# SSL VPN Client (SVC) auf IOS mit SDM-Konfigurationsbeispiel

## Inhalt



## Einführung

Der SSL VPN Client (SVC) stellt einen vollständigen Tunnel für die sichere Kommunikation mit dem internen Unternehmensnetzwerk bereit. Sie können den Zugriff auf Benutzerbasis konfigurieren oder verschiedene WebVPN-Kontexte erstellen, in die Sie einen oder mehrere Benutzer einbinden.

Die SSL VPN- oder WebVPN-Technologie wird auf den folgenden IOS-Routerplattformen unterstützt:

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

Sie können die SSL VPN-Technologie in folgenden Modi konfigurieren:

- **Clientless SSL VPN (WebVPN)** - Stellt einen Remote-Client bereit, der einen SSL-fähigen Webbrowser für den Zugriff auf HTTP- oder HTTPS-Webserver in einem lokalen Unternehmensnetzwerk (LAN) benötigt. Darüber hinaus bietet Clientless-SSL-VPN Zugriff für das Durchsuchen von Windows-Dateien über das Common Internet File System (CIFS)-Protokoll. Outlook Web Access (OWA) ist ein Beispiel für den HTTP-Zugriff.Weitere Informationen zum Clientless-SSL-VPN finden Sie unter Clientless SSL VPN (WebVPN) in Cisco IOS mit SDM-Konfigurationsbeispiel.
- **Thin-Client SSL VPN (Port Forwarding)** - Bietet einen Remote-Client, der ein kleines, Java-basiertes Applet herunterlädt und sicheren Zugriff für TCP-Anwendungen (Transmission Control Protocol) ermöglicht, die statische Portnummern verwenden. Beispiele für sicheren Zugriff sind Point of Presence (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) und Telnet. Da sich Dateien auf dem lokalen Computer ändern, müssen Benutzer über lokale Administratorberechtigungen verfügen, um diese Methode verwenden zu können. Diese SSL VPN-Methode funktioniert nicht mit Anwendungen, die dynamische Portzuweisungen verwenden, wie z. B. einige FTP-Anwendungen (File Transfer Protocol).Weitere Informationen zum Thin-Client SSL VPN (WebVPN) IOS-Konfigurationsbeispiel mit SDM finden Sie unter Thin-Client SSL VPN (WebVPN).**Hinweis:** User Datagram Protocol (UDP) wird nicht unterstützt.
- **SSL VPN Client (SVC Full Tunnel Mode)**: Lädt einen kleinen Client zur Remote-Workstation herunter und ermöglicht einen vollständigen sicheren Zugriff auf Ressourcen in einem internen Unternehmensnetzwerk. Sie können den SVC dauerhaft auf eine Remote-Workstation herunterladen oder den Client entfernen, wenn die sichere Sitzung beendet ist.

In diesem Dokument wird die Konfiguration eines Cisco IOS-Routers für die Verwendung durch einen SSL VPN-Client veranschaulicht.

# Voraussetzungen

## Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Microsoft Windows 2000 oder XP
- Webbrowser mit SUN JRE 1.4 oder höher oder einem ActiveX-gesteuerten Browser
- Lokale Administratorberechtigungen auf dem Client
- Einer der Router, der in der Einführung mit einem Advanced Security-Image (12.4(6)T oder höher) aufgeführt ist
- Cisco Security Device Manager (SDM) Version 2.3Wenn das Cisco SDM nicht bereits auf Ihrem Router geladen ist, können Sie eine kostenlose Kopie der Software vom Software Download beziehen (nur registrierte Kunden). Sie müssen über ein CCO-Konto mit einem Servicevertrag verfügen. Detaillierte Informationen zur Installation und Konfiguration von SDM finden Sie unter Cisco Router und Security Device Manager.
- Ein digitales Zertifikat auf dem RouterSie können ein persistentes, selbstsigniertes Zertifikat oder eine externe Zertifizierungsstelle (Certificate Authority, CA) verwenden, um diese Anforderung zu erfüllen. Weitere Informationen zu persistenten, selbstsignierten Zertifikaten finden Sie unter Persistent Self-Signed Certificates.

## Verwendete Komponenten

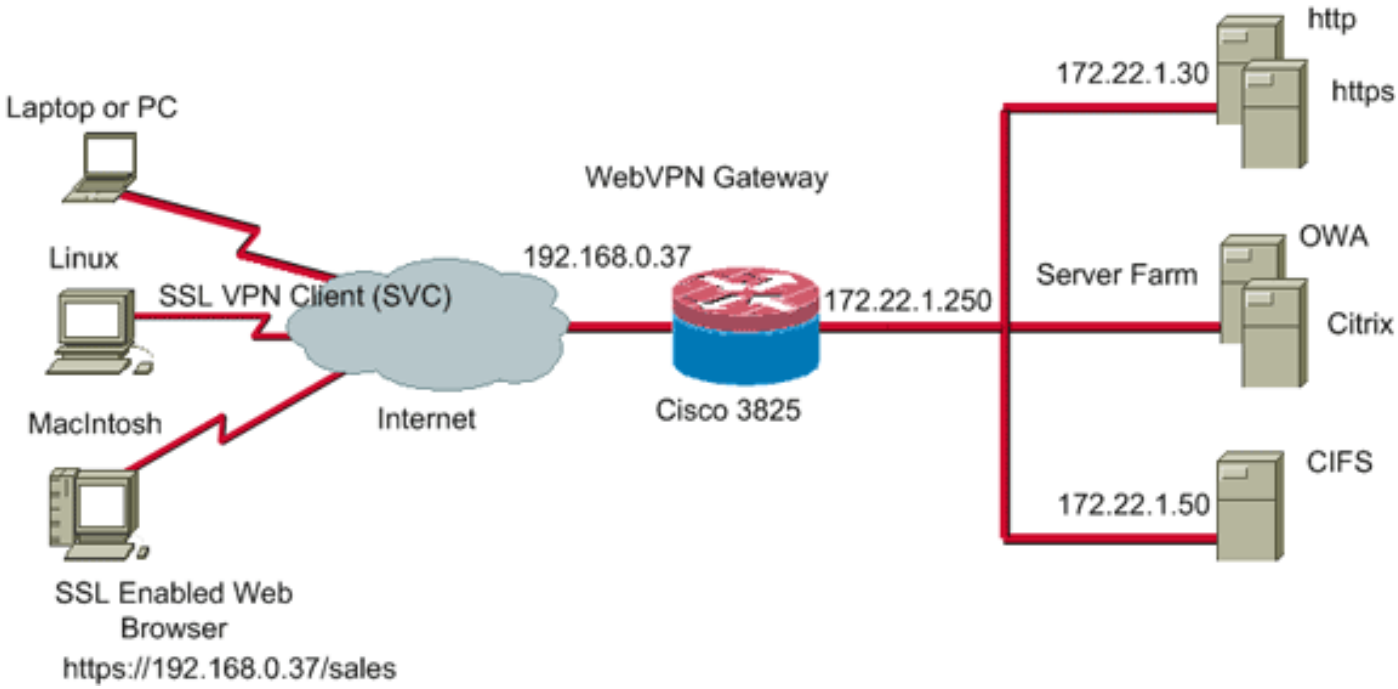
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS Router der Serie 3825 mit 12.4(9)T
- Security Device Manager (SDM) Version 2.3.1

**Hinweis:** Die Informationen in diesem Dokument wurden von Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:




## Vorkonfigurationsaufgaben

1. Konfigurieren Sie den Router für SDM. (Optional)Bei Routern mit der entsprechenden Security-Paket-Lizenz ist die SDM-Anwendung bereits im Flash-Speicher geladen. Unter Herunterladen und Installieren von Cisco Router und Security Device Manager (SDM) finden Sie Informationen zum Abrufen und Konfigurieren der Software.
2. Laden Sie eine Kopie des SVC auf Ihren Management-PC herunter.Sie können eine Kopie der SVC-Paketdatei vom Software Download beziehen: Cisco SSL VPN Client (nur registrierte Kunden) Sie benötigen ein gültiges CCO-Konto mit einem Servicevertrag.
3. Legen Sie das richtige Datum, die richtige Uhrzeit und die richtige Zeitzone fest, und konfigurieren Sie dann ein digitales Zertifikat auf dem Router.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

Conventions (Technische Tipps zu Konventionen von Cisco).

# Hintergrundinformationen

Der SVC wird zunächst auf den WebVPN-Gateway-Router geladen. Bei jeder Verbindung des Clients wird eine Kopie des SVC dynamisch auf den PC heruntergeladen. Um dieses Verhalten zu ändern, konfigurieren Sie den Router so, dass die Software dauerhaft auf dem Client-Computer verbleibt.

# Konfigurieren von SVC in IOS

In diesem Abschnitt finden Sie die erforderlichen Schritte zum Konfigurieren der in diesem Dokument beschriebenen Funktionen. In dieser Beispielkonfiguration wird der SDM-Assistent verwendet, um den Betrieb des SVC auf dem IOS-Router zu aktivieren.

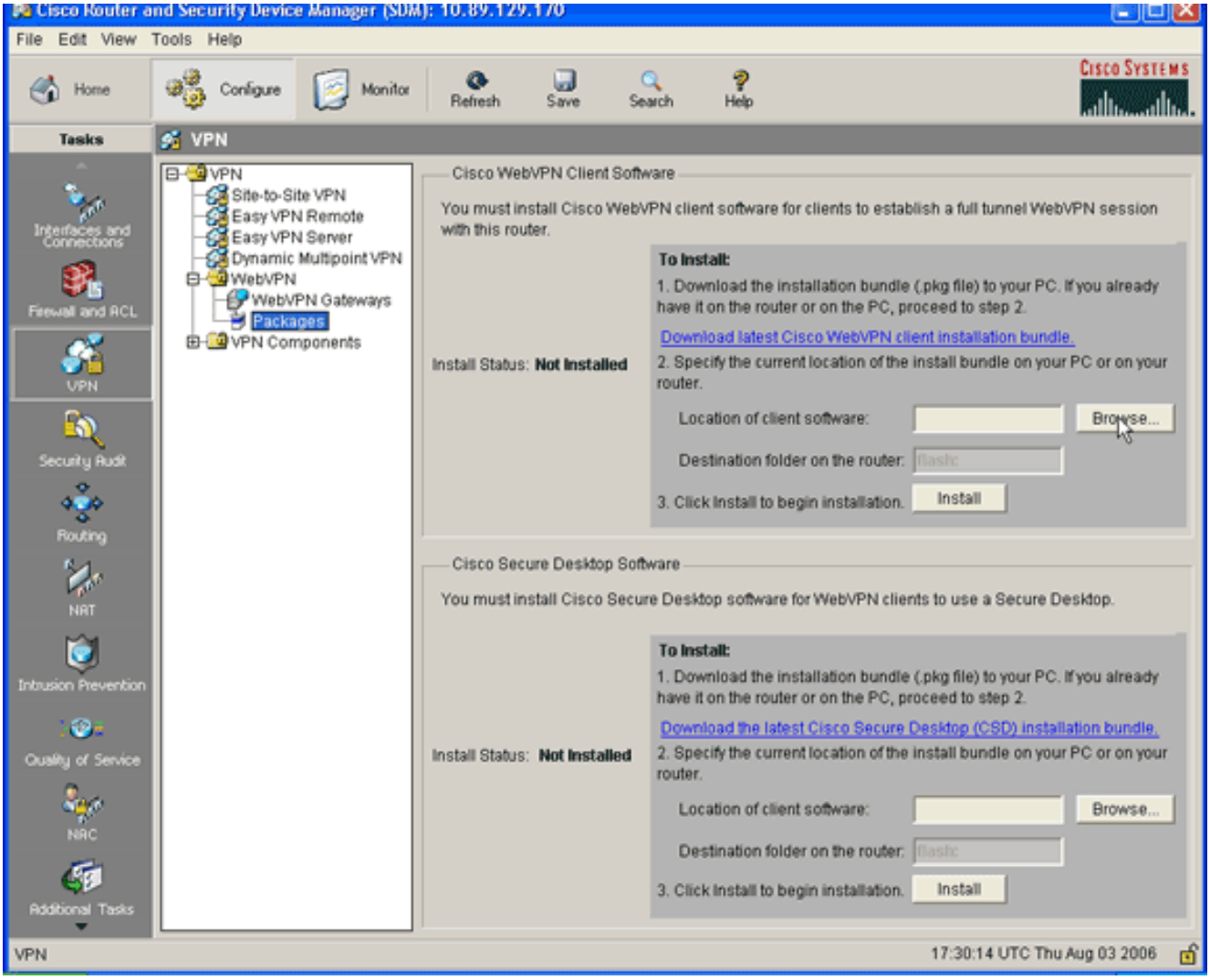
Gehen Sie wie folgt vor, um SVC auf dem IOS-Router zu konfigurieren:

1. Installation und Aktivierung der SVC-Software auf dem IOS-Router
2. Konfigurieren eines WebVPN-Kontexts und eines WebVPN-Gateways mithilfe des SDM-Assistenten
3. Konfigurieren der Benutzerdatenbank für SVC-Benutzer
4. Konfigurieren der Ressourcen zum Verfügbarmachen für Benutzer

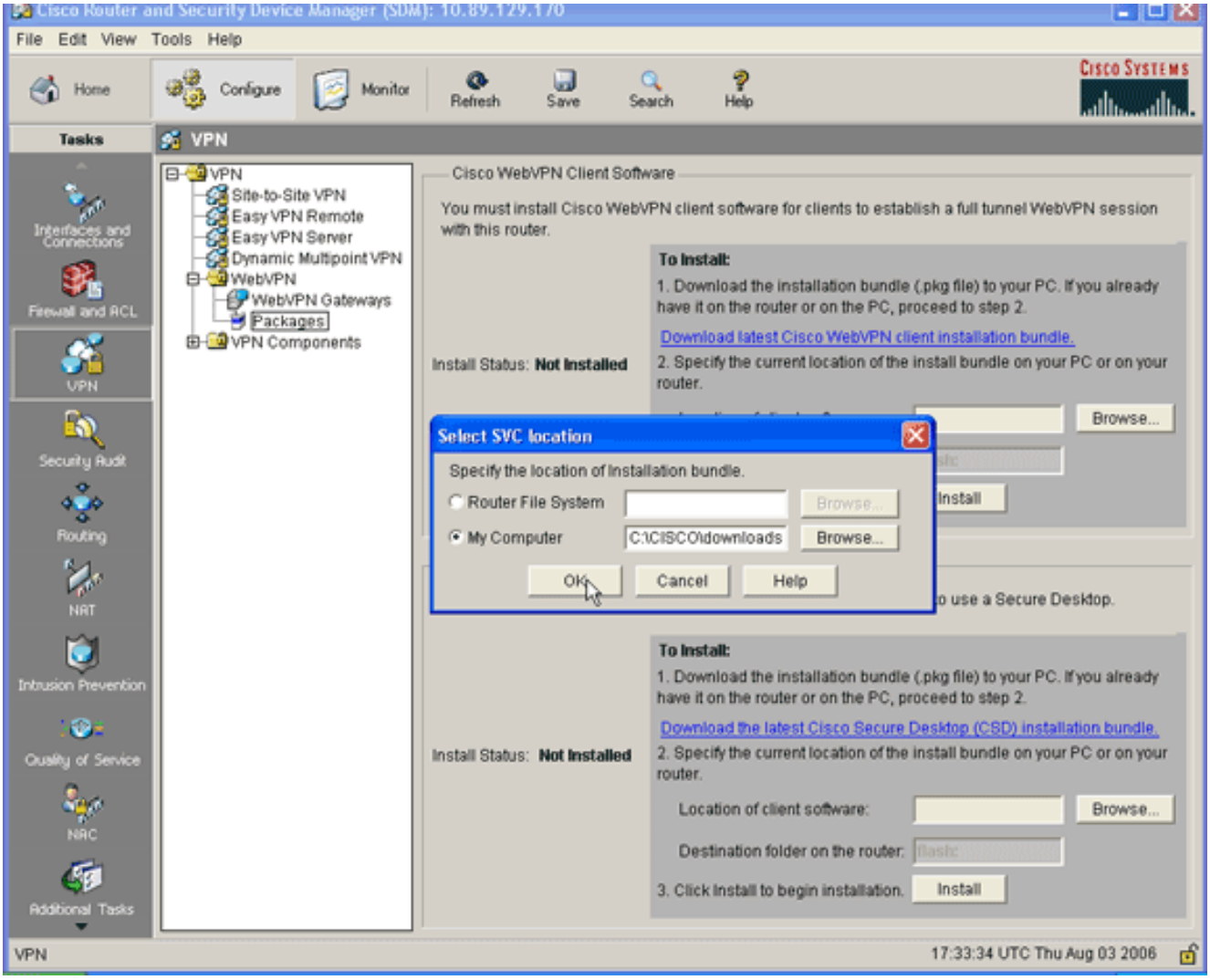
## Schritt 1: Installation und Aktivierung der SVC-Software auf dem IOS-Router

Gehen Sie wie folgt vor, um die SVC-Software auf dem IOS-Router zu installieren und zu aktivieren:

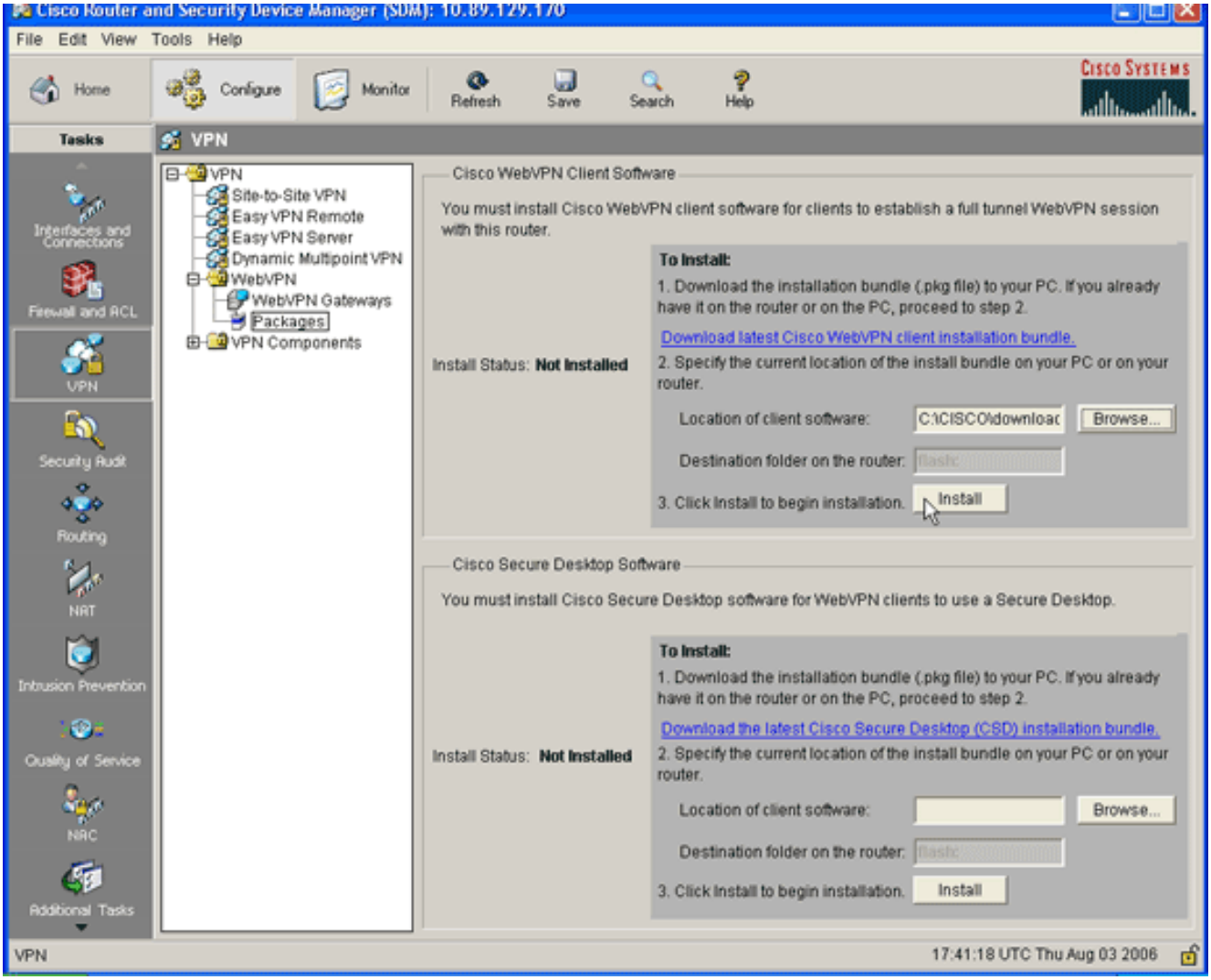
1. Öffnen Sie die SDM-Anwendung, klicken Sie auf **Konfigurieren**, und klicken Sie dann auf **VPN**.
2. Erweitern Sie **WebVPN**, und wählen Sie **Packages** aus.



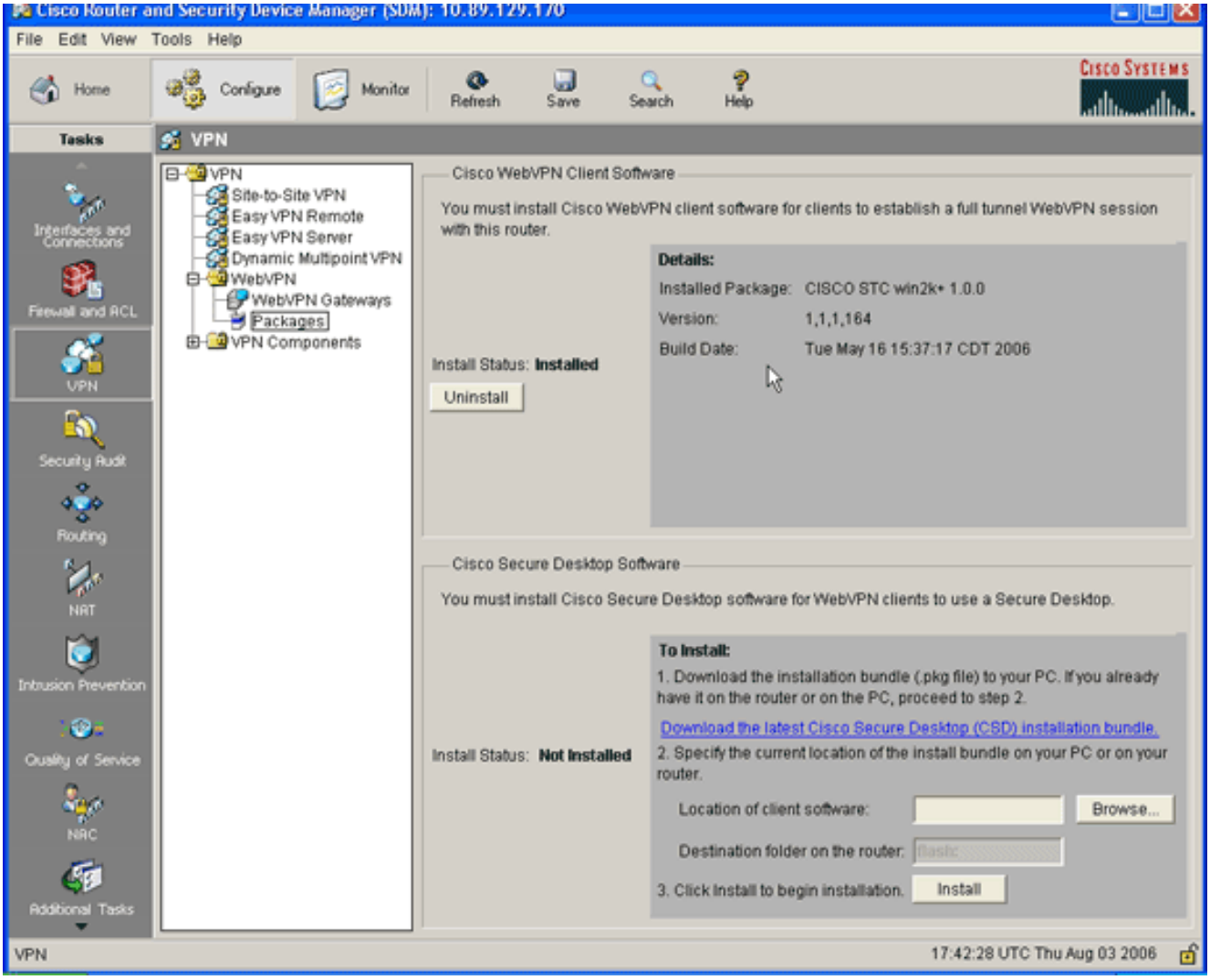

3. Klicken Sie im Bereich Cisco WebVPN Client Software auf die Schaltfläche **Browse** (Durchsuchen).Das Dialogfeld "SVC-Speicherort auswählen" wird angezeigt.




4. Klicken Sie auf das Optionsfeld **Arbeitsplatz** und dann auf **Durchsuchen**, um das SVC-Paket auf dem Management-PC zu suchen.
5. Klicken Sie auf **OK** und anschließend auf die Schaltfläche **Installieren**.



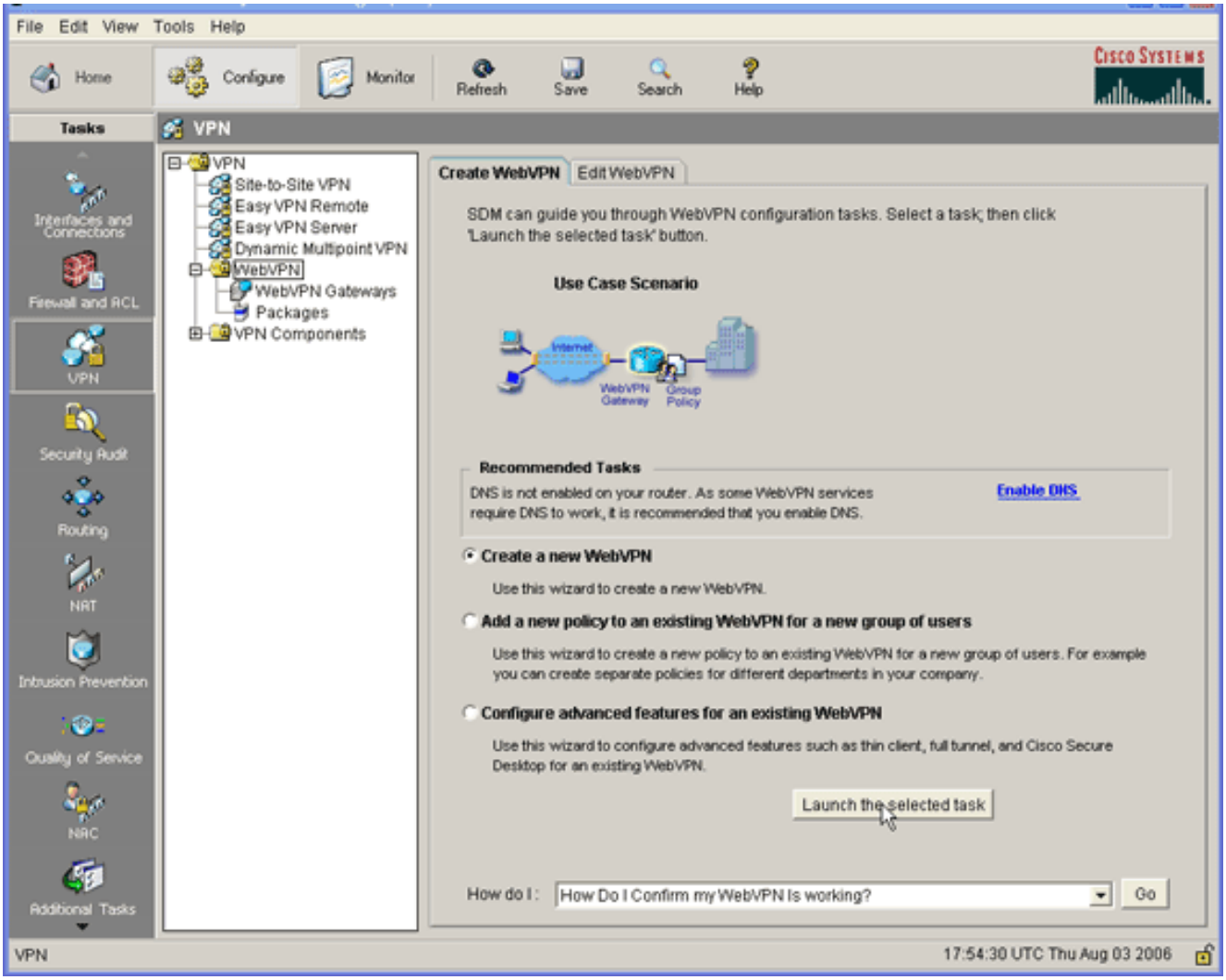

6. Klicken Sie auf **Ja** und dann auf **OK**.Eine erfolgreiche Installation des SVC-Pakets wird in diesem Bild
   angezeigt:



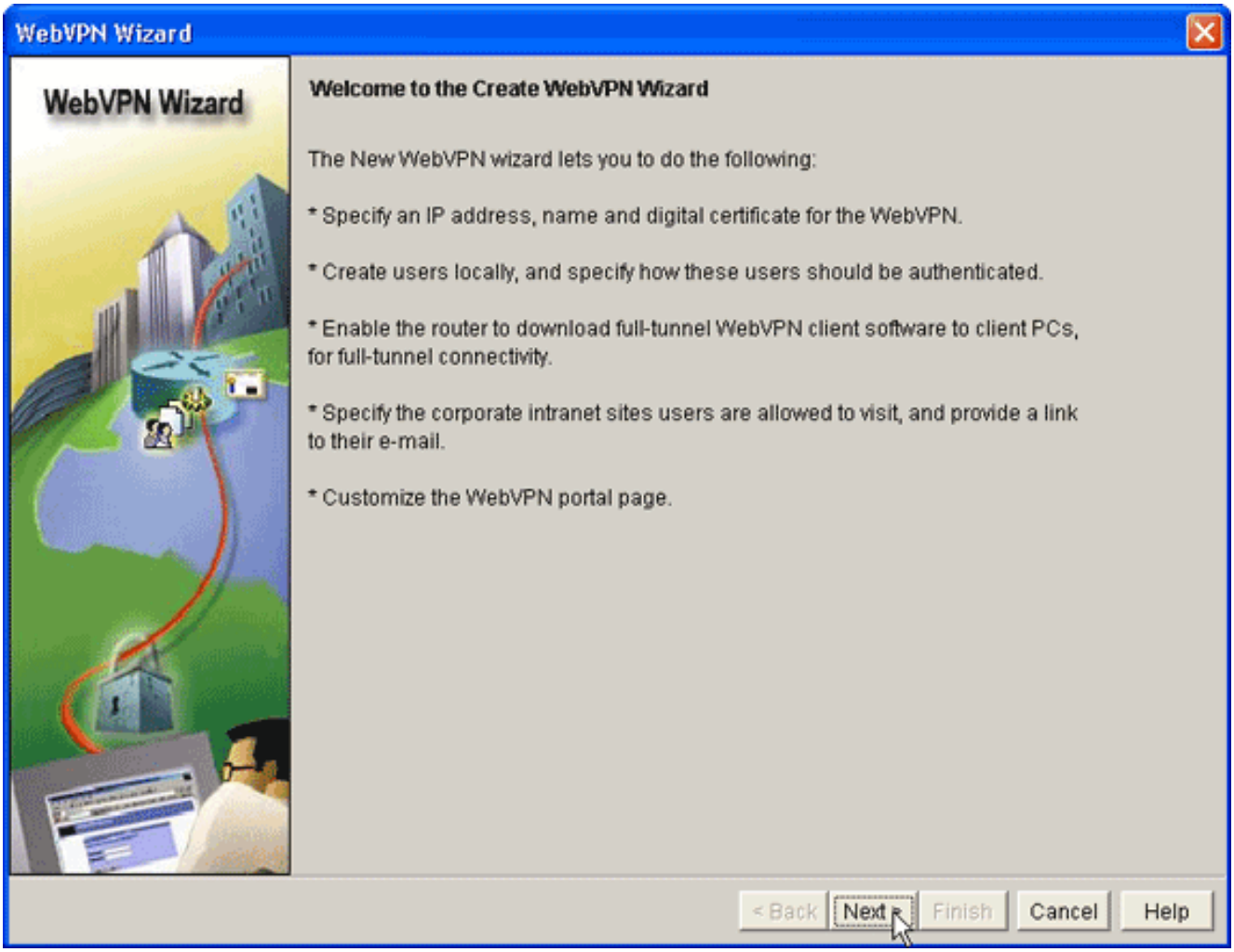

## Schritt 2: Konfigurieren eines WebVPN-Kontexts und eines WebVPN-Gateways mithilfe des SDM-Assistenten

Gehen Sie wie folgt vor, um einen WebVPN-Kontext und ein WebVPN-Gateway zu konfigurieren:

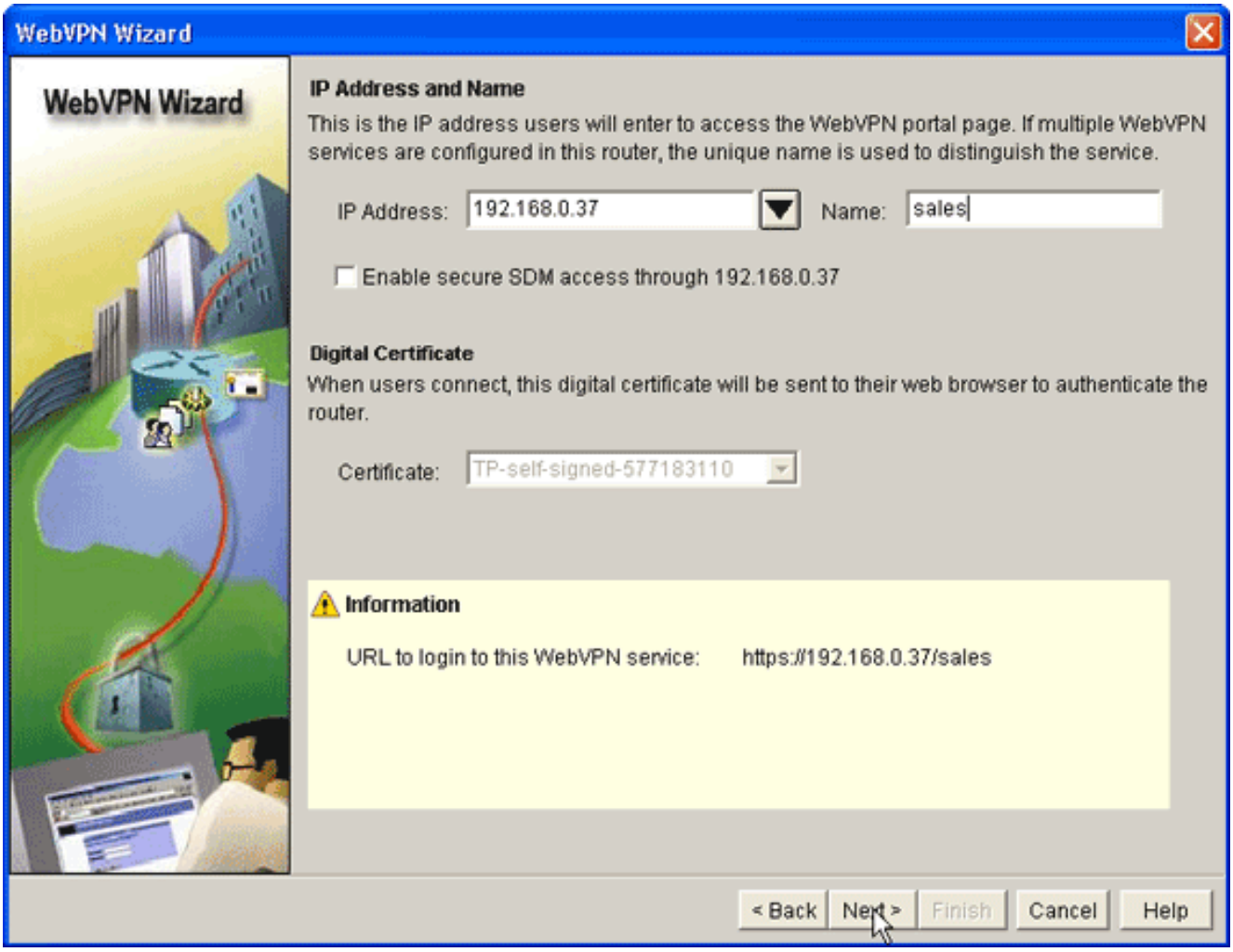
1. Wenn der SVC auf dem Router installiert ist, klicken Sie auf **Konfigurieren** und dann auf **VPN**.
2. Klicken Sie auf **WebVPN**, und klicken Sie auf die Registerkarte **Create WebVPN (WebVPN erstellen)**.




3. Aktivieren Sie das Optionsfeld **Neues WebVPN erstellen**, und klicken Sie dann auf **Ausgewählte Aufgabe starten**.Das Dialogfeld WebVPN-Assistent wird angezeigt.




4. Klicken Sie auf **Weiter**.



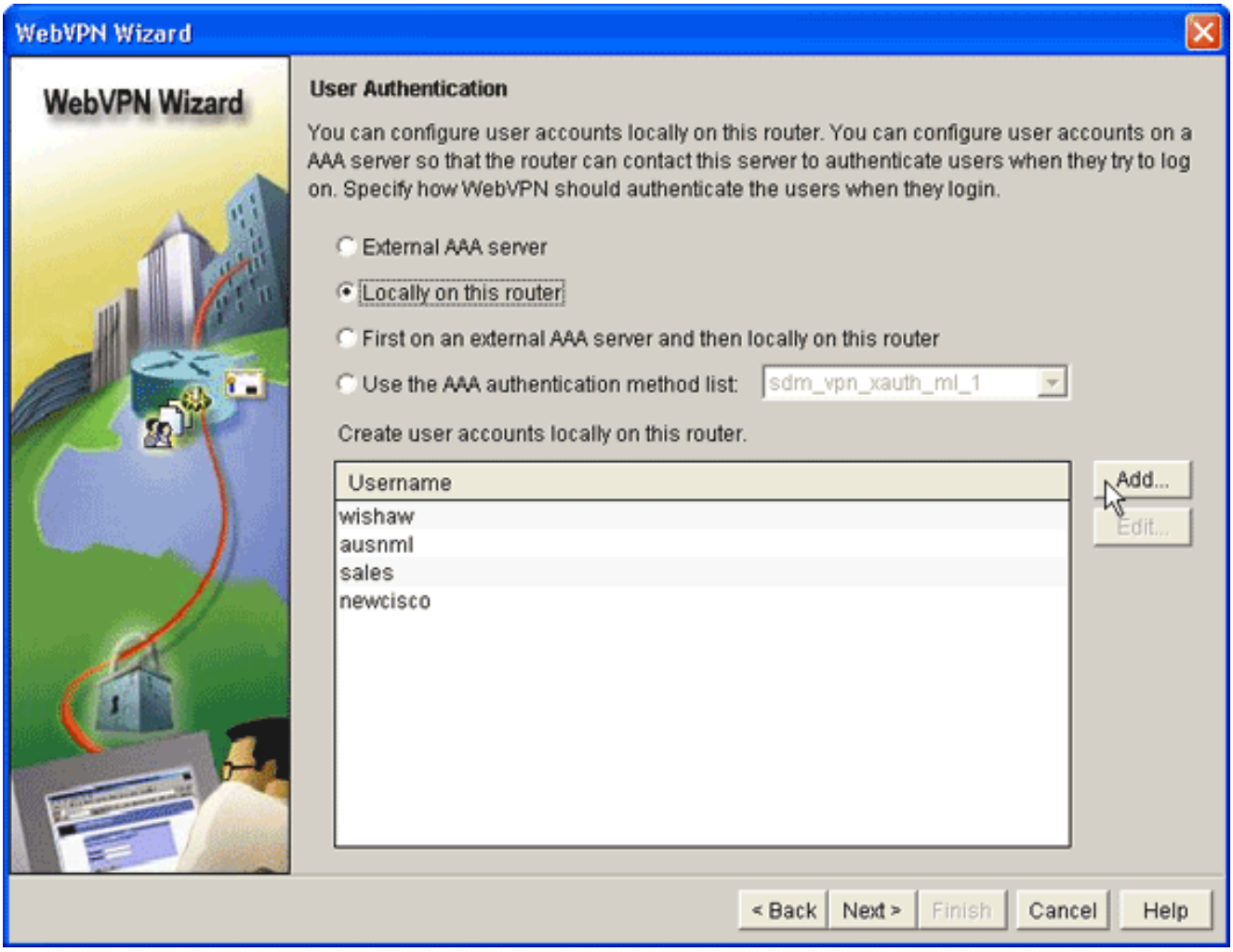

5. Geben Sie die IP-Adresse des neuen WebVPN-Gateways ein, und geben Sie einen eindeutigen Namen für diesen WebVPN-Kontext ein.Sie können verschiedene WebVPN-Kontexte für dieselbe IP-Adresse (WebVPN-Gateway) erstellen, aber jeder Name muss eindeutig sein. In diesem Beispiel wird diese IP-Adresse verwendet: *https://192.168.0.37/sales*
6. Klicken Sie auf **Weiter**, und fahren Sie mit Schritt 3 fort.

## Schritt 3: Konfigurieren der Benutzerdatenbank für SVC-Benutzer

Zur Authentifizierung können Sie einen AAA-Server, lokale Benutzer oder beide verwenden. In diesem Konfigurationsbeispiel werden lokal erstellte Benutzer für die Authentifizierung verwendet.

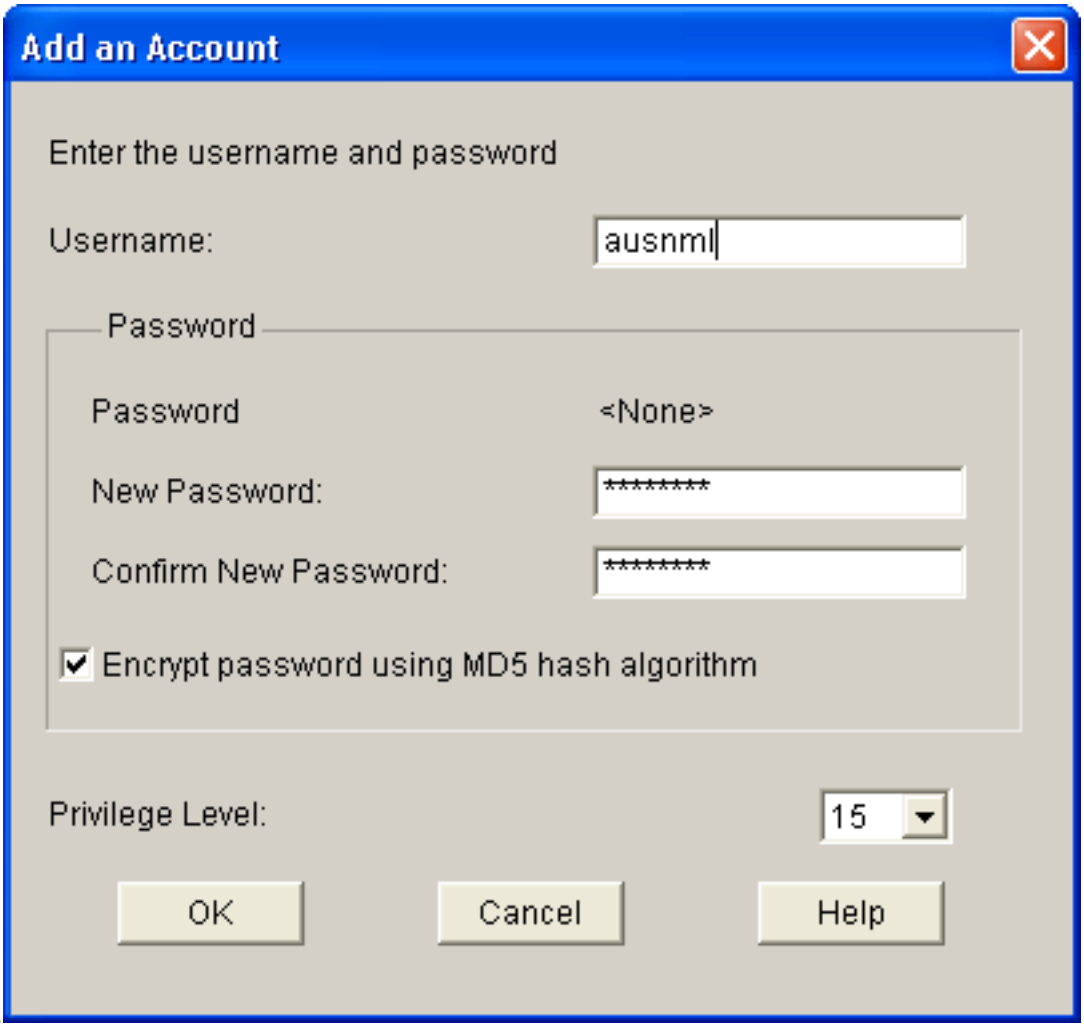
Gehen Sie wie folgt vor, um die Benutzerdatenbank für SVC-Benutzer zu konfigurieren:

1. Wenn Sie Schritt 2 abgeschlossen haben, klicken Sie auf das Optionsfeld **Lokal auf diesem Router** im Dialogfeld WebVPN Wizard User Authentication (Benutzerauthentifizierung des WebVPN-
Assistenten).




In diesem Dialogfeld können Sie Benutzer zur lokalen Datenbank hinzufügen.

2. Klicken Sie auf **Hinzufügen**, und geben Sie Benutzerinformationen




ein.

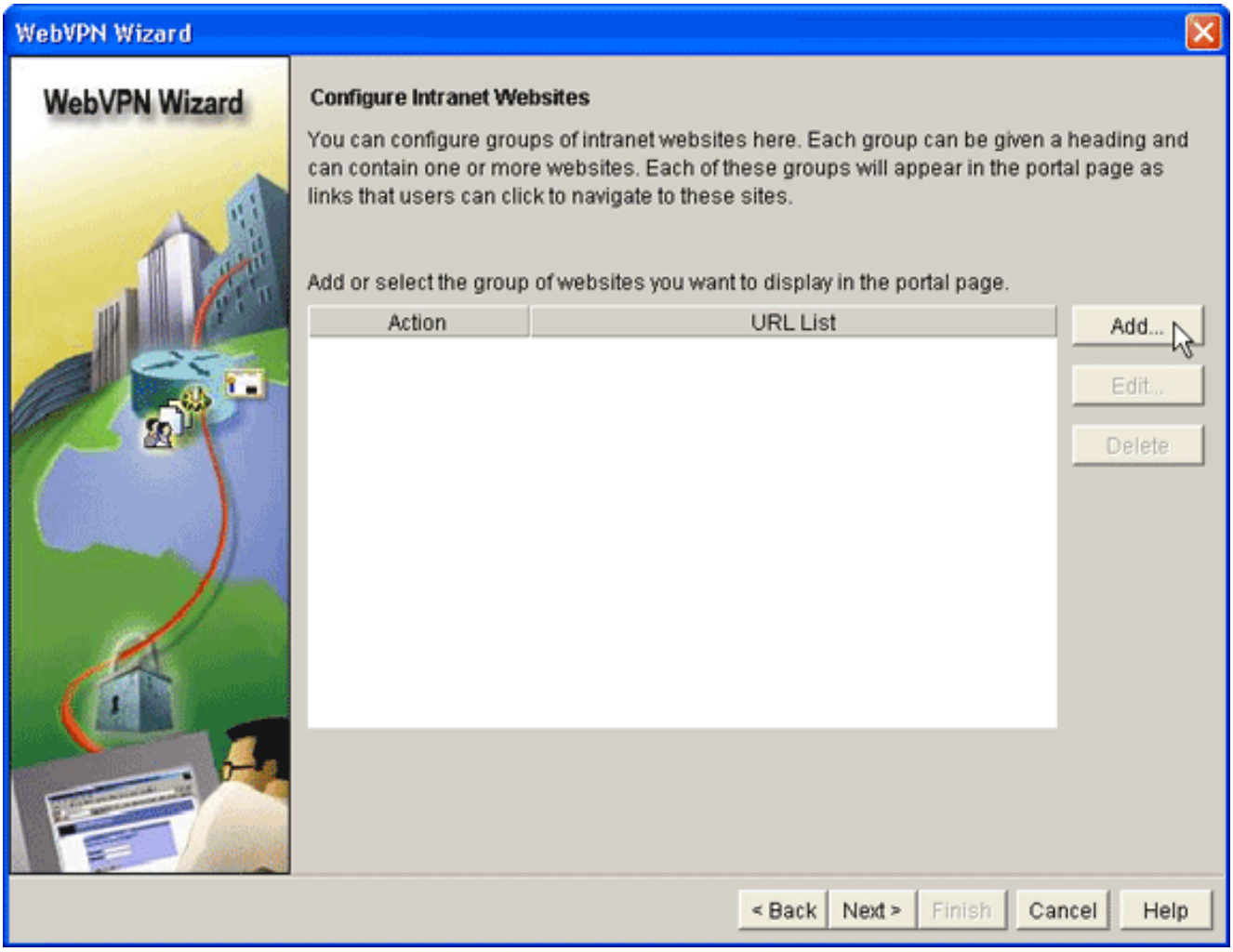
3. Klicken Sie auf **OK**, und fügen Sie bei Bedarf weitere Benutzer hinzu.
4. Nachdem Sie die erforderlichen Benutzer hinzugefügt haben, klicken Sie auf **Weiter** und fahren Sie mit Schritt 4 fort.

## Schritt 4: Konfigurieren der Ressourcen zum Verfügbarmachen für Benutzer

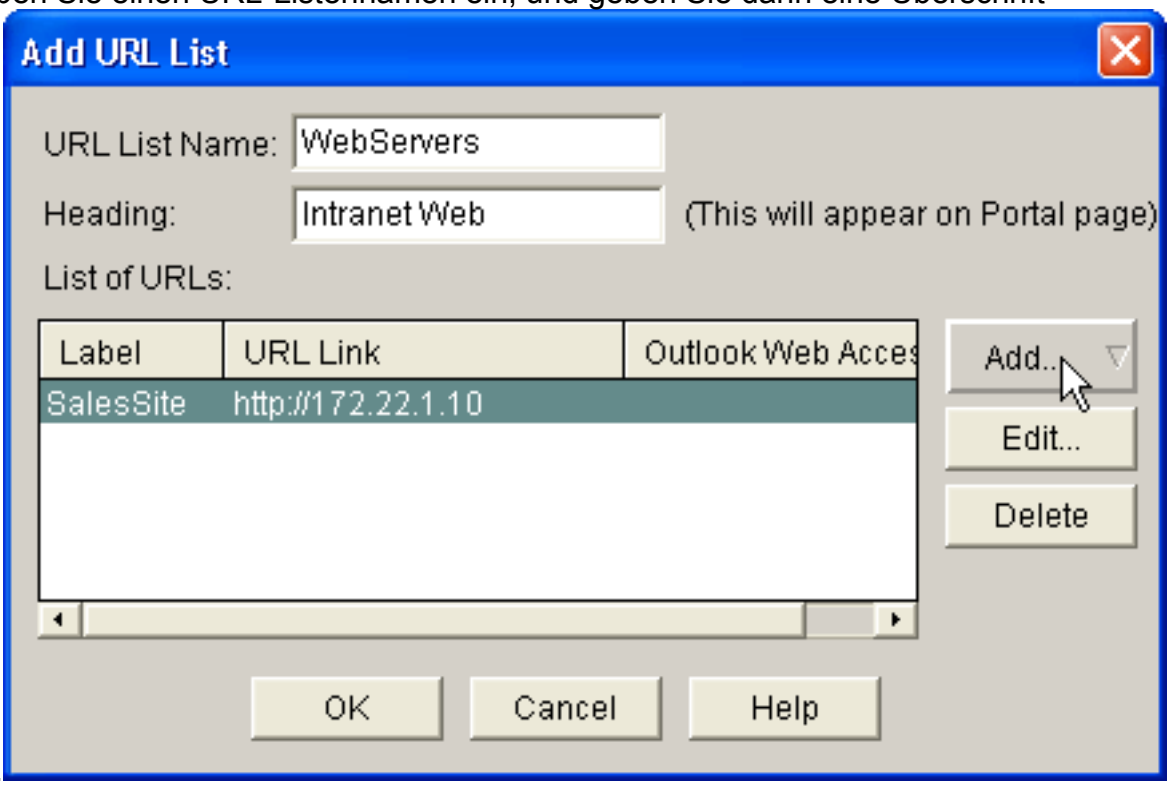
Im Dialogfeld WebVPN-Assistent für das Konfigurieren von Intranet-Websites können Sie die Intranet-Ressourcen auswählen, die Sie Ihren SVC-Clients zur Verfügung stellen möchten.

Gehen Sie wie folgt vor, um die Ressourcen zu konfigurieren, die Benutzern verfügbar gemacht werden sollen:

1. Wenn Sie Schritt 3 abgeschlossen haben, klicken Sie auf die Schaltfläche **Hinzufügen** im Dialogfeld Intranet-Websites
   konfigurieren.

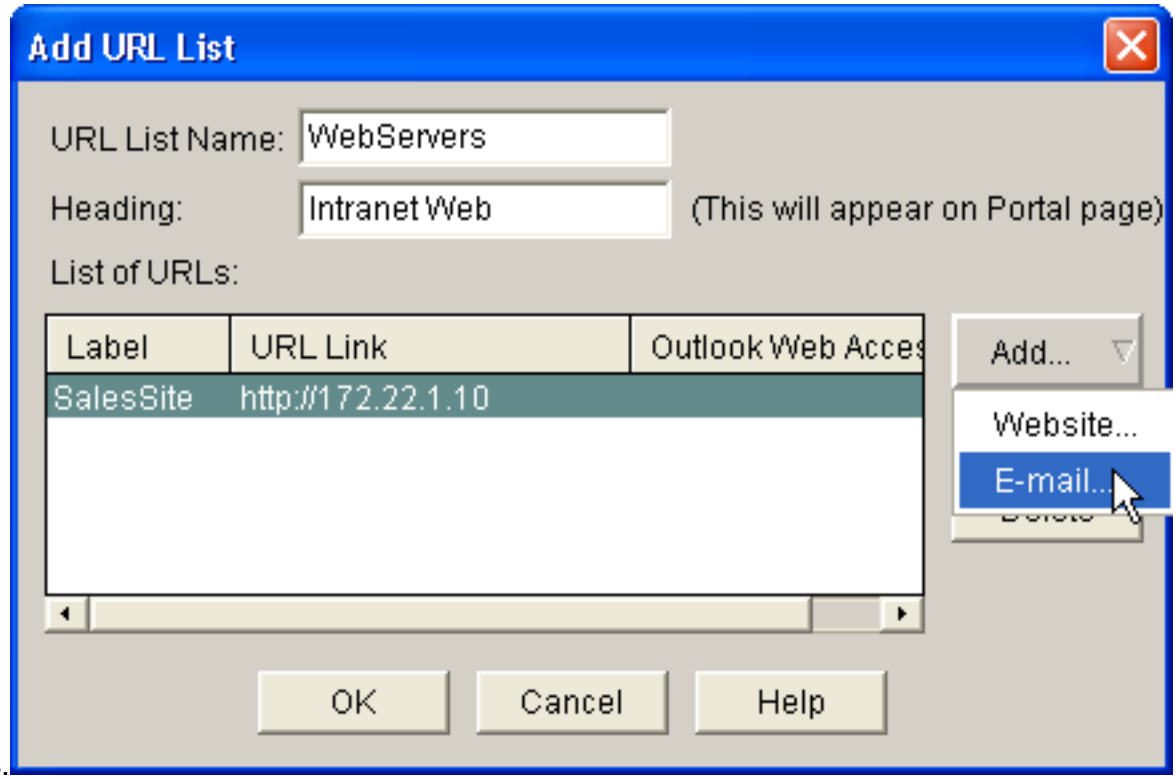



2. Geben Sie einen URL-Listennamen ein, und geben Sie dann eine Überschrift



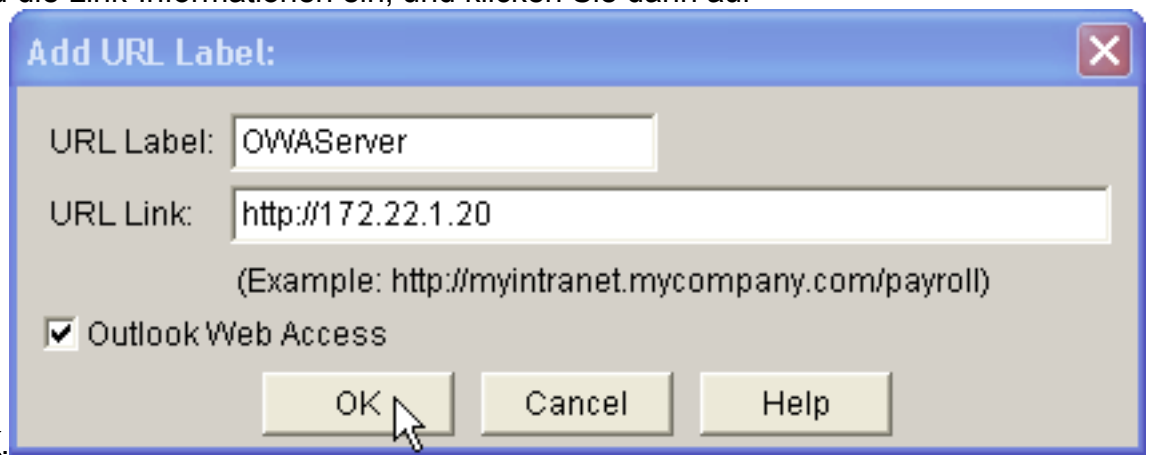

ein.

3. Klicken Sie auf **Hinzufügen**, und wählen Sie **Website** aus, um die Websites hinzuzufügen, die Sie diesem Client zugänglich machen möchten.
4. Geben Sie die URL und die Link-Informationen ein, und klicken Sie dann auf **OK**.
5. Um den Zugriff auf OWA Exchange Server hinzuzufügen, klicken Sie auf **Hinzufügen** und wählen Sie **E-Mail**



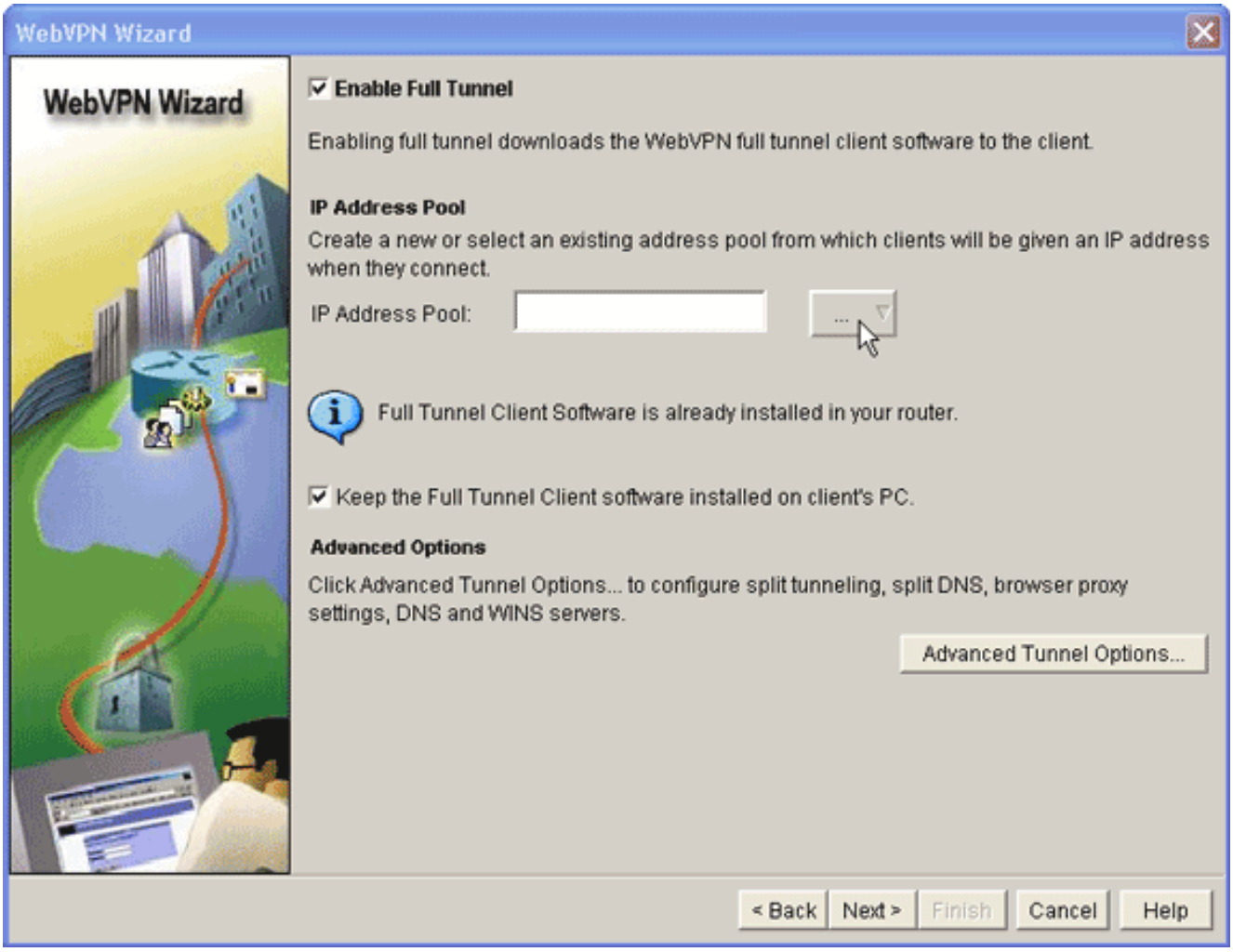

**aus**.

6. Aktivieren Sie das Kontrollkästchen **Outlook Web Access**, geben Sie die URL-Bezeichnung und die Link-Informationen ein, und klicken Sie dann auf

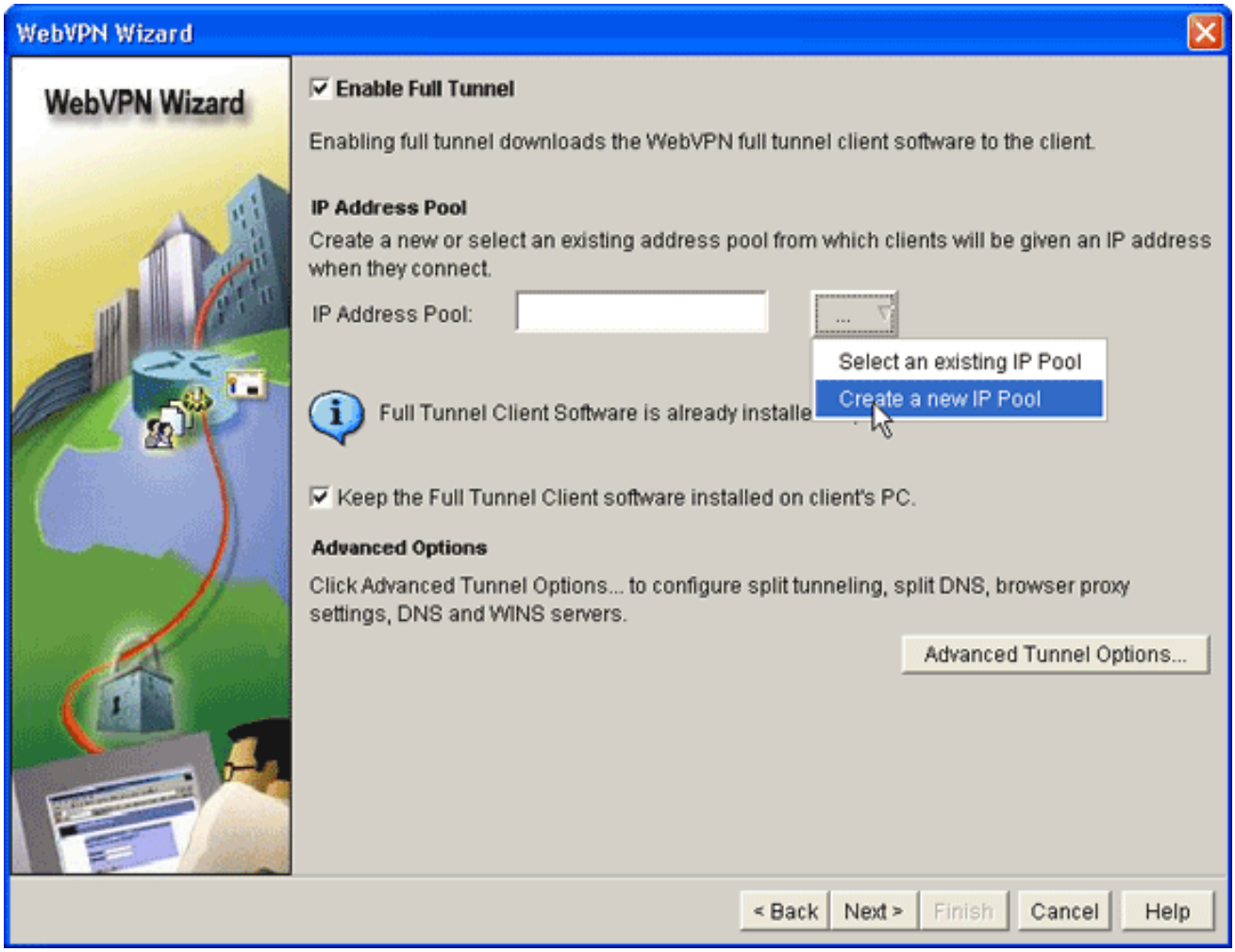



**OK**.

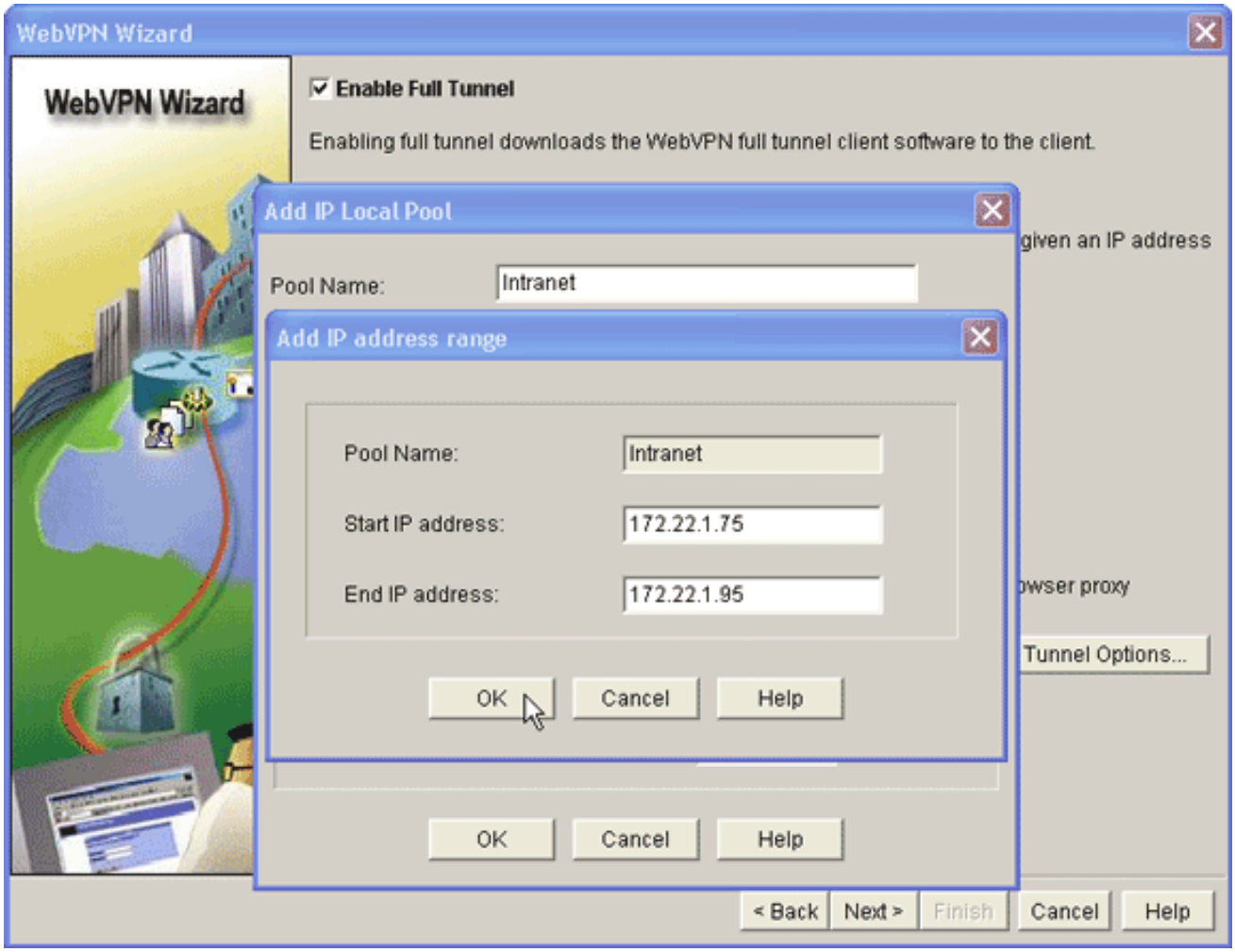
7. Nachdem Sie die gewünschten Ressourcen hinzugefügt haben, klicken Sie auf **OK** und klicken Sie anschließend auf **Weiter**.Das Dialogfeld WebVPN Wizard Full Tunnel (Vollständiger WebVPN-Assistent) wird angezeigt.



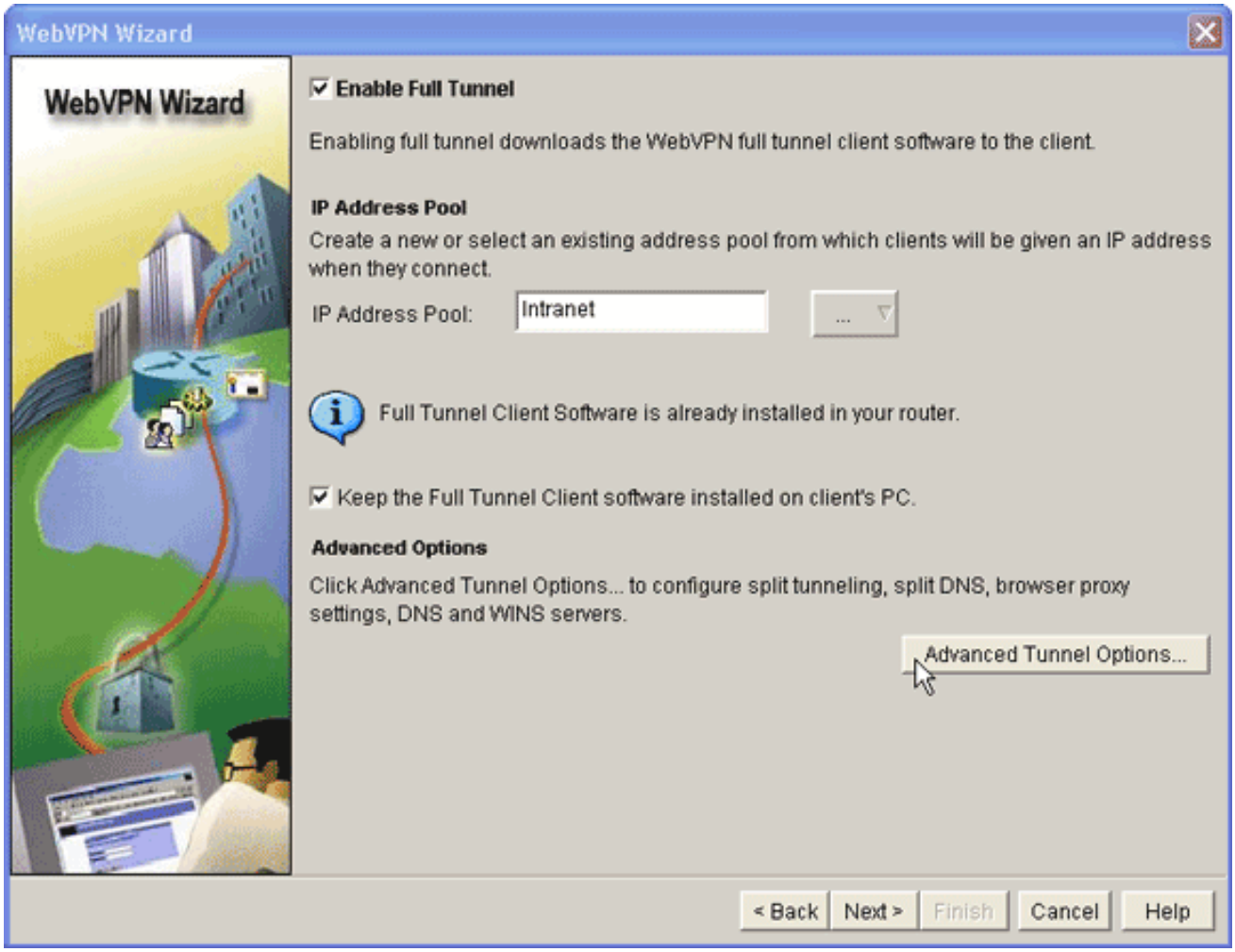

8. Vergewissern Sie sich, dass das Kontrollkästchen **Full Tunnel aktivieren** aktiviert ist.
9. Erstellen Sie einen Pool von IP-Adressen, den Clients dieses WebVPN-Kontexts verwenden können. Der Adresspool muss den im Intranet verfügbaren und routingfähigen Adressen entsprechen.
10. Klicken Sie auf die Auslassungszeichen (**...**) neben dem Feld "IP Address Pool" (IP-Adresspool), und wählen Sie **Create a new IP Pool (Neuen IP-Pool erstellen)** aus.



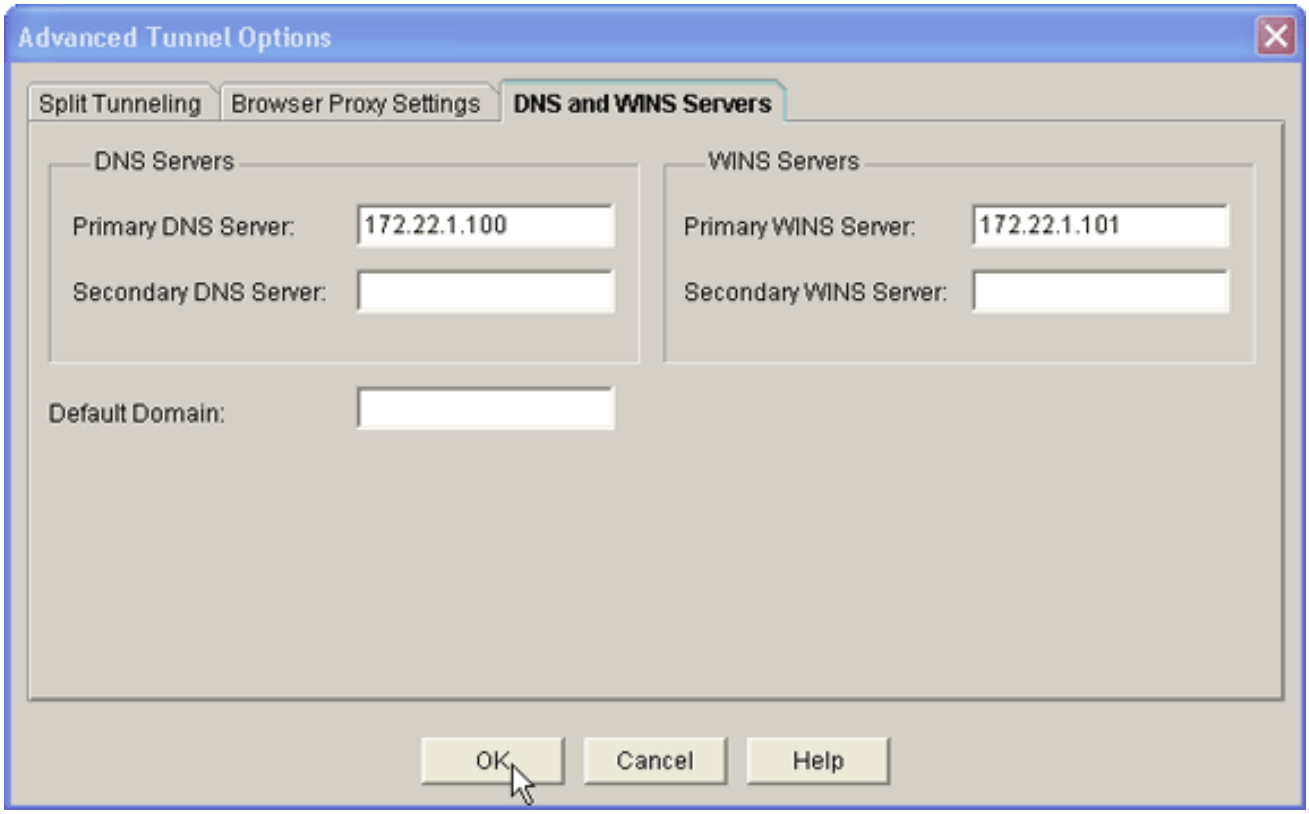

11. Geben Sie im Dialogfeld Lokalen IP-Pool hinzufügen einen Namen für den Pool ein, und klicken Sie auf **Hinzufügen**.



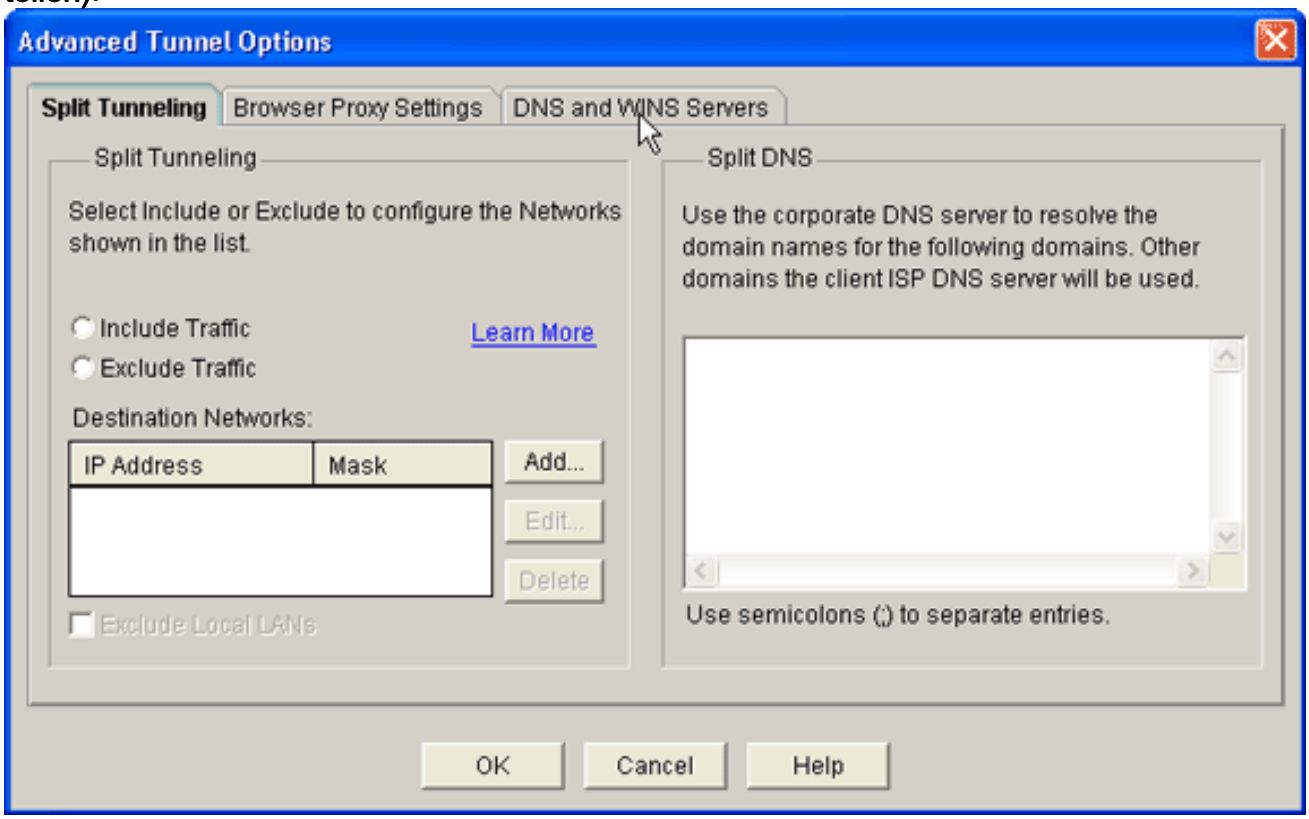

12. Geben Sie im Dialogfeld IP-Adressbereich hinzufügen den Adresspoolbereich für die SVC-Clients ein, und klicken Sie auf **OK**.**Hinweis:** Der IP-Adresspool sollte sich in einem Bereich einer Schnittstelle befinden, die direkt mit dem Router verbunden ist. Wenn Sie einen anderen Pool-Bereich verwenden möchten, können Sie eine Loopback-Adresse erstellen, die dem neuen Pool zugeordnet ist, um diese Anforderung zu erfüllen.
13. Klicken Sie auf
    **OK**.



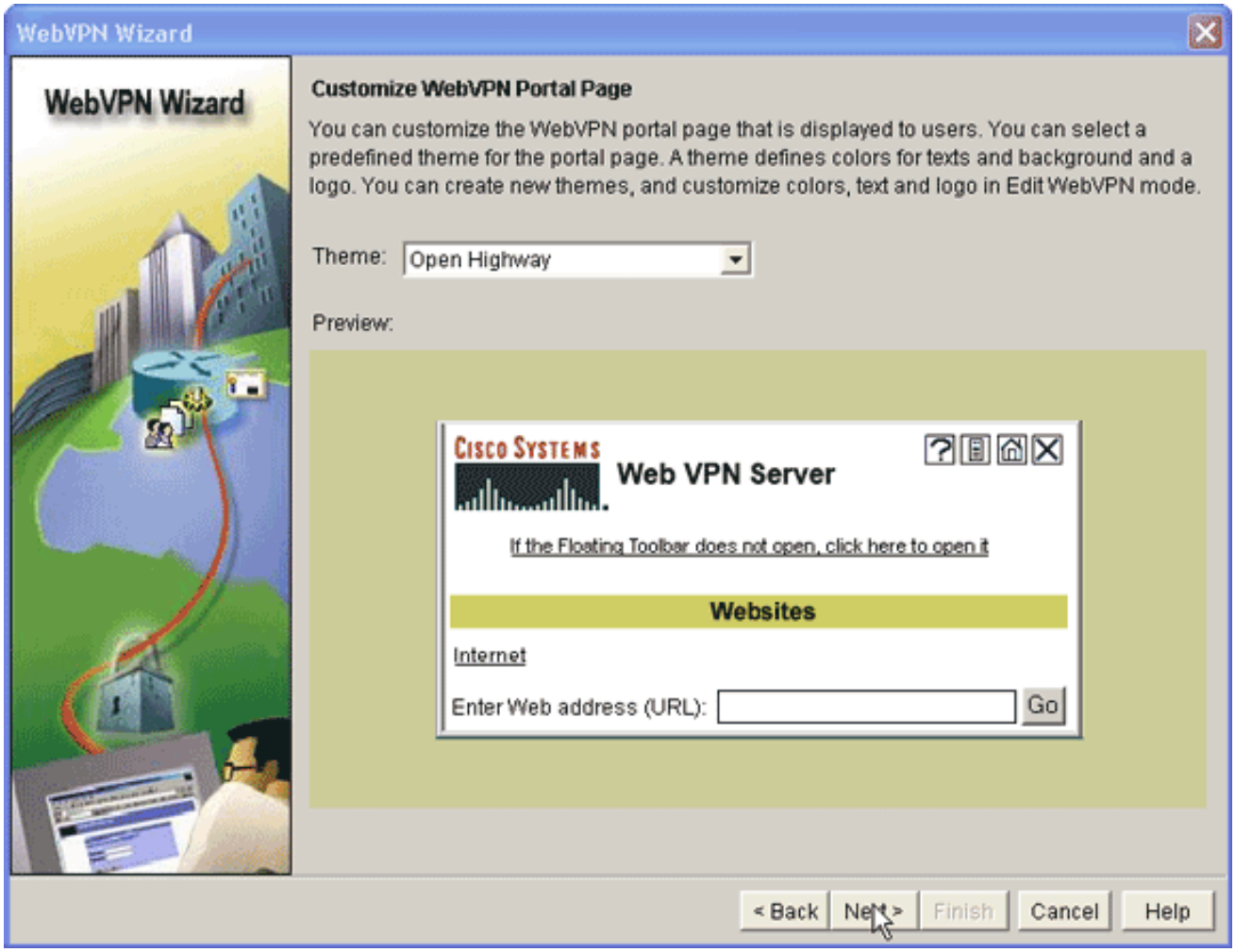

14. Wenn Sie möchten, dass Ihre Remote-Clients eine Kopie des SVC dauerhaft speichern, klicken Sie auf das Kontrollkästchen **Vollständige Tunnel-Client-Software auf dem Client-PC installieren**. Deaktivieren Sie diese Option, damit der Client die SVC-Software jedes Mal herunterladen muss, wenn ein Client eine Verbindung herstellt.
15. Erweiterte Tunneloptionen wie Split-Tunneling, Split DNS, Browser-Proxy-Einstellungen und DNS- und WNS-Server konfigurieren. Cisco empfiehlt, mindestens DNS- und WINS-Server zu konfigurieren.Gehen Sie wie folgt vor, um erweiterte Tunneloptionen zu konfigurieren:Klicken Sie auf die Schaltfläche **Erweiterte Tunneloptionen**.



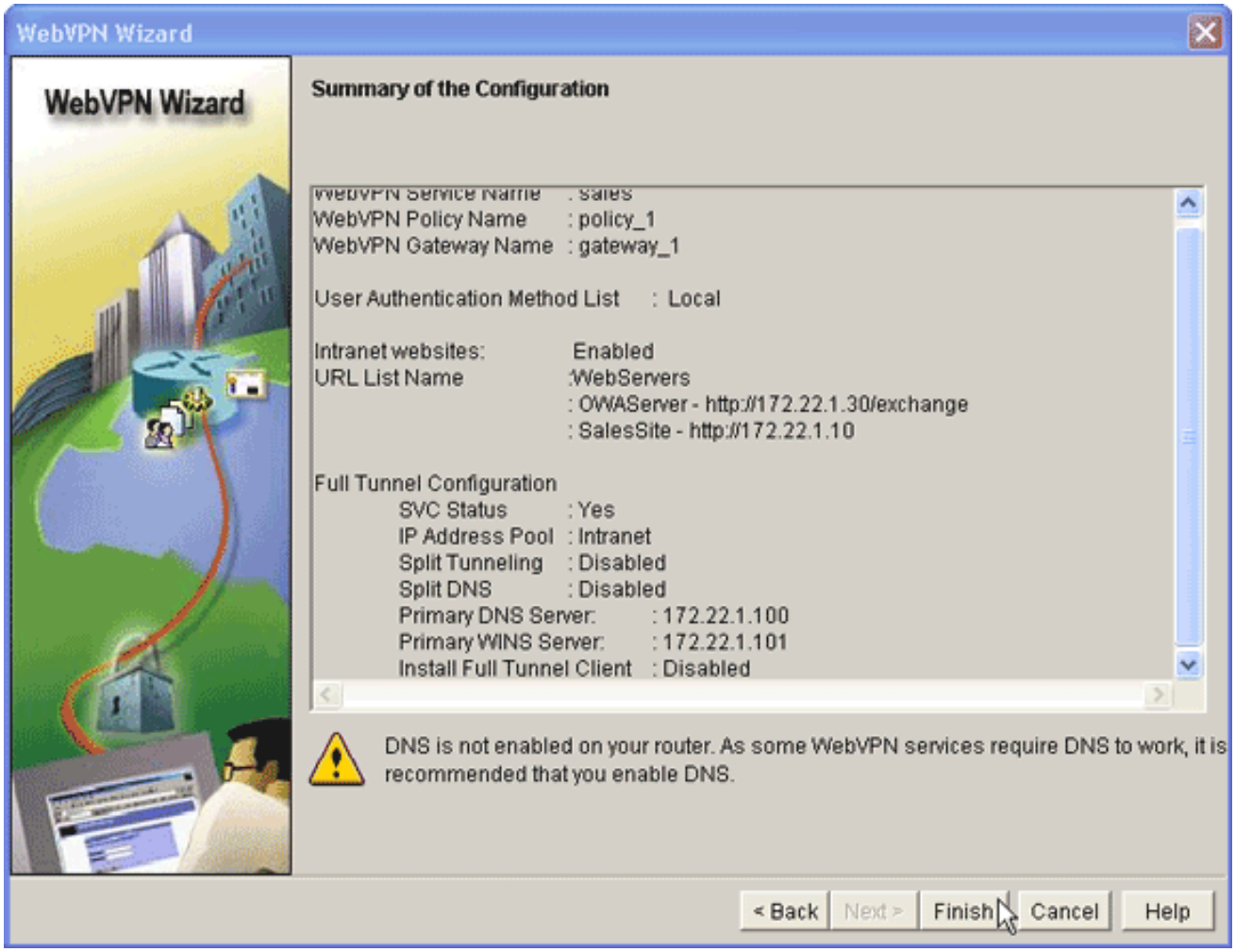

Klicken Sie auf die Registerkarte **DNS- und WINS-Server**, und geben Sie die primären IP-Adressen für die DNS- und WINS-Server ein.Zum Konfigurieren von Split-Tunneling- und Browser-Proxy-Einstellungen klicken Sie auf die Registerkarte **Split Tunneling** oder **Browser Proxy Settings (Browserproxy-Einstellungen teilen)**.



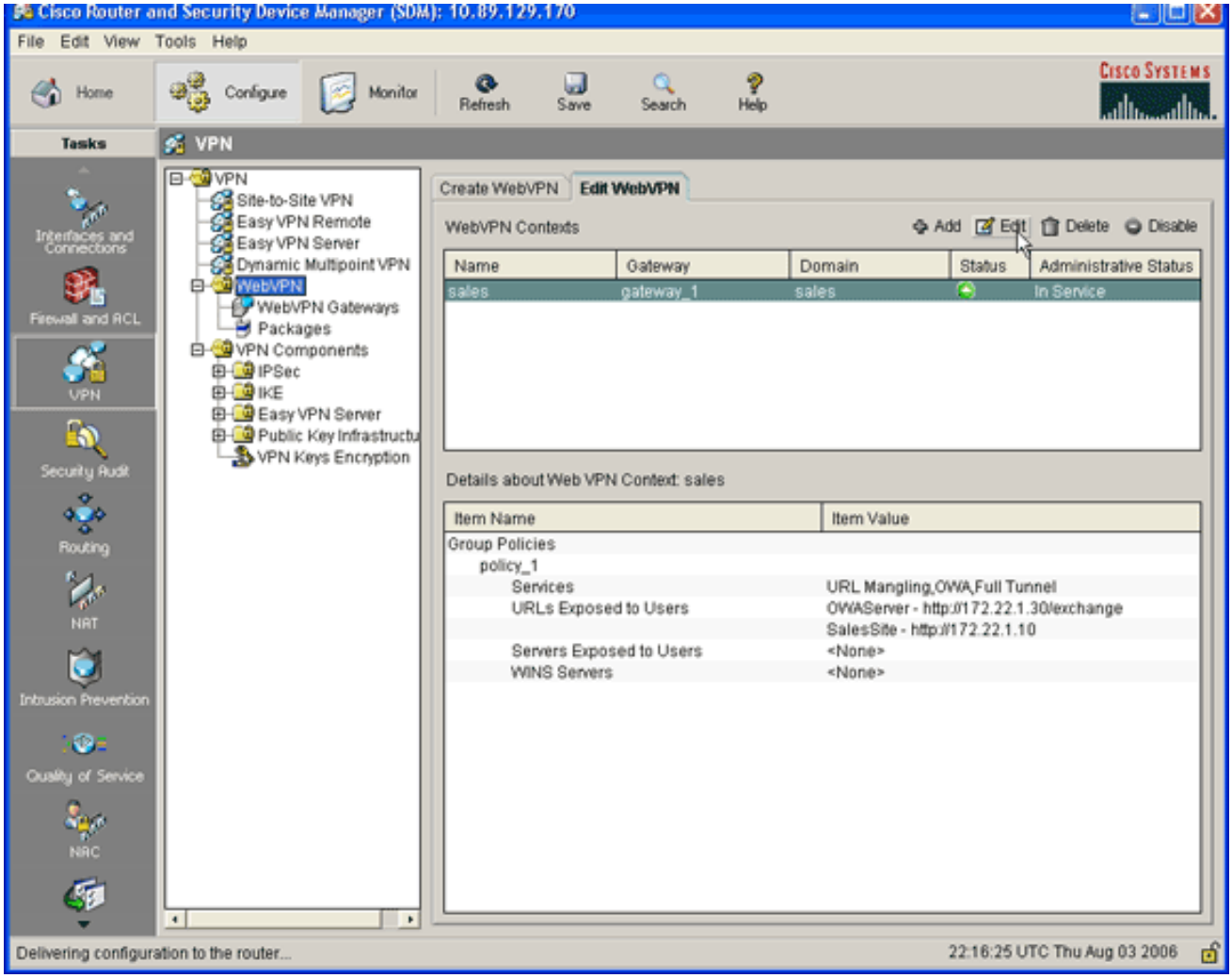

16. Wenn Sie die erforderlichen Optionen konfiguriert haben, klicken Sie auf **Weiter**.
17. Passen Sie die WebVPN-Portalseite an, oder wählen Sie die Standardwerte aus.Auf der Seite WebVPN-Portal anpassen können Sie festlegen, wie die WebVPN-Portalseite für Ihre Kunden angezeigt
wird.



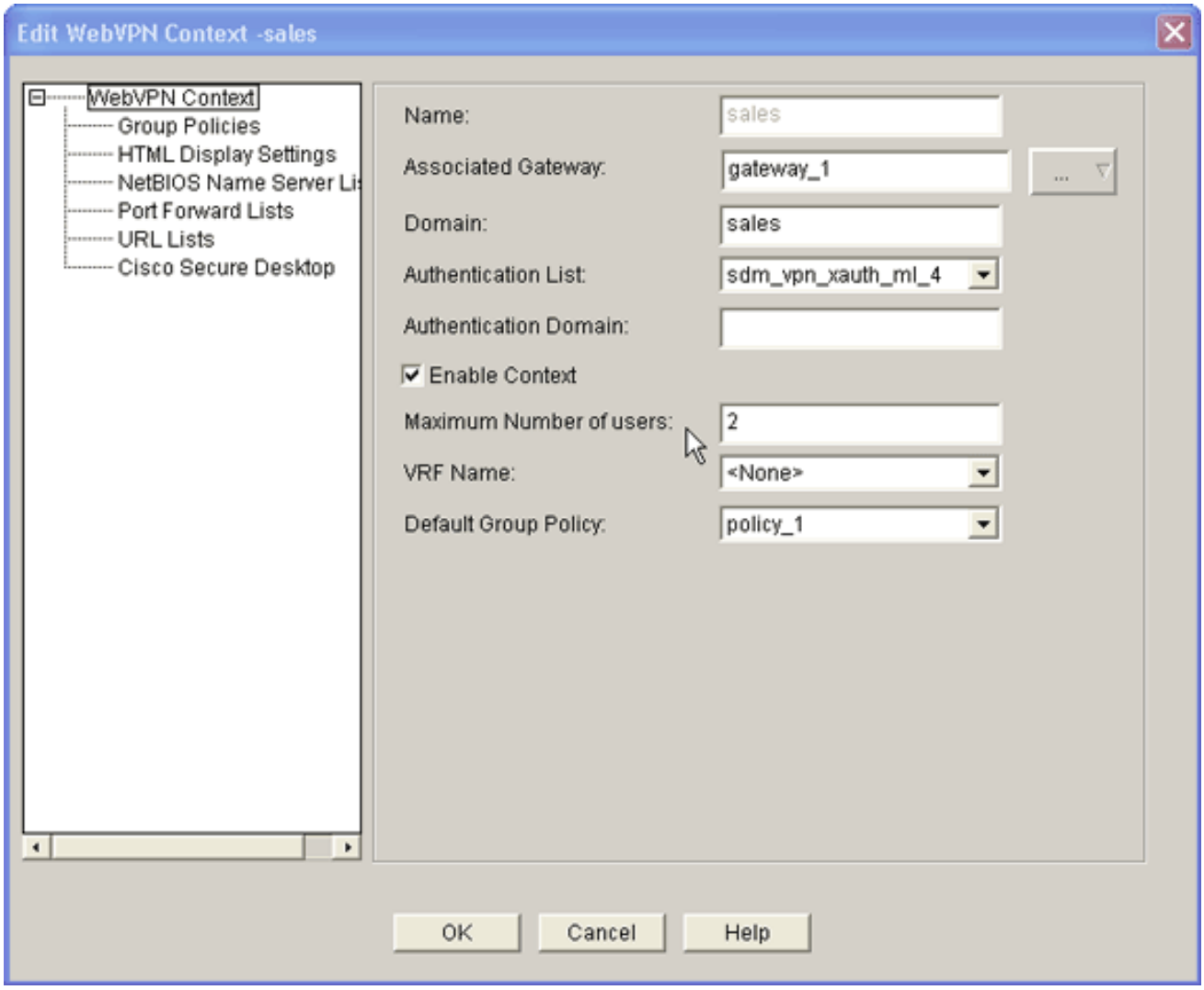

18. Nachdem Sie die WebVPN-Portalseite konfiguriert haben, klicken Sie auf **Weiter**, auf **Fertig stellen** und dann auf **OK**.Der WebVPN-Assistent sendet Tourbefehle an den Router.
19. Klicken Sie auf **OK**, um die Konfiguration zu speichern.**Hinweis:** Wenn Sie eine Fehlermeldung erhalten, ist die WebVPN-Lizenz möglicherweise falsch. In diesem Bild wird eine Beispielfehlermeldung
angezeigt:




Gehen Sie wie folgt vor, um ein Lizenzproblem zu beheben:Klicken Sie auf **Konfigurieren** und dann auf **VPN**.Erweitern Sie **WebVPN**, und klicken Sie auf die Registerkarte **WebVPN bearbeiten**.




Markieren Sie den neu erstellten Kontext, und klicken Sie auf die Schaltfläche **Bearbeiten**.




Geben Sie im Feld Maximum Number of users (Maximale Anzahl von Benutzern) die richtige Anzahl von Benutzern für Ihre Lizenz ein.Klicken Sie auf **OK** und dann auf **OK**.Ihre Befehle werden in die Konfigurationsdatei geschrieben.Klicken Sie auf **Speichern** und dann auf **Ja**, um die Änderungen zu übernehmen.

## Ergebnisse

Der ASDM erstellt folgende Befehlszeilenkonfigurationen:

**ausml-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
```

# Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

### Vorgehensweise

Um Ihre Konfiguration zu testen, geben Sie *http://192.168.0.37/sales* in einen SSL-fähigen Client-Webbrowser ein.

## Befehle

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Detaillierte Informationen zu **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.

**Hinweis:** Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

# Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

## Problem mit der SSL-Verbindung

**Problem:** SSL VPN-Clients können keine Verbindung zum Router herstellen.

**Lösung:** Dieses Problem kann durch unzureichende IP-Adressen im IP-Adresspool verursacht werden. Erhöhen Sie die Anzahl der IP-Adressen im Pool der IP-Adressen auf dem Router, um dieses Problem zu beheben.

## Befehle zur Fehlerbehebung

Dem WebVPN sind mehrere **Clear** Befehle zugeordnet. Detaillierte Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN Clear-Befehlen.

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Ausführliche Informationen zu diesen Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen.

**Hinweis:** Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

# Zugehörige Informationen

- Cisco IOS SSL VPN
- SSL VPN - WebVPN
- Clientless-SSL-VPN (WebVPN) auf Cisco IOS mit SDM-Konfigurationsbeispiel
- Beispiel einer IOS-Konfiguration mit Thin-Client SSL VPN (WebVPN) mit SDM
- Implementierungsleitfaden für WebVPN- und DMVPN-Konvergenz
- Technischer Support und Dokumentation - Cisco Systems