Konfigurieren von Thin-Client SSL VPN (WebVPN) Cisco IOS mit SDM

Inhalt

Einleitung

Die Thin-Client SSL VPN-Technologie ermöglicht den sicheren Zugriff für Anwendungen, die statische Ports verwenden. Beispiele hierfür sind Telnet (23), SSH (22), POP3 (110), IMAP4 (143) und SMTP (25). Der Thin-Client kann benutzergesteuert, richtliniengesteuert oder beides sein. Der Zugriff kann für jeden Benutzer konfiguriert werden, oder es können Gruppenrichtlinien erstellt werden, die einen oder mehrere Benutzer enthalten. Die SSL VPN-Technologie kann in drei Hauptmodi konfiguriert werden: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port Forwarding) und SSL VPN Client (SVC Full Tunnel Mode).

1. Clientless-SSL-VPN (WebVPN):

Ein Remote-Client benötigt nur einen SSL-fähigen Webbrowser, um auf HTTP- oder HTTPS-fähige Webserver im Firmen-LAN zuzugreifen. Über das Common Internet File System (CIFS) können Sie auch nach Windows-Dateien suchen. Ein gutes Beispiel für den http-Zugriff ist der Outlook Web Access (OWA)-Client.

Weitere Informationen zum Clientless-SSL-VPN finden Sie unter Clientless SSL VPN (WebVPN) auf Cisco IOS mit SDM-Konfigurationsbeispiel.

2. Thin-Client SSL VPN (Port Forwarding)

Ein Remote-Client muss ein kleines, Java-basiertes Applet für den sicheren Zugriff auf TCP-Anwendungen herunterladen, die statische Portnummern verwenden. UDP wird nicht unterstützt. Beispiele sind der Zugriff auf POP3, SMTP, IMAP, SSH und Telnet. Der Benutzer benötigt lokale Administratorberechtigungen, da Änderungen an Dateien auf dem lokalen Computer vorgenommen werden. Diese SSL VPN-Methode funktioniert nicht mit Anwendungen, die dynamische Portzuweisungen verwenden, z. B. mehrere FTP-Anwendungen.

3. SSL VPN-Client (SVC-Full Tunnel Mode):

Der SSL VPN Client lädt einen kleinen Client auf die Remote-Workstation herunter und ermöglicht einen vollständigen, sicheren Zugriff auf die Ressourcen im internen Unternehmensnetzwerk. Der SVC kann dauerhaft auf die Remote-Station heruntergeladen oder nach Beendigung der sicheren Sitzung entfernt werden.

Weitere Informationen zum SSL VPN Client finden Sie unter SSL VPN Client (SVC) unter IOS mit SDM Configuration Example.

Dieses Dokument zeigt eine einfache Konfiguration für das Thin-Client SSL VPN auf einem Cisco IOS®-Router. Das Thin-Client SSL VPN wird auf den folgenden Cisco IOS-Routern ausgeführt:

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

Voraussetzungen

Anforderungen

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

Anforderungen für den Cisco IOS-Router

- Jeder der aufgeführten Router, der mit SDM und einem erweiterten Image der IOS-Version 12.4(6)T oder höher geladen wurde
- Management-Station mit SDMCisco liefert neue Router mit vorinstallierter SDM-Kopie. Wenn auf Ihrem Router kein SDM installiert ist, können Sie die Software unter Software Download - Cisco Security Device Manager beziehen. Sie müssen über ein CCO-Konto mit einem Servicevertrag verfügen. Detaillierte Anweisungen hierzu finden Sie unter Konfigurieren des Routers mit dem Sicherheitsgerätemanager.

Anforderungen an Client-Computer

- Remote-Clients sollten über lokale Administratorberechtigungen verfügen. Sie ist nicht erforderlich, wird jedoch nachdrücklich empfohlen.
- Remote-Clients müssen über Java Runtime Environment (JRE) Version 1.4 oder höher verfügen.
- Remote-Client-Browser: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 oder Firefox 1.0
- Cookies aktiviert und Popups auf Remote-Clients zugelassen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Advanced Enterprise Software Image 12.4(9)T
- Cisco Integrated Services Router 3825
- Cisco Router and Security Device Manager (SDM) Version 2.3.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer leeren (Standard-)Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen. Die für diese Konfiguration verwendeten IP-Adressen stammen aus dem RFC 1918-Adressbereich. Sie sind im Internet nicht legal.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

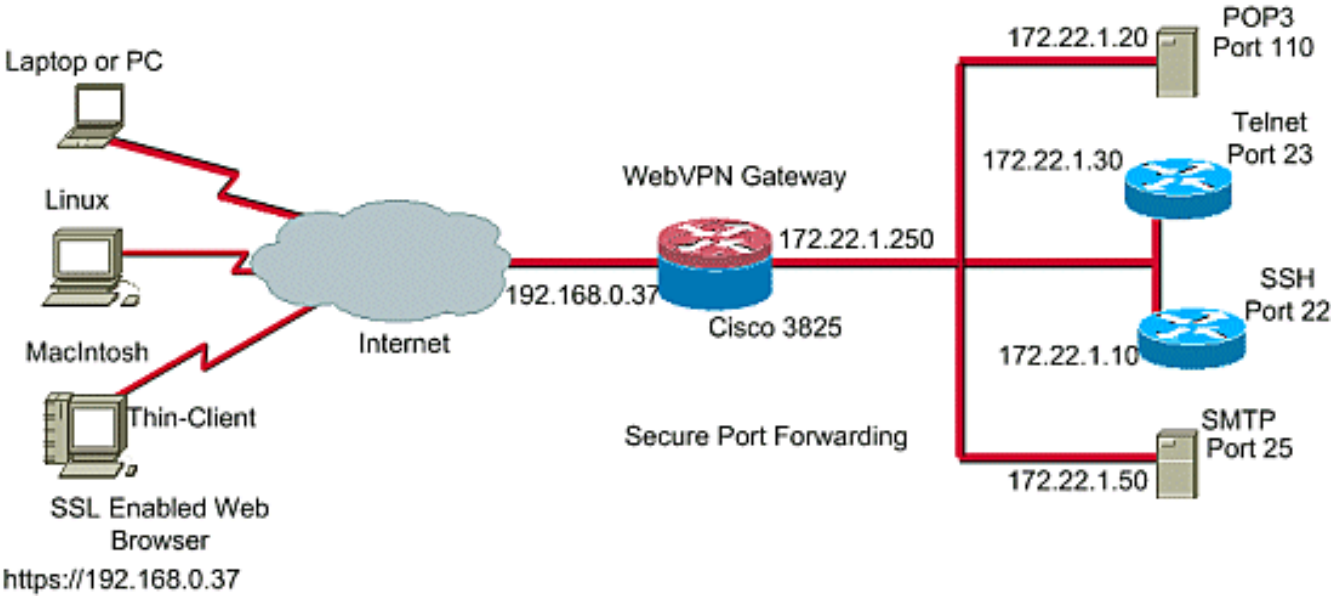
Konfigurieren

Aufgabe

Dieser Abschnitt enthält die erforderlichen Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

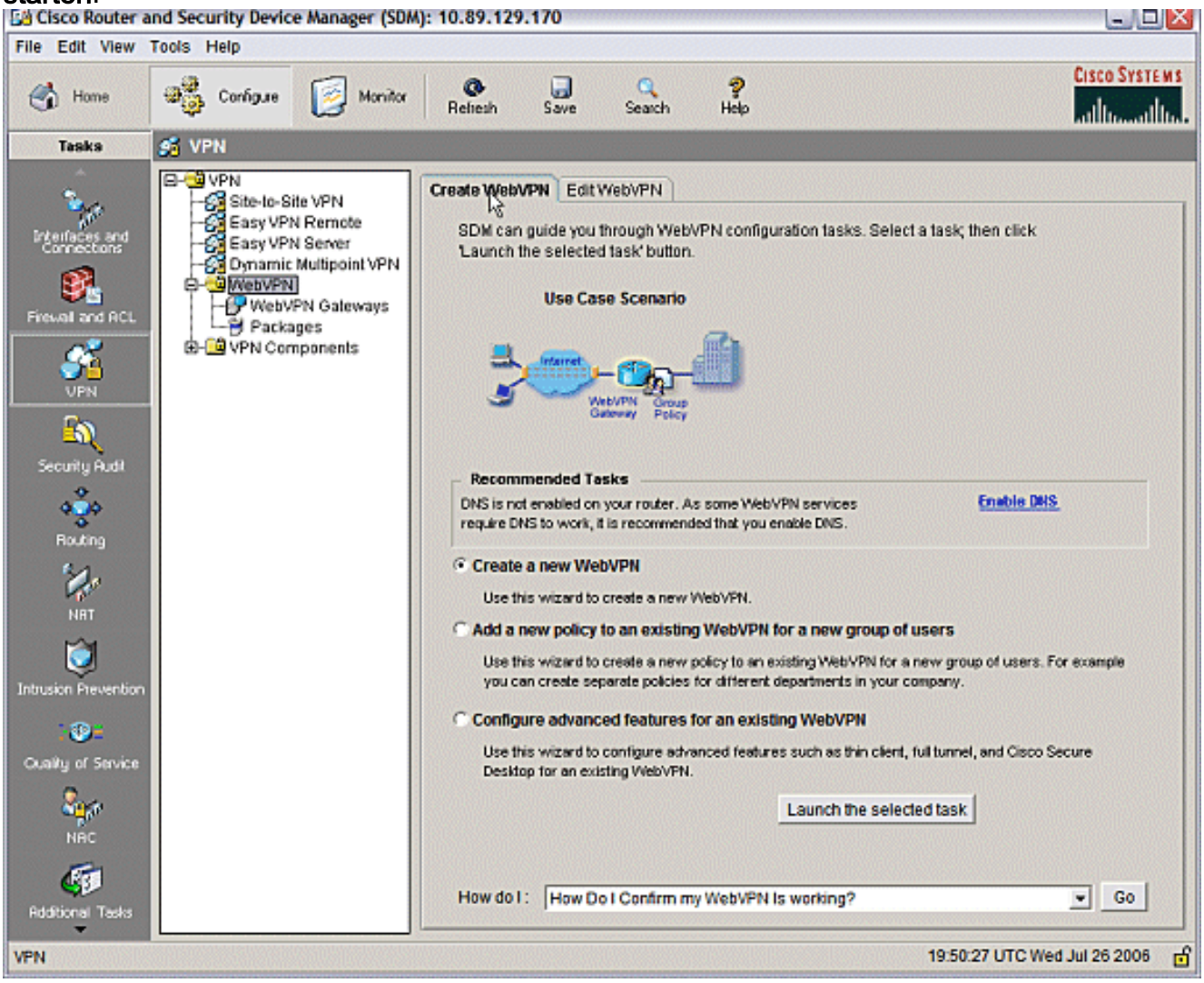


Konfigurieren des Thin-Client SSL VPN

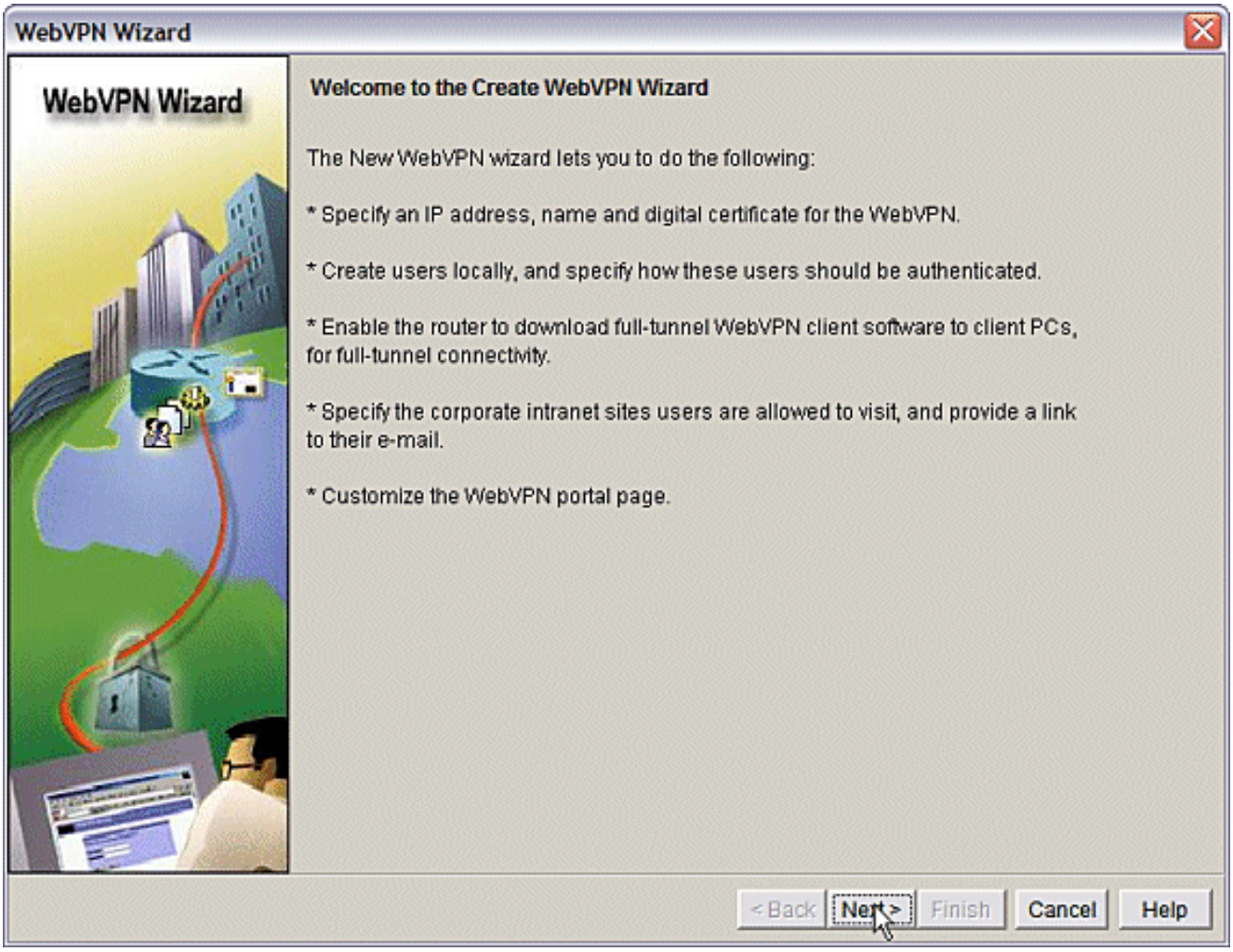
Verwenden Sie den in der SDM-Schnittstelle (Security Device Manager) bereitgestellten

Assistenten, um das Thin-Client SSL VPN in Cisco IOS zu konfigurieren, oder konfigurieren Sie es entweder über die Befehlszeilenschnittstelle (CLI) oder manuell in der SDM-Anwendung. In diesem Beispiel wird der Assistent verwendet.

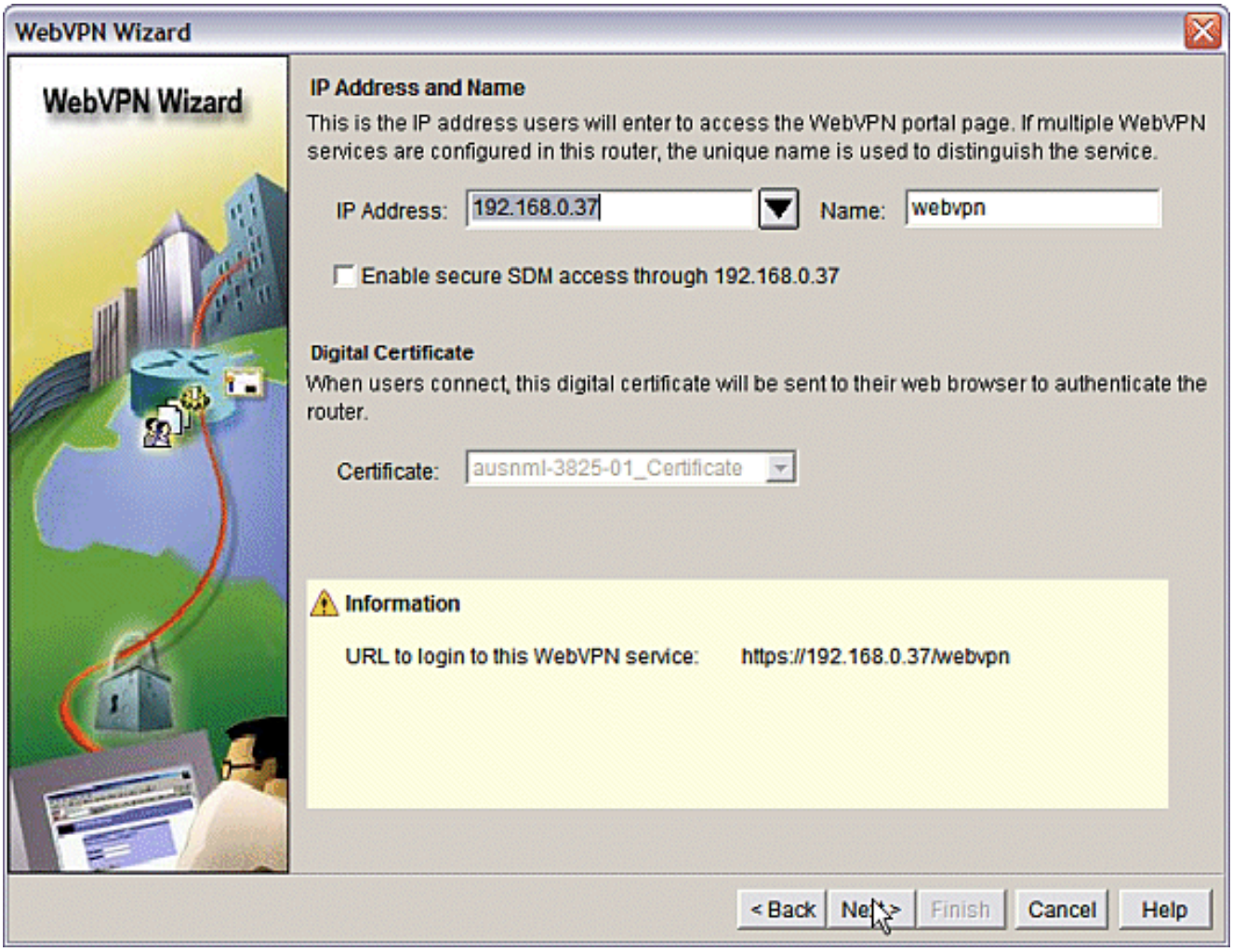
1. Wählen Sie die Registerkarte **Konfigurieren**.Wählen Sie im Navigationsbereich **VPN > WebVPN aus**.Klicken Sie auf die Registerkarte **WebVPN erstellen**.Klicken Sie auf das Optionsfeld neben **Neues WebVPN erstellen**.Klicken Sie auf die Schaltfläche **Ausgewählte Aufgabe starten**.



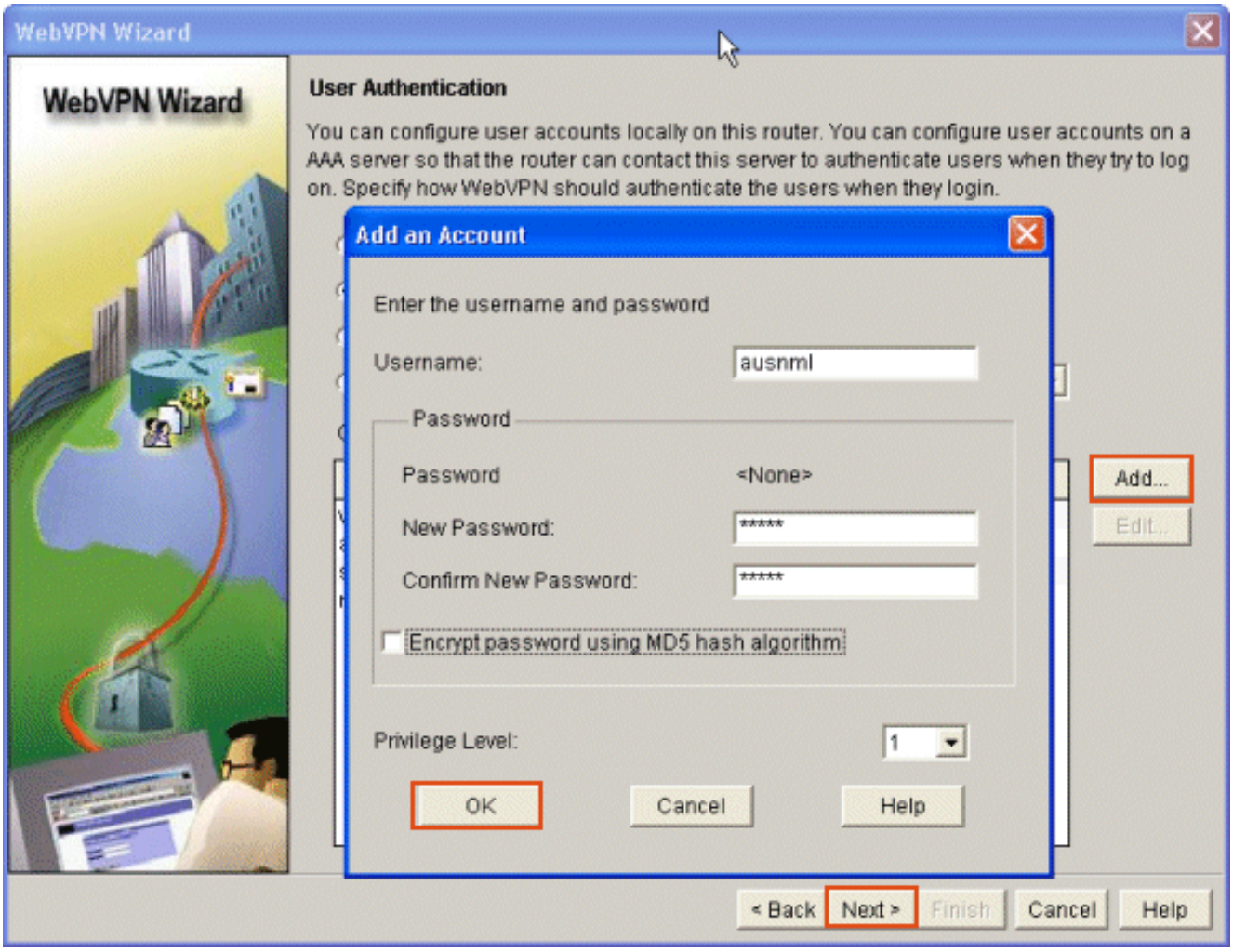
2. Der WebVPN-Assistent wird gestartet. Klicken Sie auf **Weiter**.



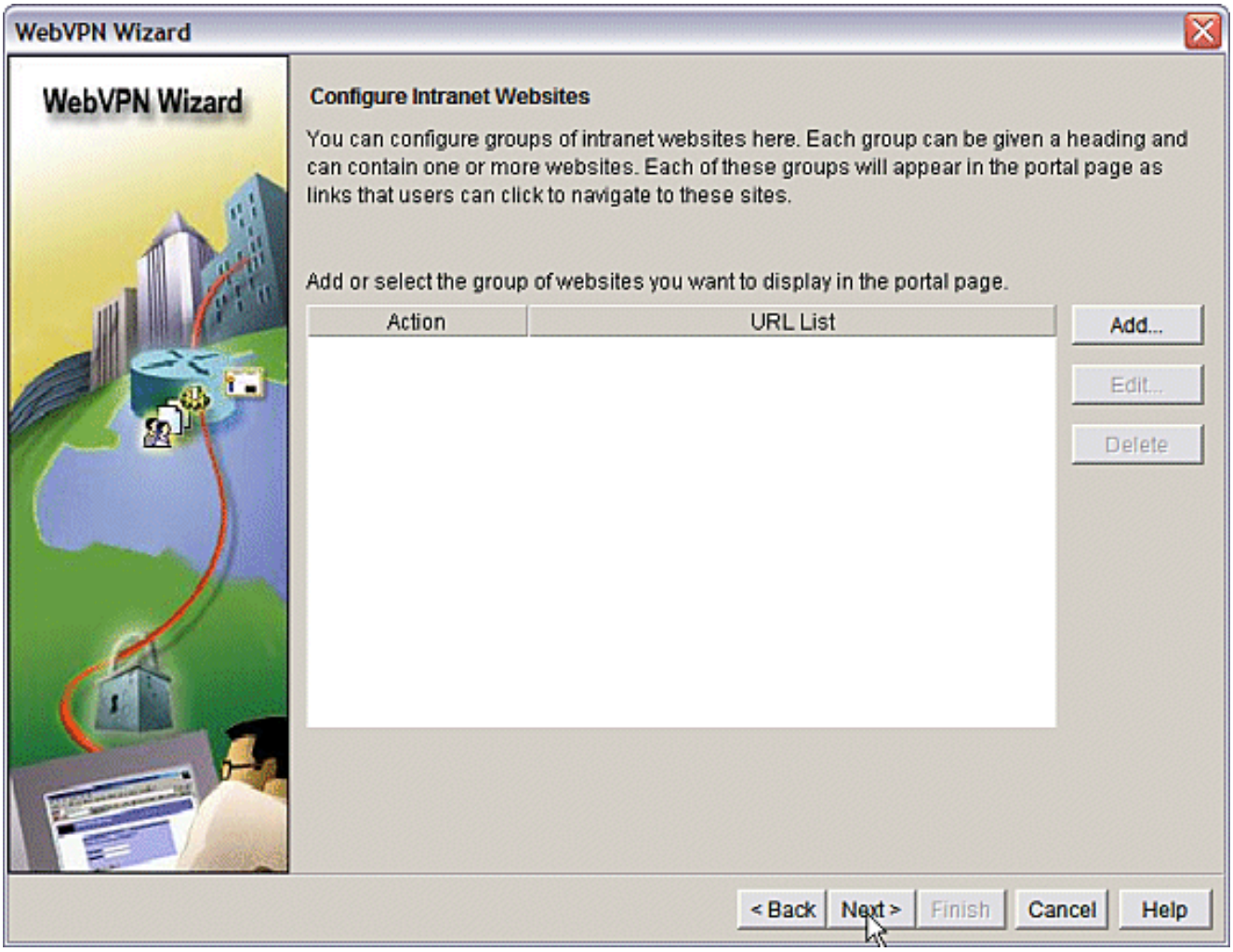
Geben Sie die IP-Adresse und einen eindeutigen Namen für dieses WebVPN-Gateway ein. Klicken Sie auf
Weiter.



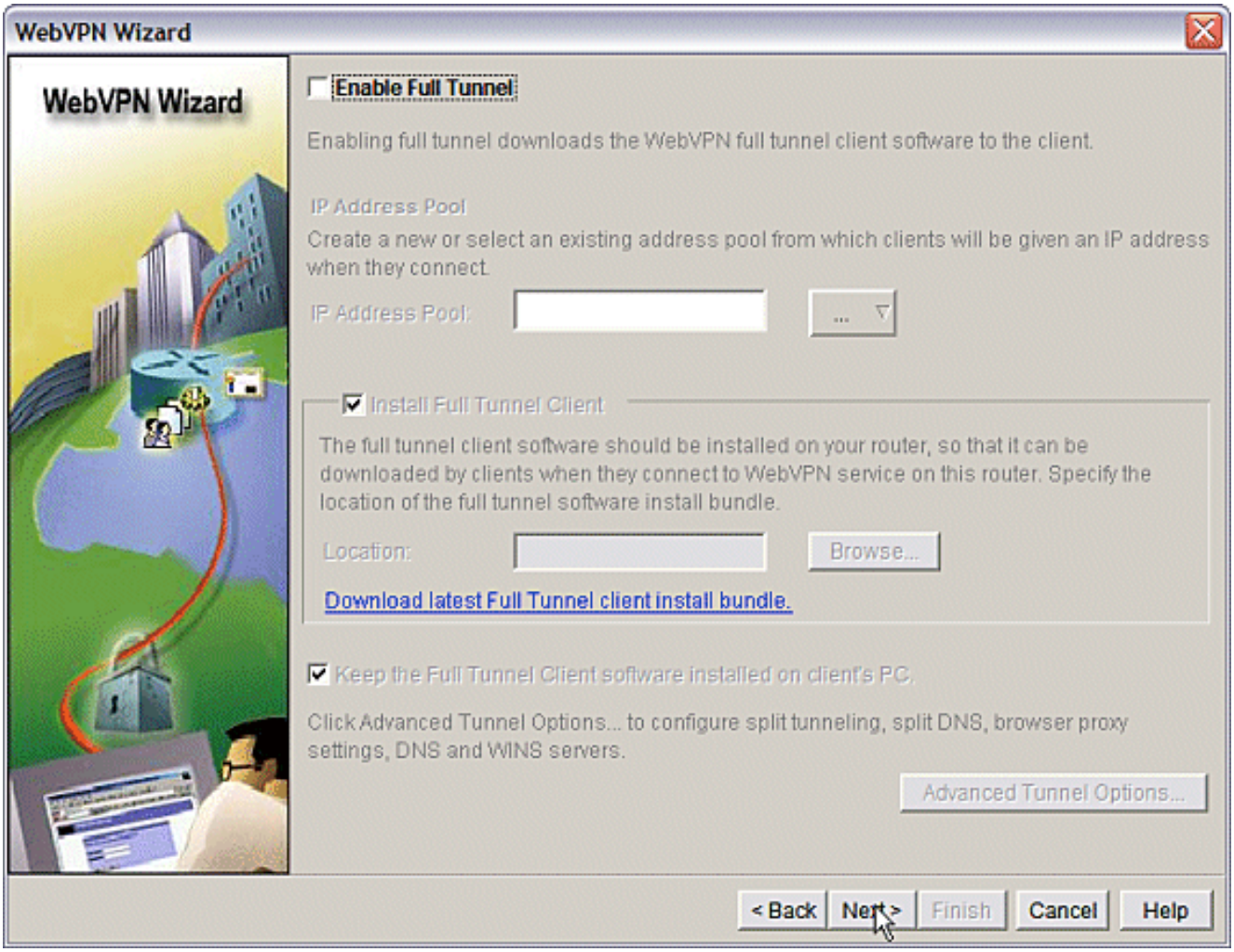
3. Der Bildschirm "User Authentication" ermöglicht die Bereitstellung der Authentifizierung von Benutzern. Bei dieser Konfiguration wird ein lokal auf dem Router erstelltes Konto verwendet. Sie können auch einen AAA-Server (Authentication, Authorization, and Accounting) verwenden.Zum Hinzufügen eines Benutzers klicken Sie auf **Hinzufügen**.Geben Sie die Benutzerinformationen auf dem Bildschirm Konto hinzufügen ein, und klicken Sie auf **OK**.Klicken Sie im Bildschirm "Benutzerauthentifizierung" auf **Weiter**.



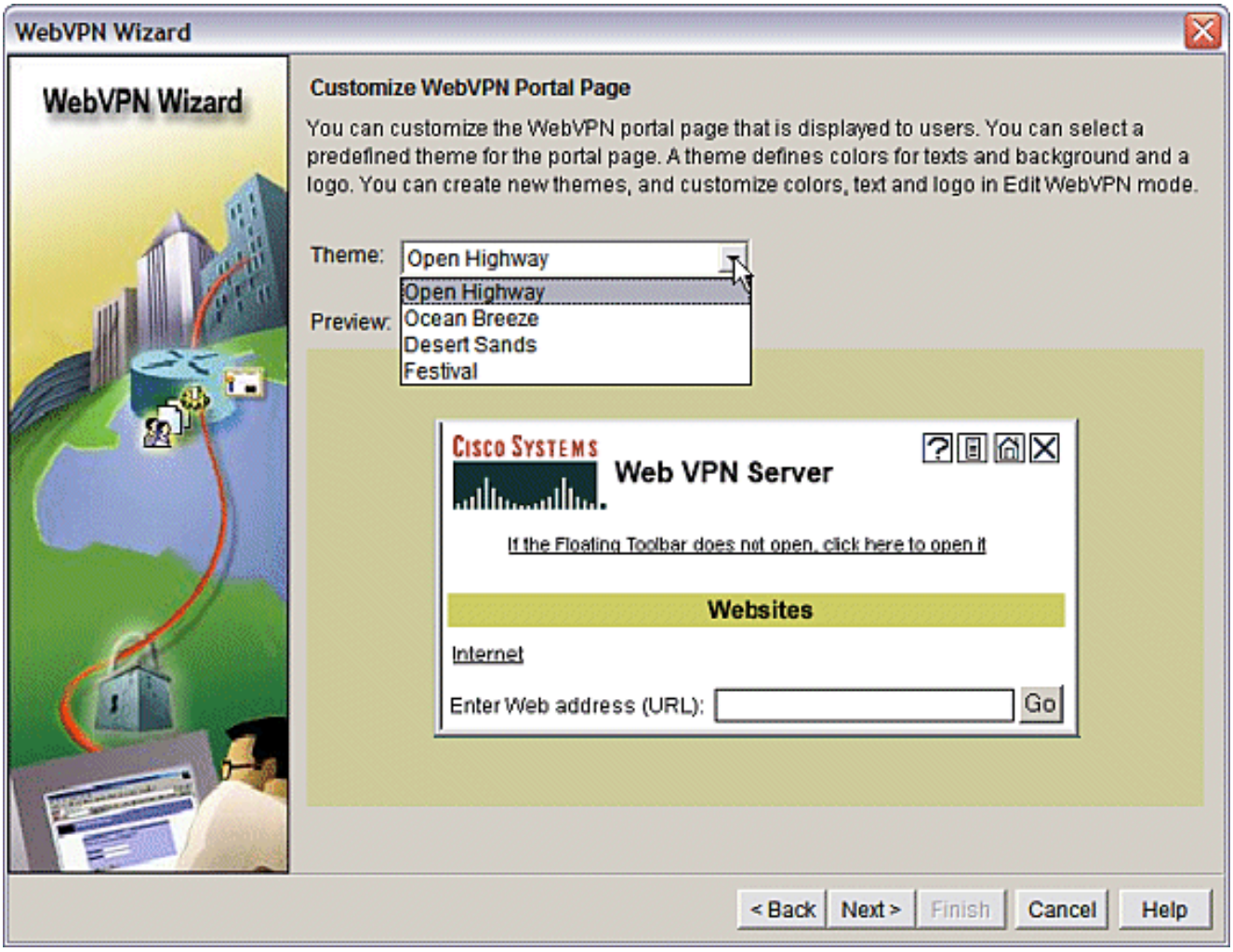
Der Bildschirm WebVPN Wizard (WebVPN-Assistent) ermöglicht die Konfiguration von Intranet-Websites. Dieser Schritt wird jedoch weggelassen, da für diesen Anwendungszugriff Port-Forwarding verwendet wird. Wenn Sie den Zugriff auf Websites zulassen möchten, verwenden Sie die Clientless- oder Full-Client-SSL-VPN-Konfigurationen, die nicht in den Anwendungsbereich dieses Dokuments
fallen.



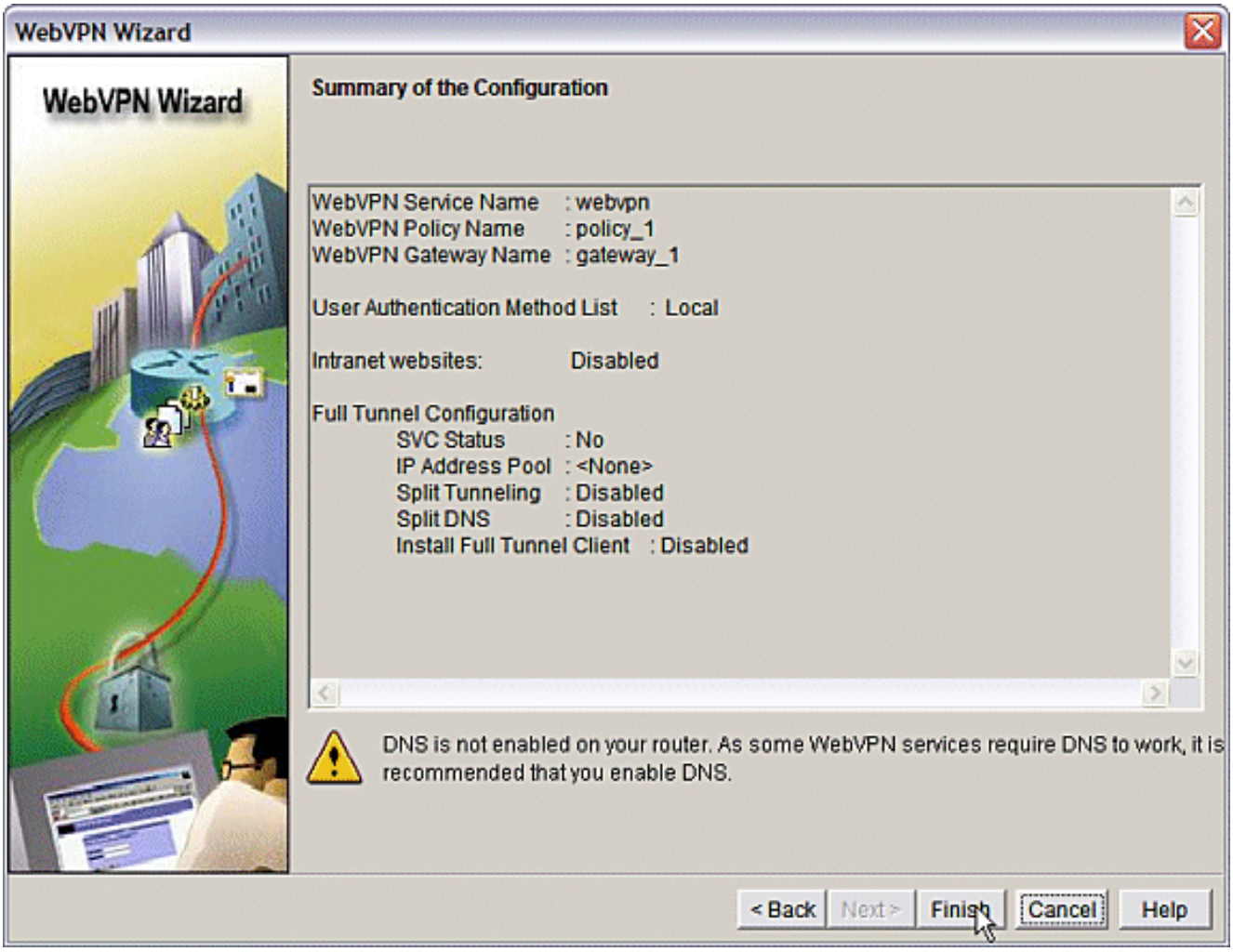
Klicken Sie auf **Weiter**. Der Assistent zeigt einen Bildschirm an, der die Konfiguration des Full Tunnel-Clients ermöglicht. Dies gilt nicht für das Thin-Client SSL VPN (Port Forwarding).Deaktivieren Sie **Vollständigen Tunnel aktivieren**. Klicken Sie auf **Weiter**.



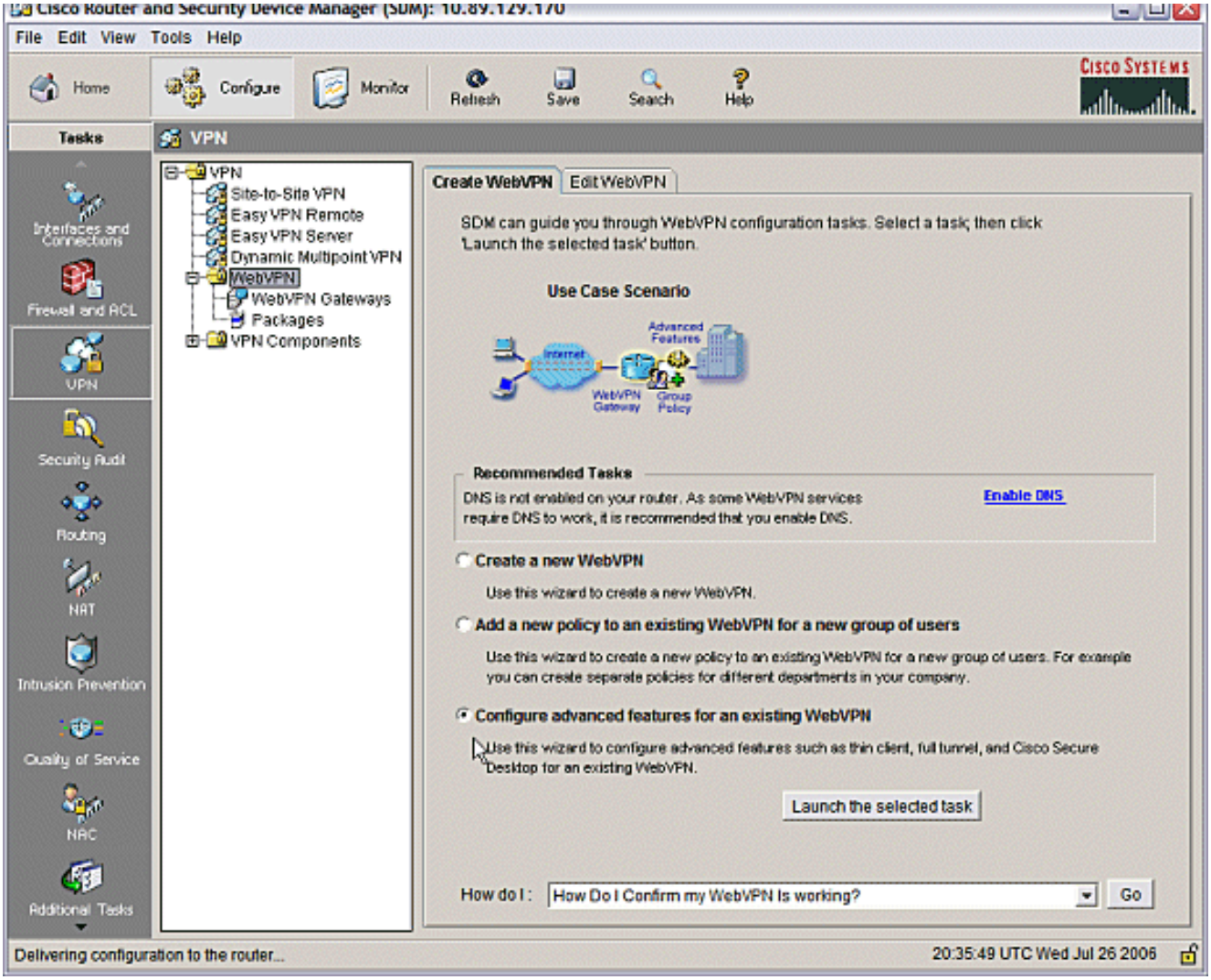
4. Passen Sie die Darstellung der WebVPN-Portalseite an, oder akzeptieren Sie die Standarddarstellung.Klicken Sie auf **Weiter**.



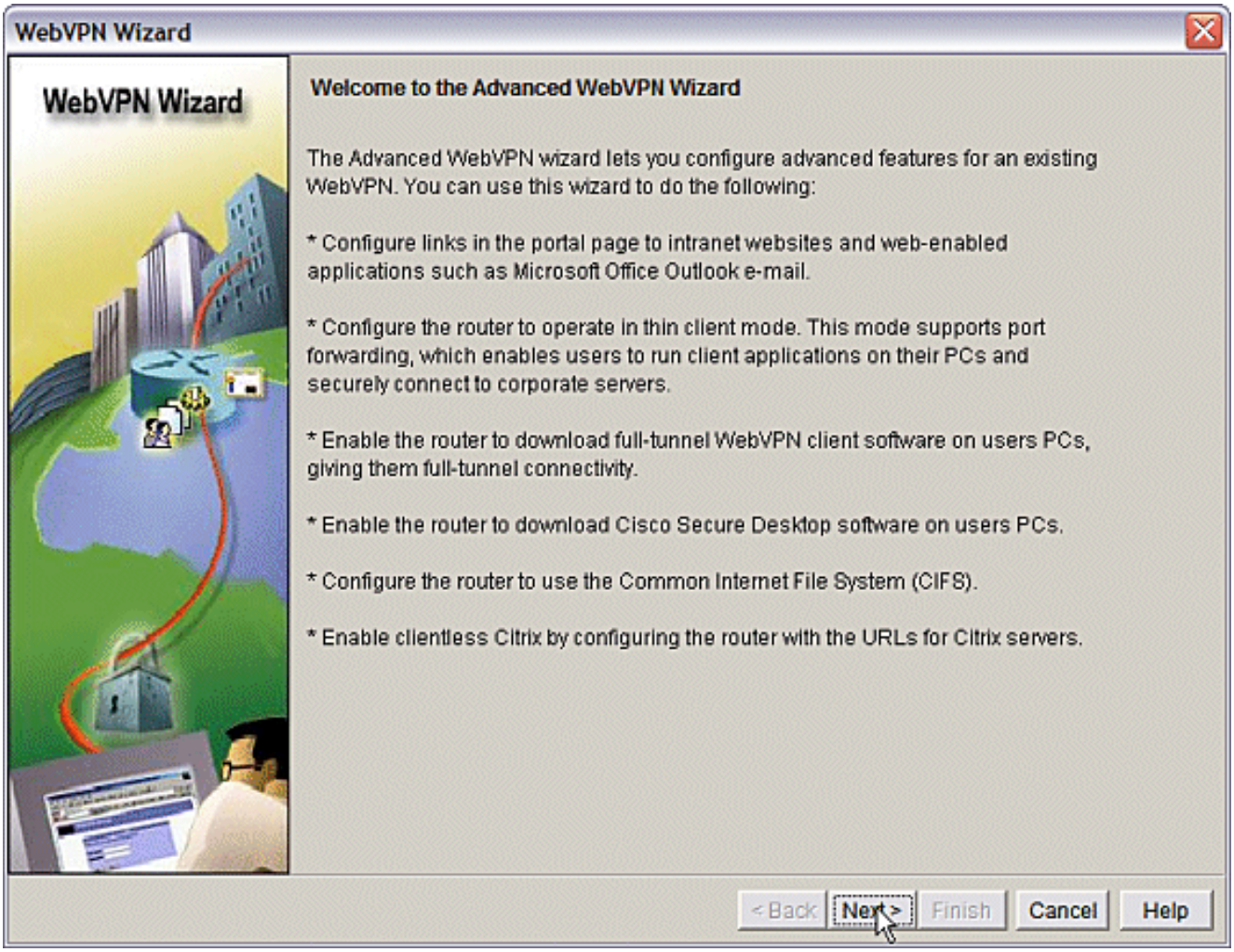
Zeigen Sie die Zusammenfassung der Konfiguration an, und klicken Sie auf **Fertig stellen > Speichern**.



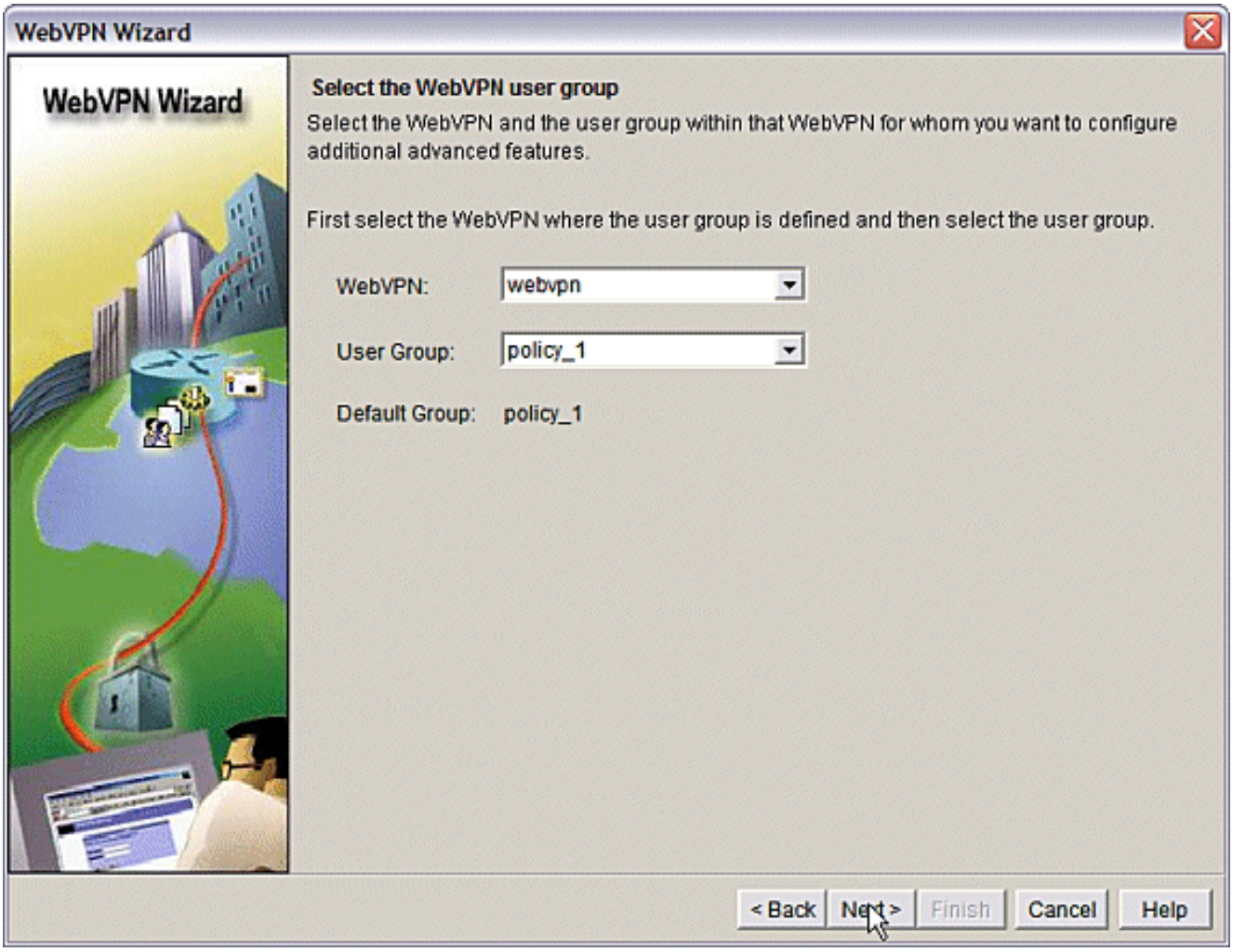
5. Sie haben ein WebVPN-Gateway und einen WebVPN-Kontext mit einer verknüpften Gruppenrichtlinie erstellt. Konfigurieren Sie die Thin-Client-Ports, die verfügbar sind, wenn Clients eine Verbindung zum WebVPN herstellen.Wählen Sie **Konfigurieren aus**.Wählen Sie **VPN > WebVPN aus**.Wählen Sie **WebVPN erstellen aus**.Aktivieren Sie das Optionsfeld **Erweiterte Funktionen für ein vorhandenes WebVPN konfigurieren** und klicken Sie auf **Ausgewählte Aufgabe starten**.



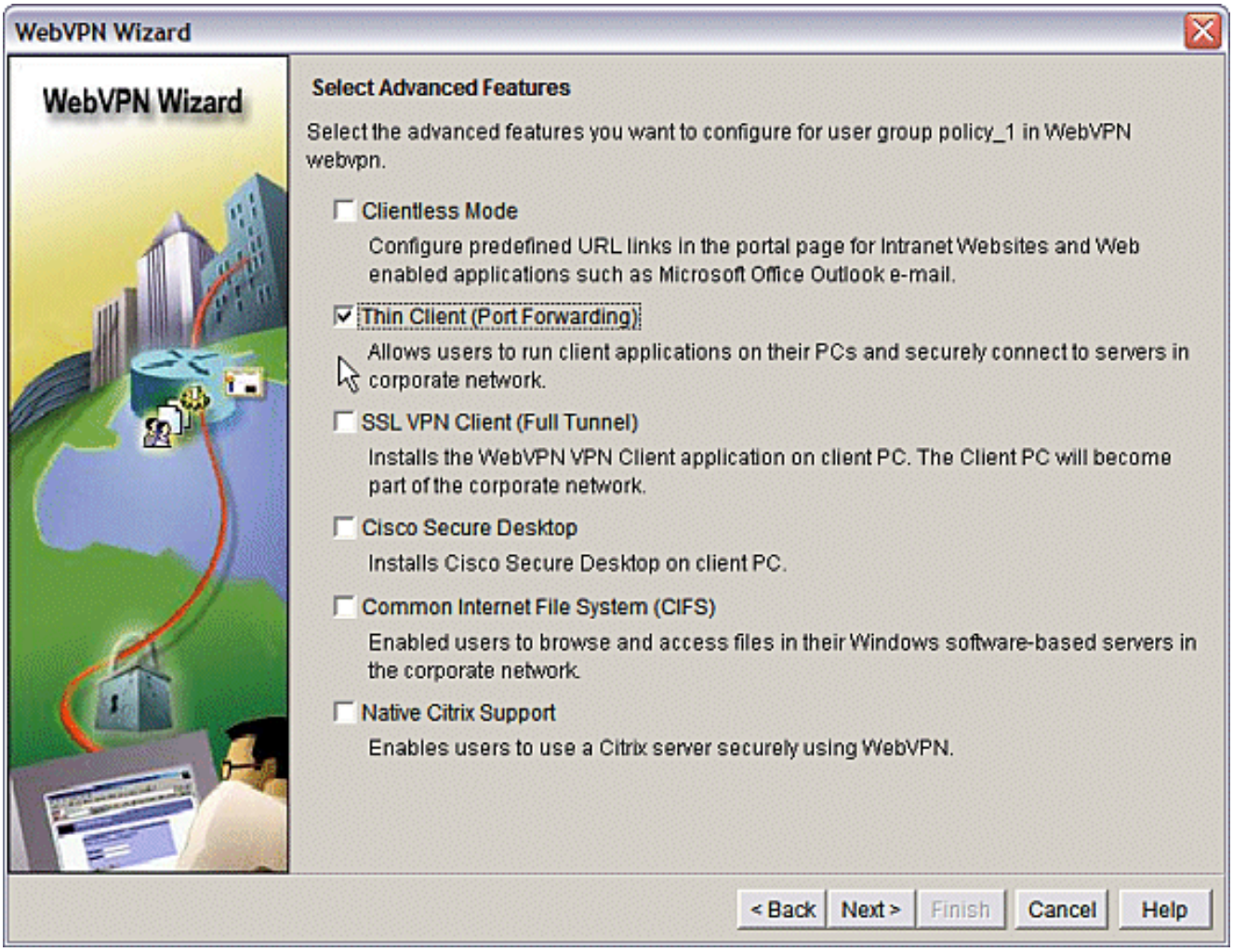
Der Willkommensbildschirm zeigt die Funktionen des Assistenten an. Klicken Sie auf **Weiter**.



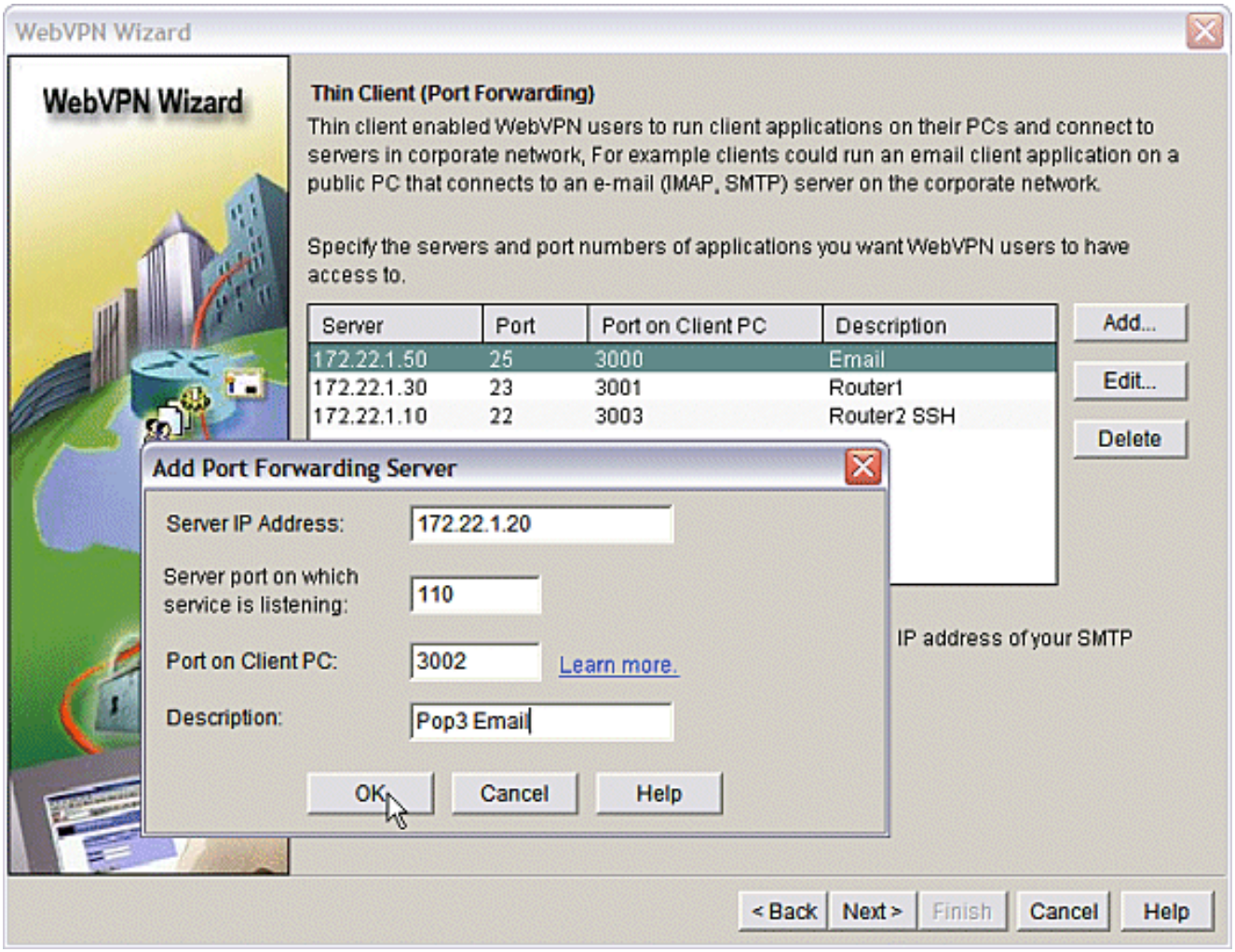
Wählen Sie den WebVPN-Kontext und die Benutzergruppe aus den Dropdown-Menüs aus. Klicken Sie auf
Weiter.



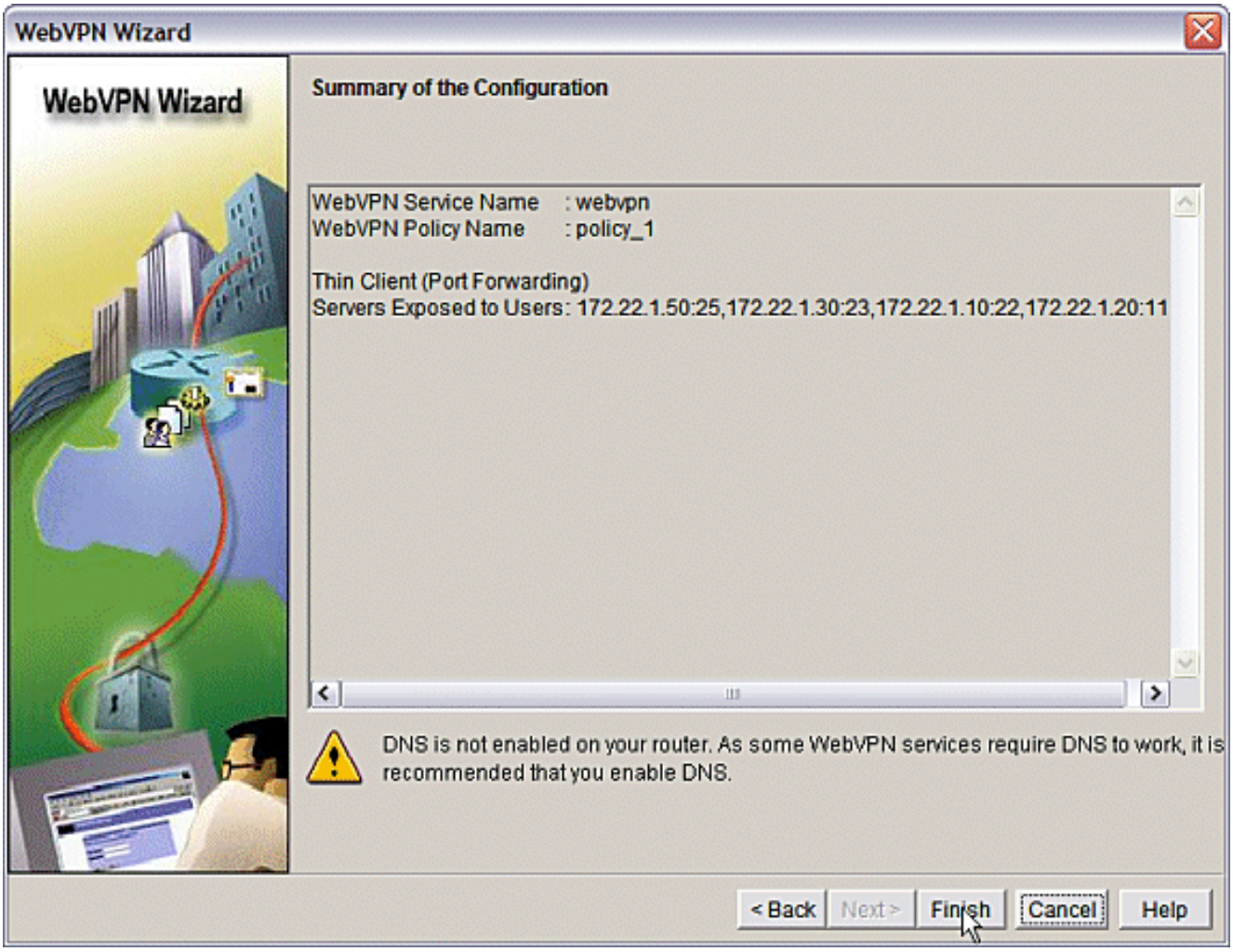
Wählen Sie **Thin Client (Port Forwarding)** und klicken Sie auf **Next (Weiter)**.



Geben Sie die Ressourcen ein, die Sie über Port Forwarding bereitstellen möchten. Beim Service-Port muss es sich um einen statischen Port handeln, Sie können jedoch den vom Assistenten zugewiesenen Standard-Port auf dem Client-PC akzeptieren. Klicken Sie auf **Weiter**.



Vorschau der Konfigurationsübersicht und klicken Sie auf **Fertig stellen > OK > Speichern**.



Konfiguration

Ergebnisse der SDM-Konfiguration.

ausml-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/
```

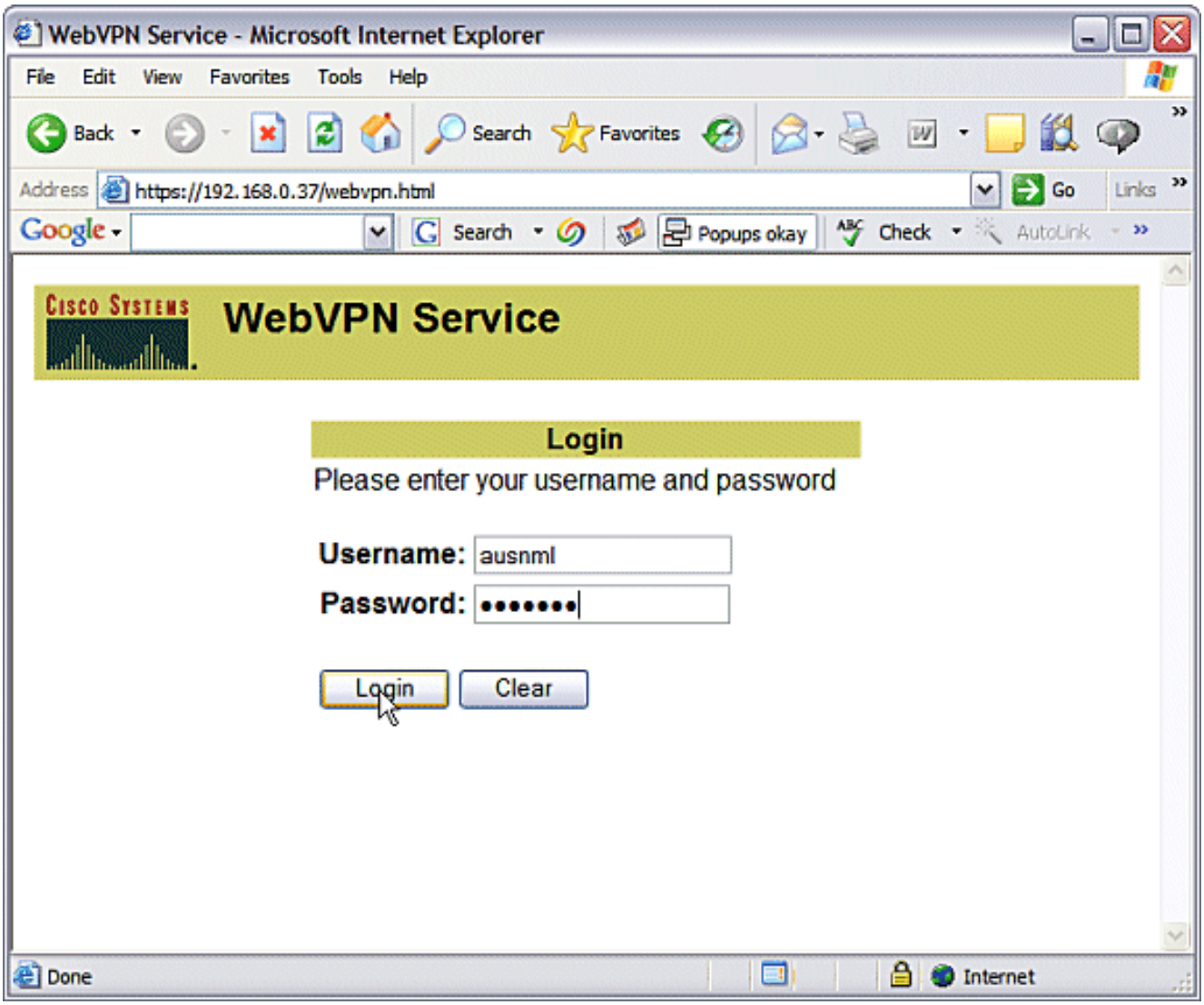
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- 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
```

Überprüfung

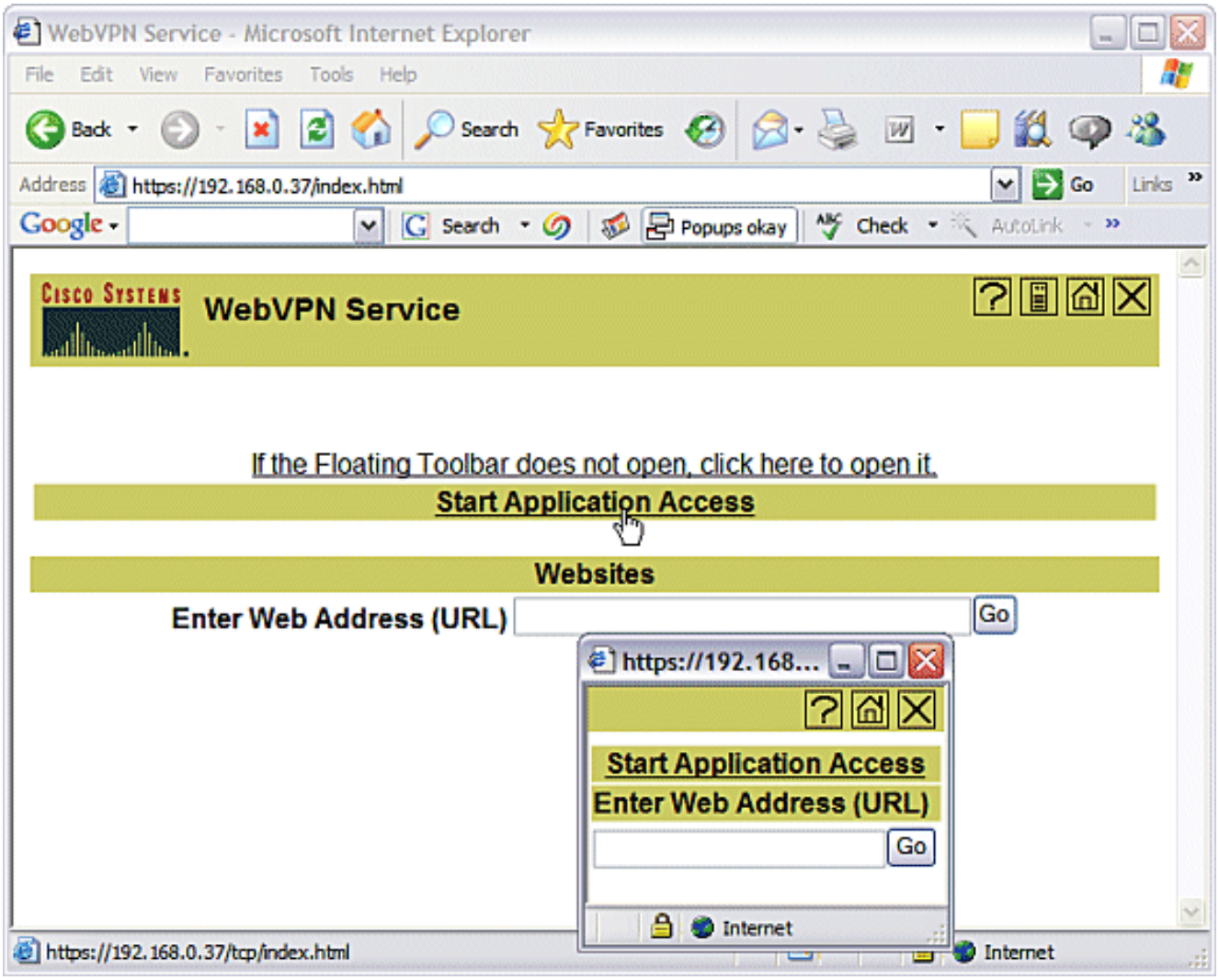
Überprüfen Sie Ihre Konfiguration

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

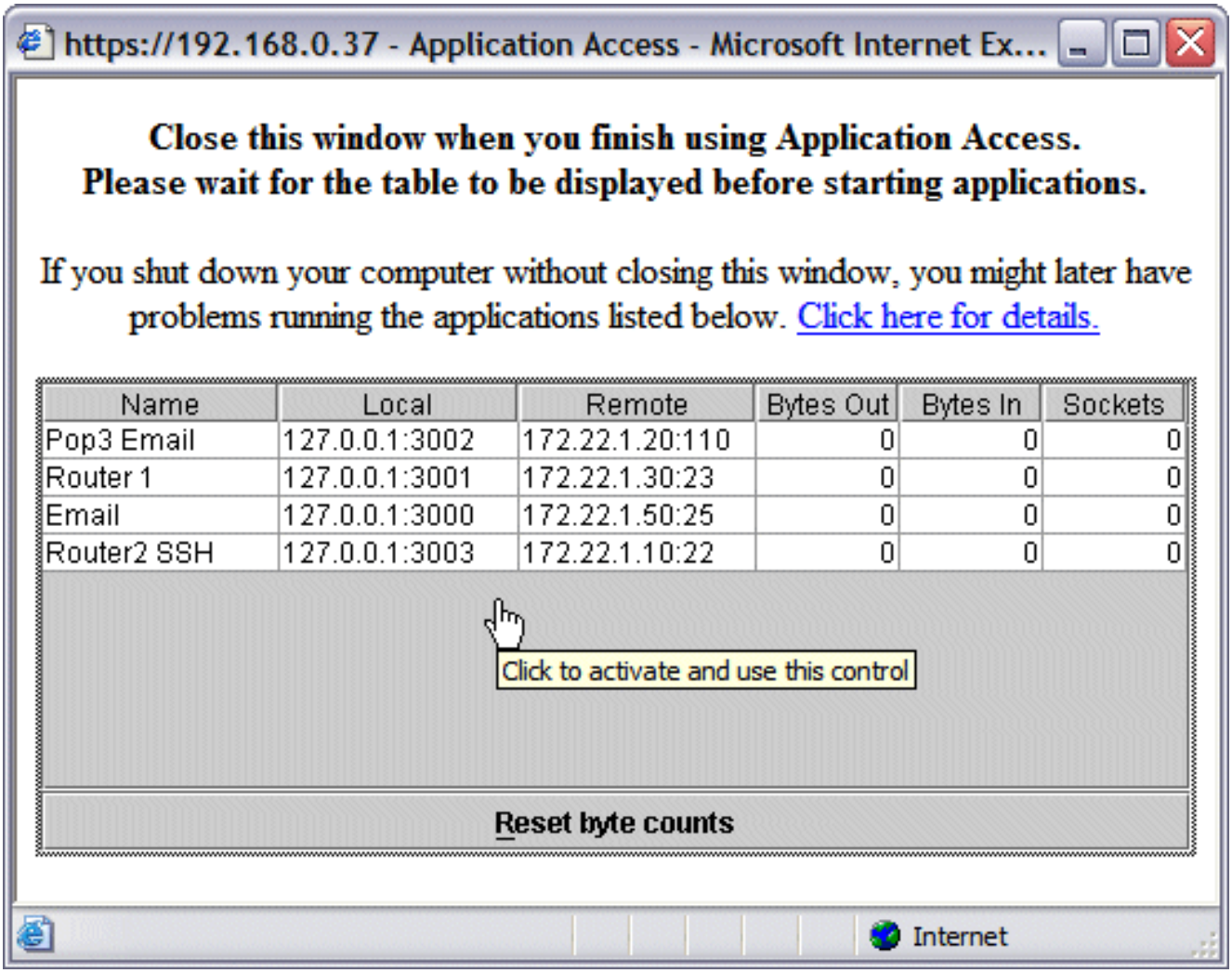
1. Verwenden Sie einen Client-Computer, um auf das WebVPN-Gateway unter **https://gateway_ip_address** zuzugreifen. Denken Sie daran, den WebVPN-Domänennamen einzuschließen, wenn Sie eindeutige WebVPN-Kontexte erstellen. Wenn Sie beispielsweise eine Domäne namens sales erstellt haben, geben Sie **https://gateway_ip_address/sales** ein.



2. Melden Sie sich an, und akzeptieren Sie das Zertifikat des WebVPN-Gateways. Klicken Sie auf **Anwendungszugriff starten**.



3. Es wird ein Bildschirm "Application Access" (Anwendungszugriff) angezeigt. Sie können auf eine Anwendung mit der lokalen Portnummer und der lokalen Loopback-IP-Adresse zugreifen. Geben Sie beispielsweise bei Telnet zu Router 1 **Telnet 127.0.0.1 3001 ein**. Das kleine Java-Applet sendet diese Informationen an das WebVPN-Gateway, das die beiden Enden der Sitzung sicher miteinander verknüpft. Erfolgreiche Verbindungen können dazu führen, dass die Spalten **Bytes Out** und **Bytes In** zunehmen.



Befehle

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

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.

Client-Computer müssen mit SUN Java Version 1.4 oder höher geladen werden. Eine Kopie dieser Software vom Java Software Download erhalten

Befehle zur Fehlerbehebung

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **show webvpn** - Es gibt viele **show**-Befehle, die mit WebVPN verknüpft sind. Diese können an

der CLI ausgeführt werden, um Statistiken und andere Informationen anzuzeigen. Weitere Informationen zur Verwendung von **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.
- **debug webvpn ?** - Die Verwendung von **Debug-**Befehlen kann den Router negativ beeinflussen. Weitere Informationen zur Verwendung von **Debugbefehlen** finden Sie unter Verwenden von WebVPN-Debug-Befehlen.

Zugehörige Informationen

- Cisco IOS SSL VPN
- SSL VPN - WebVPN
- Fragen und Antworten zu Cisco IOS WebVPN
- Technischer Support und Dokumentation für Cisco Systeme