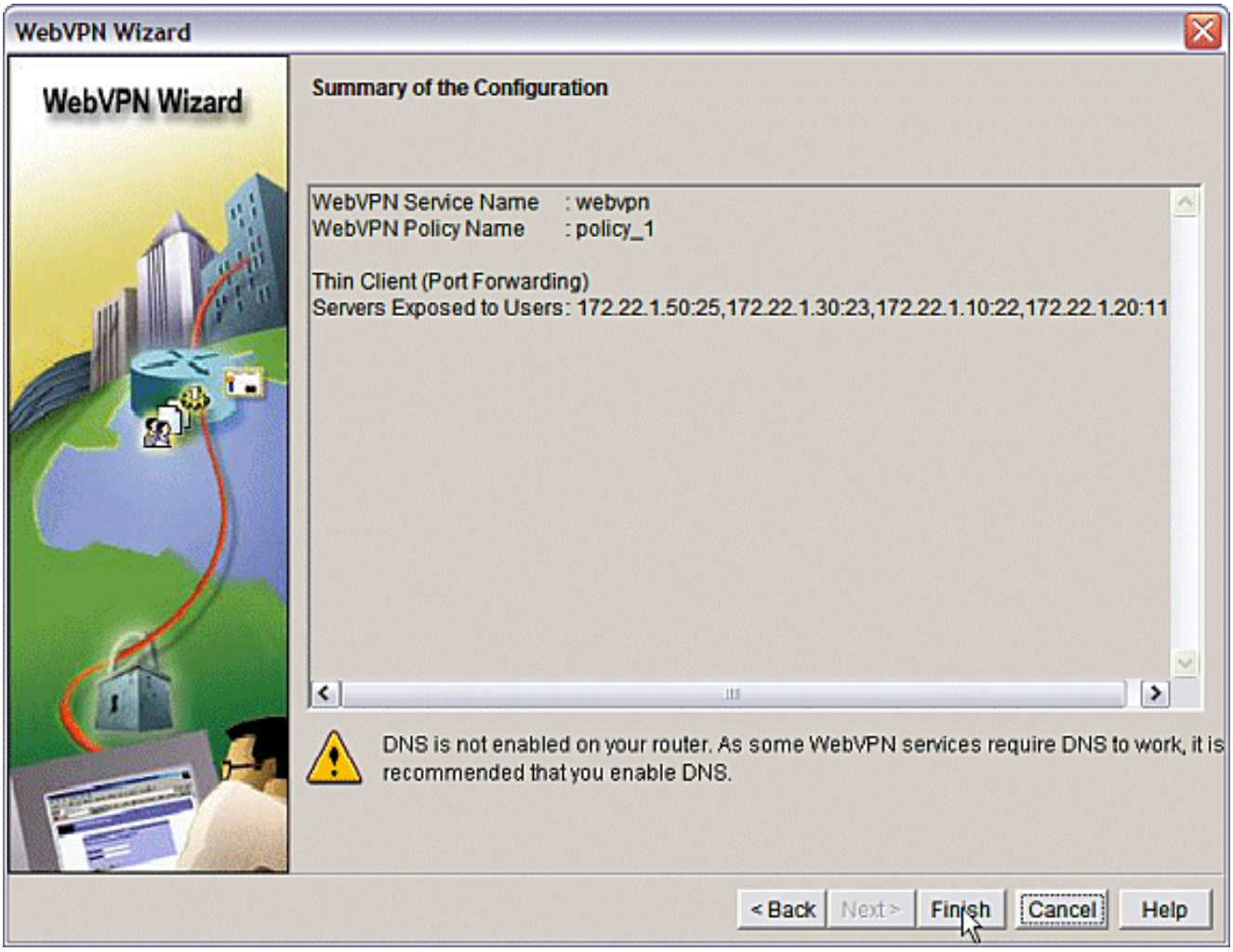
Kies **Thin Client (Port Forwarding)** en klik op **Volgende**.



Voer de middelen in die u via Port Forwarding beschikbaar wilt maken. De servicepoort moet een statische poort zijn, maar u kunt de standaardpoort op de client-pc accepteren die door de Wizard is toegewezen. Klik op
Volgende.



Bekijk de samenvatting van de configuratie en klik op **Voltooien > OK > Opslaan**.



Configuratie

Resultaten van de configuratie van het agm.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
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
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
```

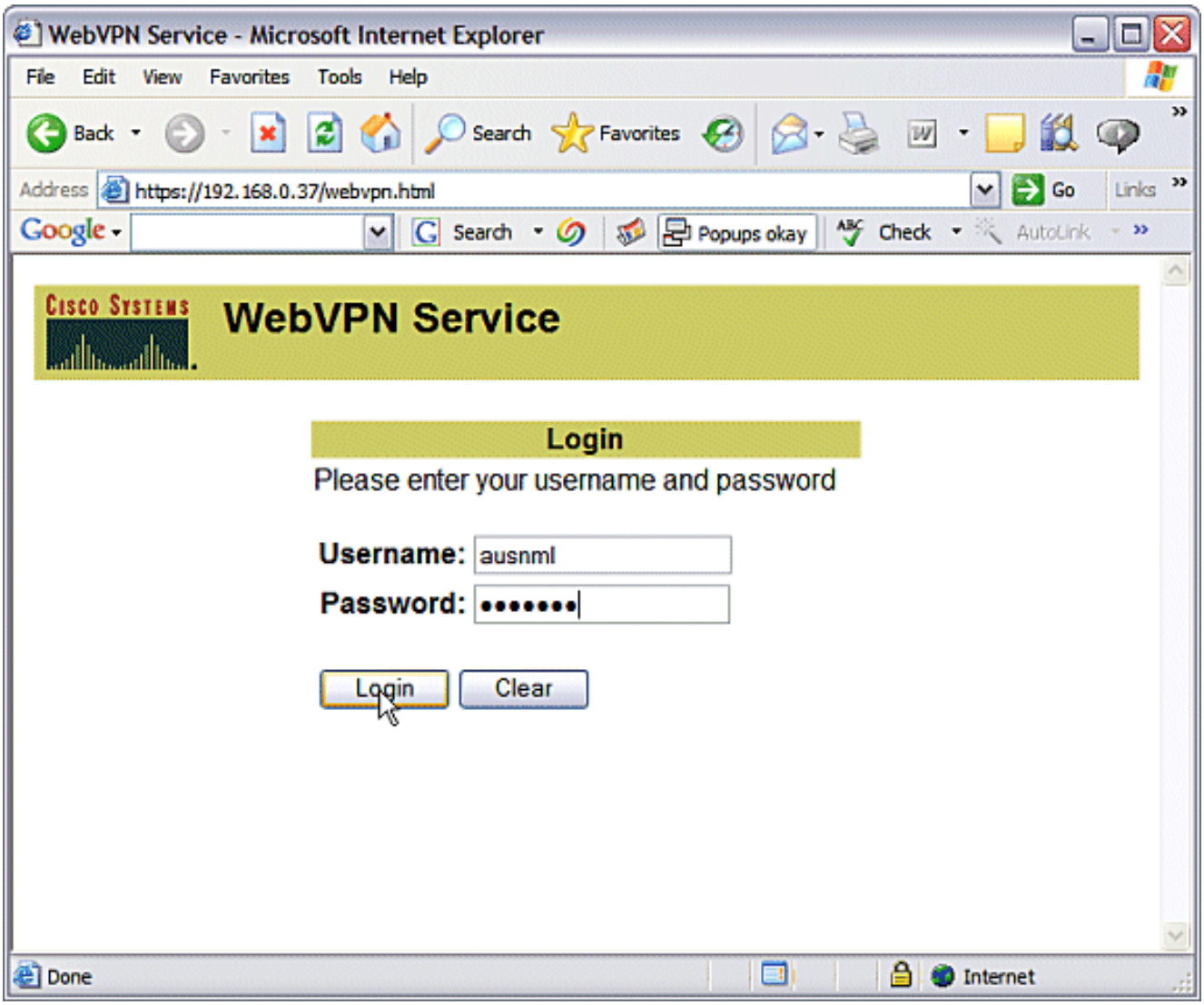
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

Verifiëren

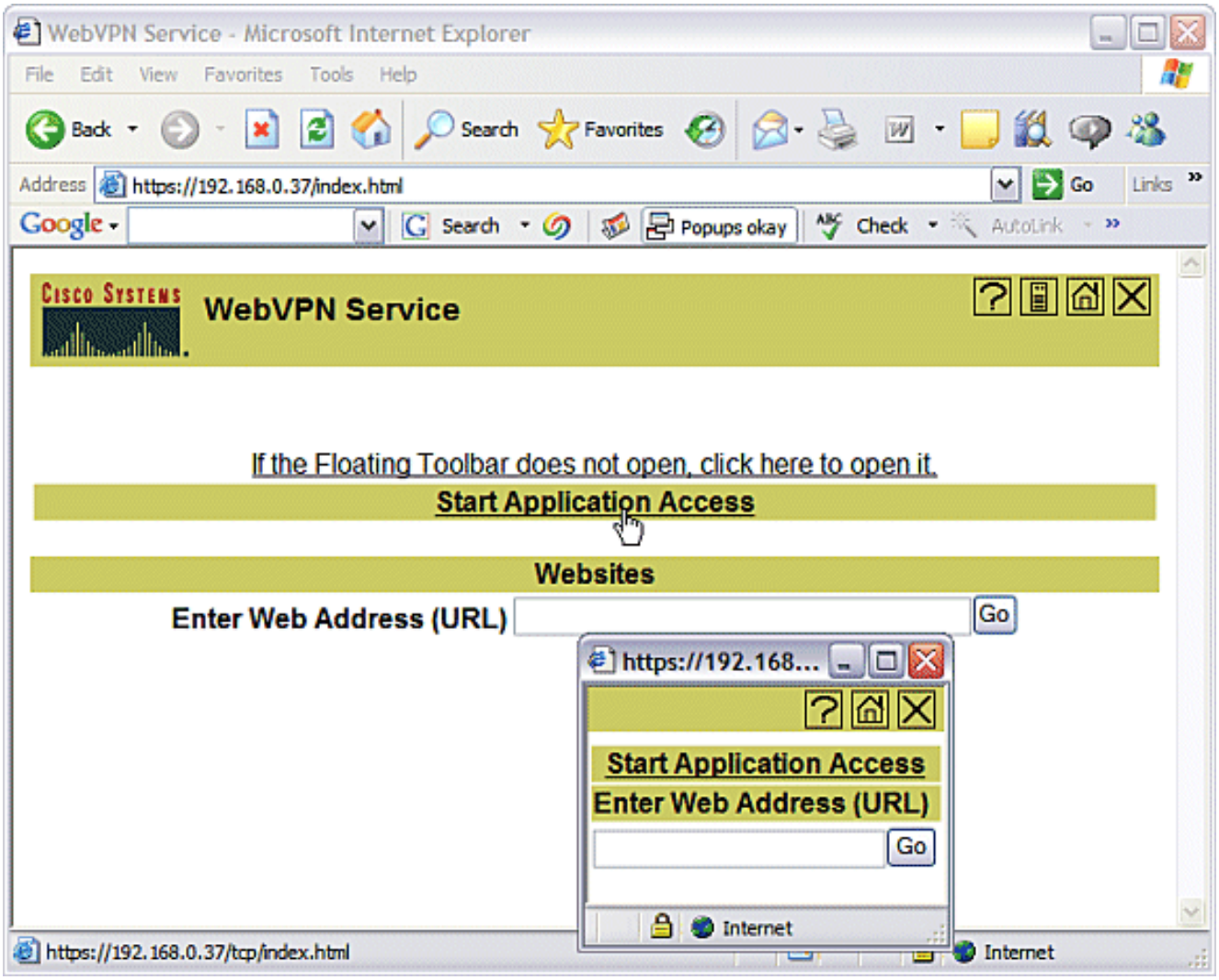
Controleer uw configuratie

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

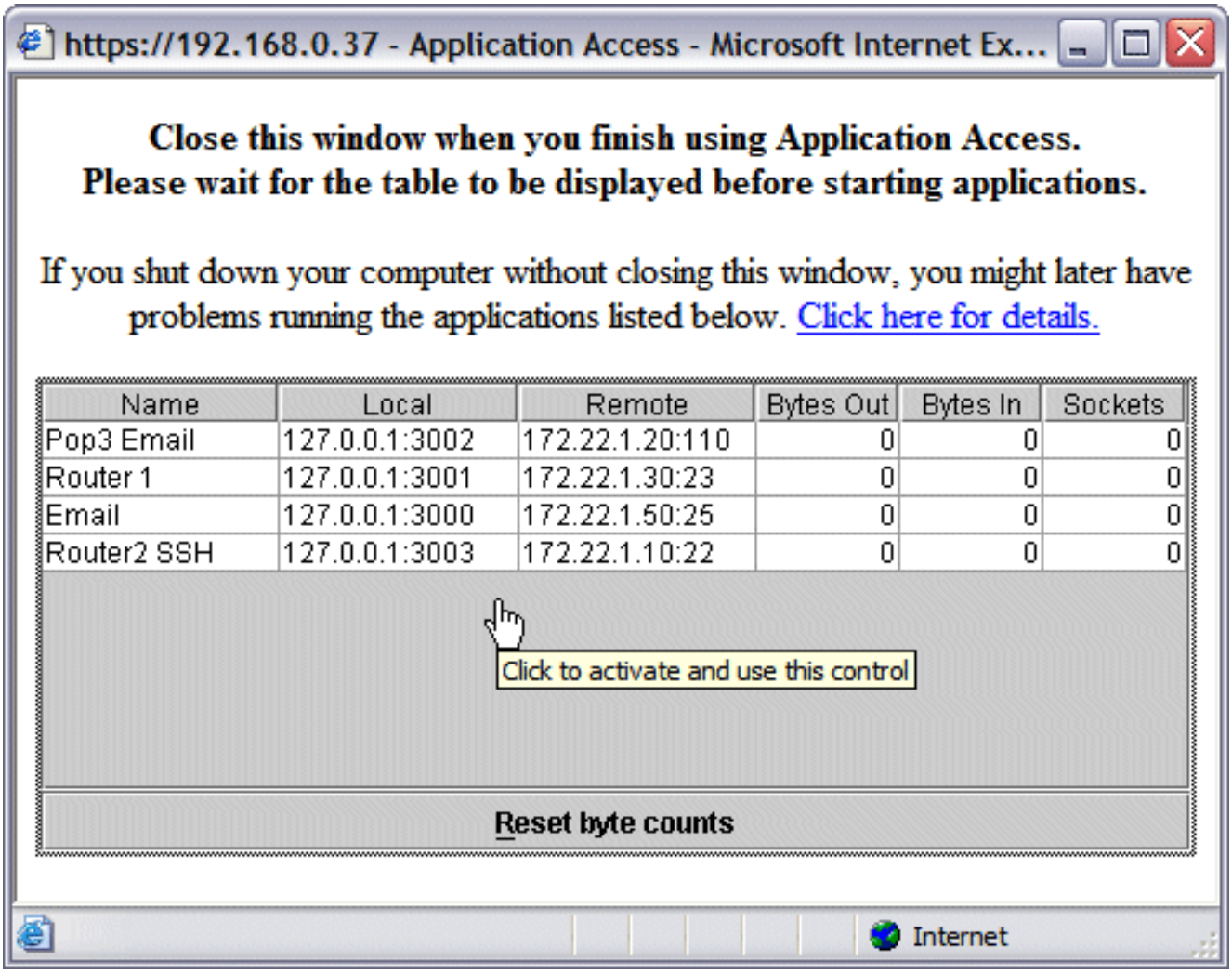
1. Gebruik een clientcomputer om toegang te krijgen tot de WebVPN-gateway op **https://gateway_ip_address.** Vergeet niet de WebexVPN-domeinnaam in te sluiten als u een unieke WebVPN-context maakt. Als u bijvoorbeeld een domein hebt gemaakt dat verkopen wordt genoemd, voer dan **https://gateway_ip_address/sales in**.



2. Vastleggen en aanvaarden het certificaat dat door de gateway van WebVPN wordt aangeboden. Klik op **Start Application Access**.



3. Het toegangsscherm van de toepassing toont. U kunt toegang krijgen tot een toepassing met het lokale poortnummer en uw lokale IP-adres. Bijvoorbeeld, aan Telnet aan router 1, ga **telnet 127.0.0.1 3001 in**. De kleine Java-applicatie stuurt deze informatie naar de WebVPN-gateway, die vervolgens de twee uiteinden van de sessie op een veilige manier met elkaar verbindt. Succesvolle verbindingen kunnen de **Bytes Out** en **Bytes in** kolommen doen toenemen.



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. Zie WebVPN-configuratie controleren van het gebruik van de opdrachten in detail controleren.

Het Uitvoer Tolk (uitsluitend 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.

Clientcomputers moeten worden geladen met versie 1.4 van SUN Java of hoger. Een kopie van deze software verkrijgen van Java-softwaredownloads

Opdrachten gebruikt voor probleemoplossing

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **toon web?** - Er zijn veel **show** opdrachten verbonden met WebVPN. Deze kunnen bij de CLI worden uitgevoerd om statistieken en andere informatie weer te geven. Zie Configuratie

WebVPN controleren om het gebruik van opdrachten in detail te zien **verschijnen** in de VPN-configuratie.

- **debug web?** Het gebruik van **debug** opdrachten kan een negatieve invloed hebben op de router. Om het gebruik van **debug**-opdrachten in meer detail te zien, raadpleegt u Opdrachten WebVPN gebruiken

Gerelateerde informatie

- Cisco IOS VPN-SLVPN
- SSL VPN - WebVPN
- Cisco IOS WebVPN Q&A
- Technische ondersteuning en documentatie – Cisco Systems