# Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM

## Índice



## Introdução

O Cliente VPN com SSL (SVC) fornece um túnel completo para comunicações seguras à rede interna corporativa. Você pode configurar o acesso em um usuário pela base do usuário, ou você pode criar os contextos diferentes WebVPN em que você coloca uns ou vários usuários.

A tecnologia de VPN SSL ou WebVPN possui suporte nas seguintes plataformas do IOS Router:

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

Você pode configurar a tecnologia de VPN SSL nestes modos:

- **Sem clientes SSL VPN (WebVPN)** — Fornece um cliente remoto que exija um web browser SSL-permitido alcançar servidores de Web HTTP ou HTTPS em uma rede de área local (LAN) corporativa. Além, os sem clientes SSL VPN fornecem o acesso para o arquivo de

Windows que consulta com o protocolo do Common Internet File System (CIFS). O acesso à Web da probabilidade (OWA) é um acesso do exemplo de HTTP.Refira os sem clientes SSL VPN (WebVPN) no Cisco IOS com exemplo da configuração de SDM a fim aprender mais sobre os sem clientes SSL VPN.

- **O thin client SSL VPN (transmissão da porta)** — fornece um cliente remoto que transfira um applet com base em Java pequeno e permite o acesso seguro para os aplicativos do Transmission Control Protocol (TCP) que usam números de porta estática. O Point of Presence (POP3), o Simple Mail Transfer Protocol (SMTP), o Internet Message Access Protocol (IMAP), o Shell Seguro (ssh), e o telnet são exemplos do acesso seguro. Porque os arquivos na máquina local mudam, os usuários devem ter privilégios administrativos locais usar este método. Este método de SSL VPN não trabalha com aplicativos que usam atribuições de porta dinâmica, tais como alguns aplicativos do File Transfer Protocol (FTP).Consulte o Exemplo de Configuração do IOS da VPN SSL Thin-Client (WebVPN) com SDM para obter mais informações sobre a VPN SSL thin-client.**Nota:** O User Datagram Protocol (UDP) não é apoiado.
- **Cliente VPN SSL (modo de túnel completo SVC)** — transfere um cliente pequeno à estação de trabalho remota e permite o acesso seguro completo aos recursos em uma rede corporativa interna. Você pode transferir o SVC a uma estação de trabalho remota permanentemente, ou você pode remover o cliente uma vez que a sessão segura é fechada.

Este original demonstra a configuração de um roteador do Cisco IOS para o uso de um cliente VPN SSL.

# Pré-requisitos

## Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Microsoft Windows 2000 ou XP
- Navegador da Web com SUN JRE 1.4 ou posterior ou um navegador controlado por ActiveX
- Privilégios administrativos locais no cliente
- Um do Roteadores alistado na introdução com uma imagem da segurança avançada (12.4(6)T ou mais tarde)
- Versão 2.3 do gerenciador do dispositivo de segurança da Cisco (SDM)Se o Cisco SDM já não estiver carregado em seu roteador, você poderá obter uma cópia gratuita do software de Download de Software (somente clientes registrados). Você deve possuir uma conta CCO com um contrato de serviço. Para obter informações detalhadas sobre a instalação e a configuração do SDM, consulte Cisco Router and Security Device Manager.
- Um certificado digital no roteadorVocê pode usar um certificado auto-assinado persistente ou um Certificate Authority (CA) externo para satisfazer esta exigência. Para obter mais informações sobre dos certificados auto-assinados persistentes, refira certificados auto-assinados persistentes.

## Componentes Utilizados

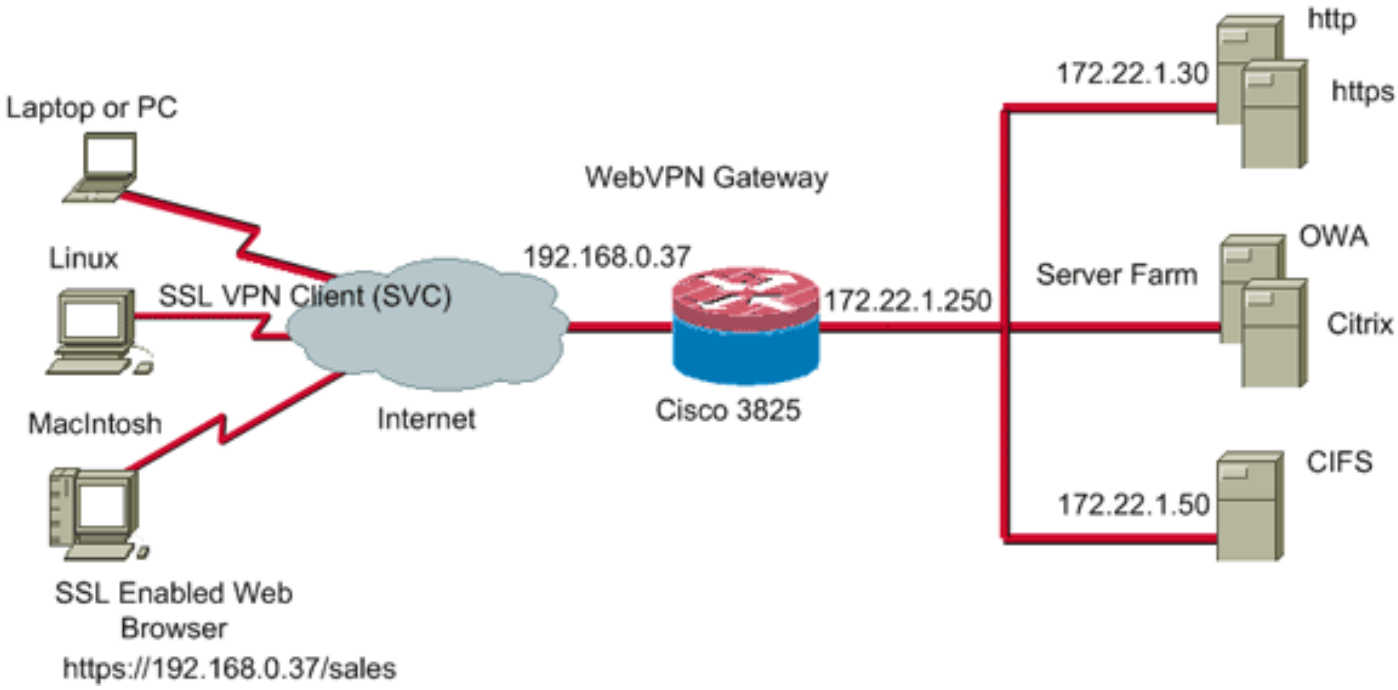
As informações neste documento são baseadas nestas versões de software e hardware:

- 3825 Series do roteador do Cisco IOS com 12.4(9)T
- Versão 2.3.1 do Security Device Manager (SDM)

**Nota:** As informações apresentadas neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Tarefas de Pré-configuração

1. Configure o roteador para SDM. (Opcional)O Roteadores com a licença apropriada do pacote da Segurança já tem o aplicativo SDM carregado no flash. Refira a transferência e a instalação de Roteador Cisco e Security Device Manager (SDM) para obter e configurar o software.
2. Transfira uma cópia do SVC a seu PC do Gerenciamento.Você pode obter uma cópia do arquivo de pacote SVC do download do software: Cisco SSL VPN Client (clientes registrados somente). Você deve ter uma conta válida CCO com um contrato de serviço.
3. Ajuste a data, a hora, e a zona de hora (fuso horário) corretas, e configurar então um certificado digital no roteador.

## Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

# Informações de Apoio

O SVC é carregado inicialmente no gateway router WebVPN. Cada vez que o cliente conecta, uma cópia do SVC está transferida dinamicamente no PC. A fim mudar este comportamento, configurar o roteador para permitir o software de permanecer permanentemente no computador de cliente.

# Configurar o SVC em IO

Nesta seção, você será apresentado aos passos necessários para configurar os recursos descritos neste documento. Este exemplo de configuração usa o assistente SDM para permitir a operação do SVC no IOS Router.

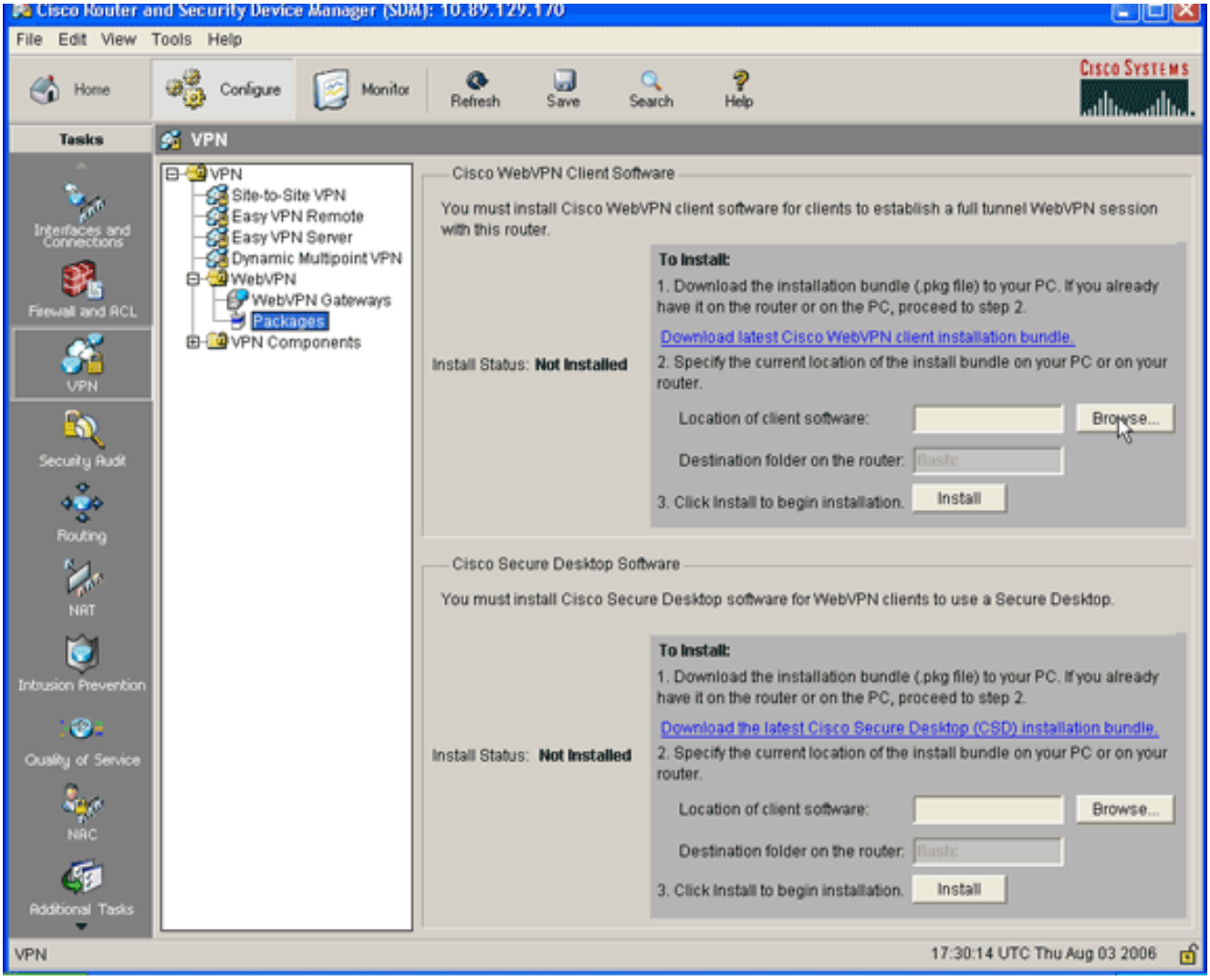
Termine estas etapas a fim configurar o SVC no IOS Router:

1. Instale e permita o software SVC no IOS Router
2. Configurar um contexto WebVPN e o gateway WebVPN com o assistente SDM
3. Configurar a base de dados de usuário para usuários SVC
4. Configurar os recursos para expor aos usuários

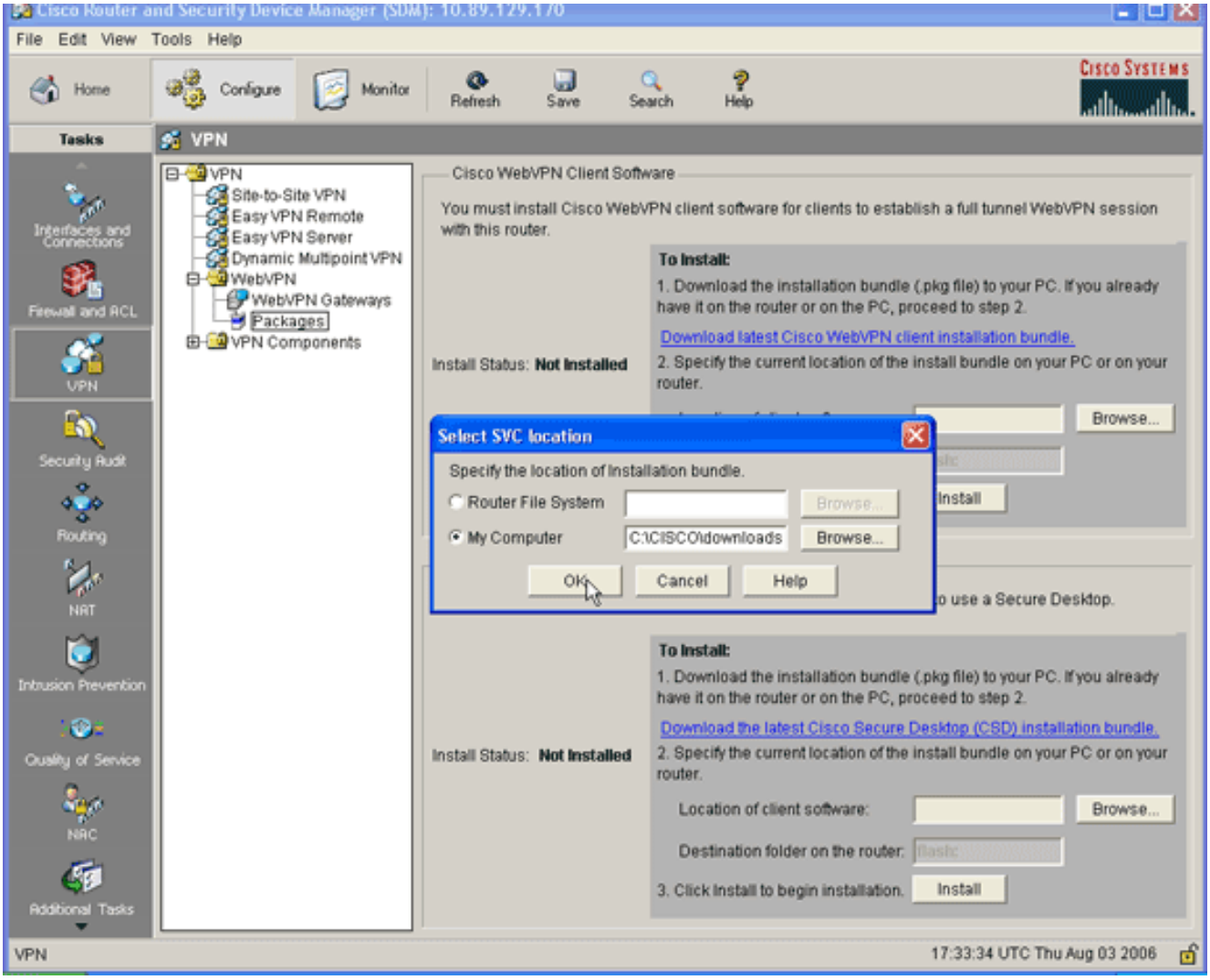
## Etapa 1. Instale e permita o software SVC no IOS Router

Termine estas etapas a fim instalar e permitir o software SVC no IOS Router:

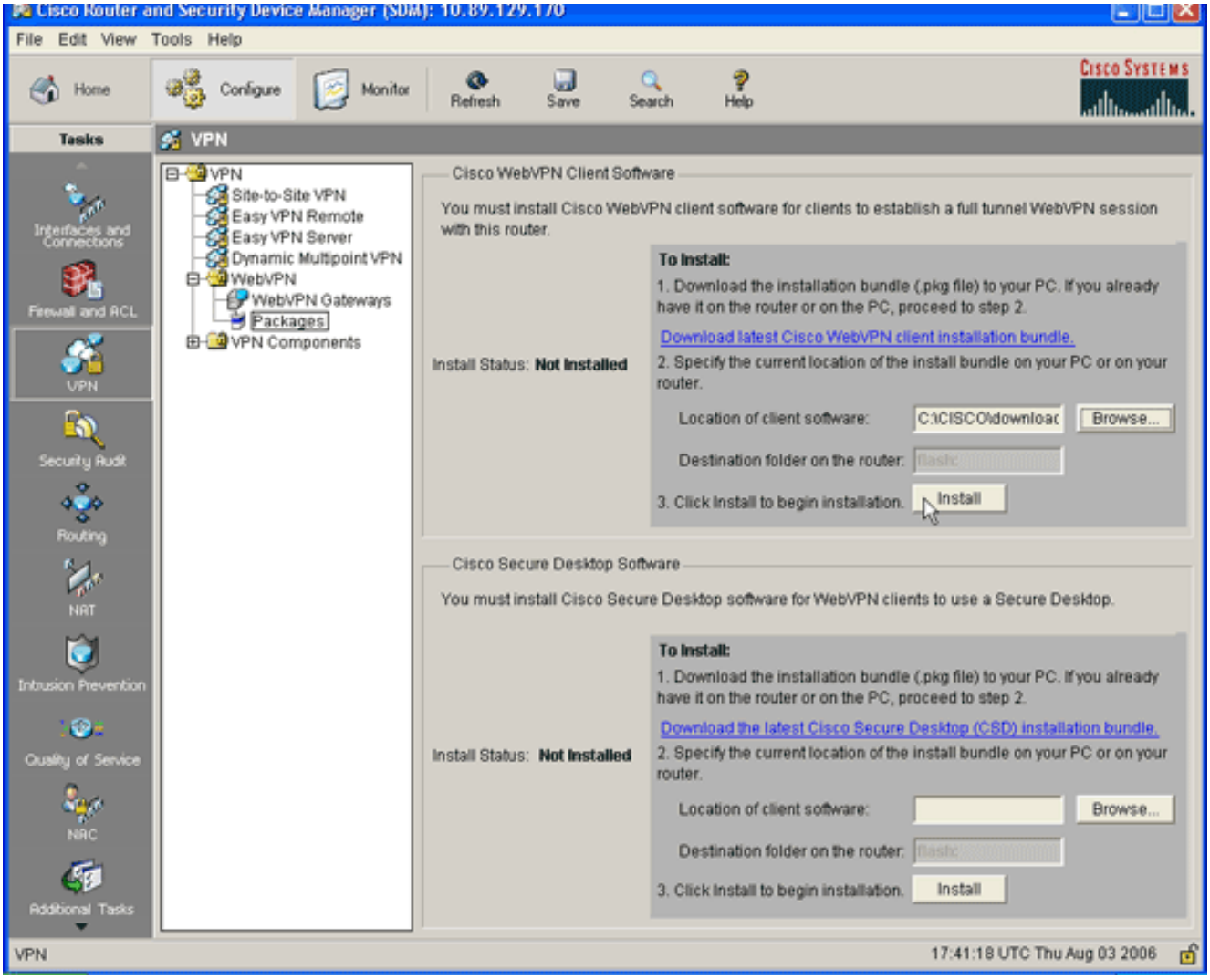
1. Abra o aplicativo SDM, o clique **configura**, e clica então o **VPN**.
2. Expanda o **WebVPN**, e escolha
   **pacotes**.



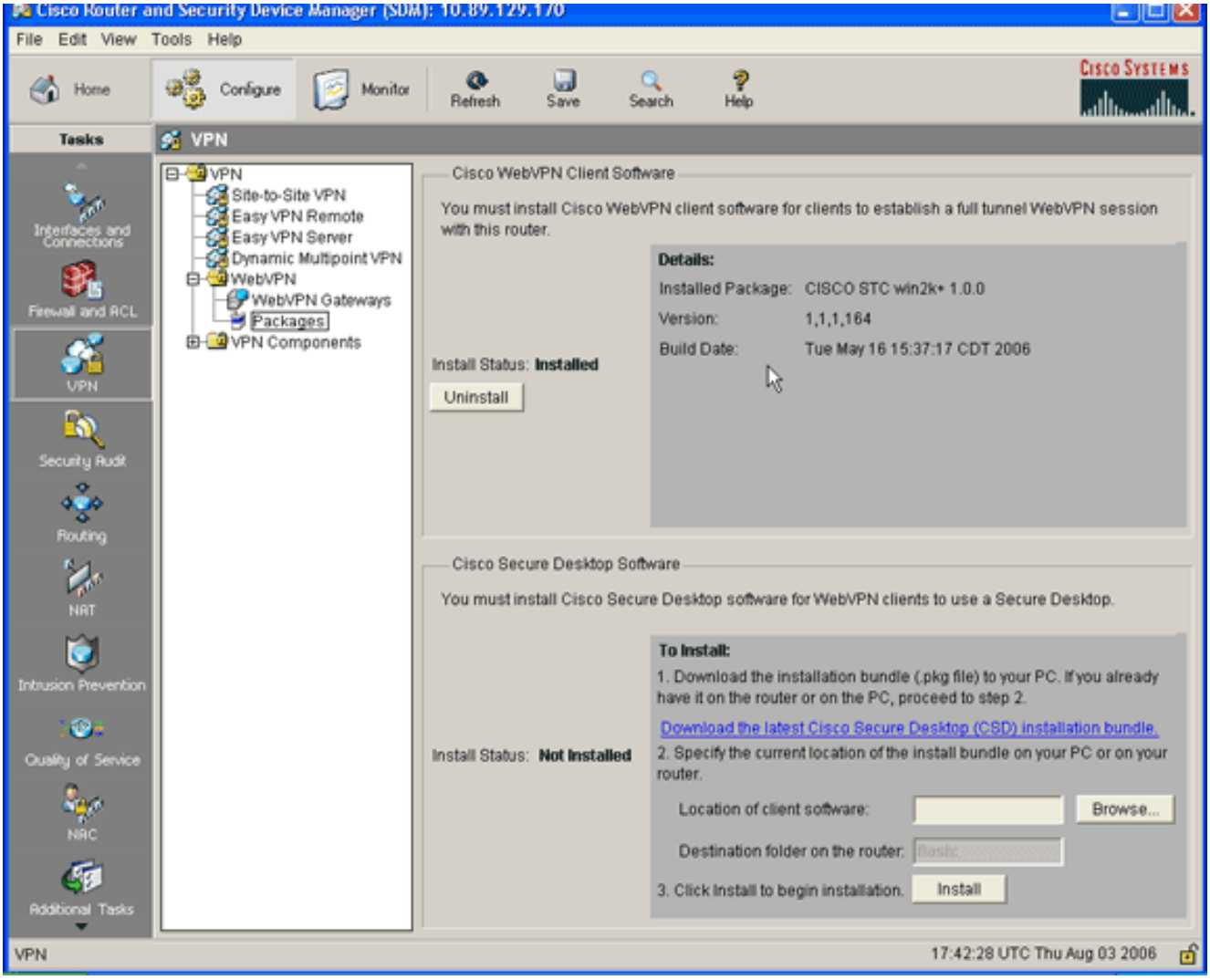

3. Dentro da área do software do cliente de Cisco WebVPN, clique o **botão Browse**.A caixa de diálogo seleta do lugar SVC
aparece.




4. Clique o botão de rádio do **meu computador**, e clique-o então **consultam** para encontrar o pacote SVC em seu PC do Gerenciamento.
5. Clique a **APROVAÇÃO**, e clique então o **botão Install Button**.



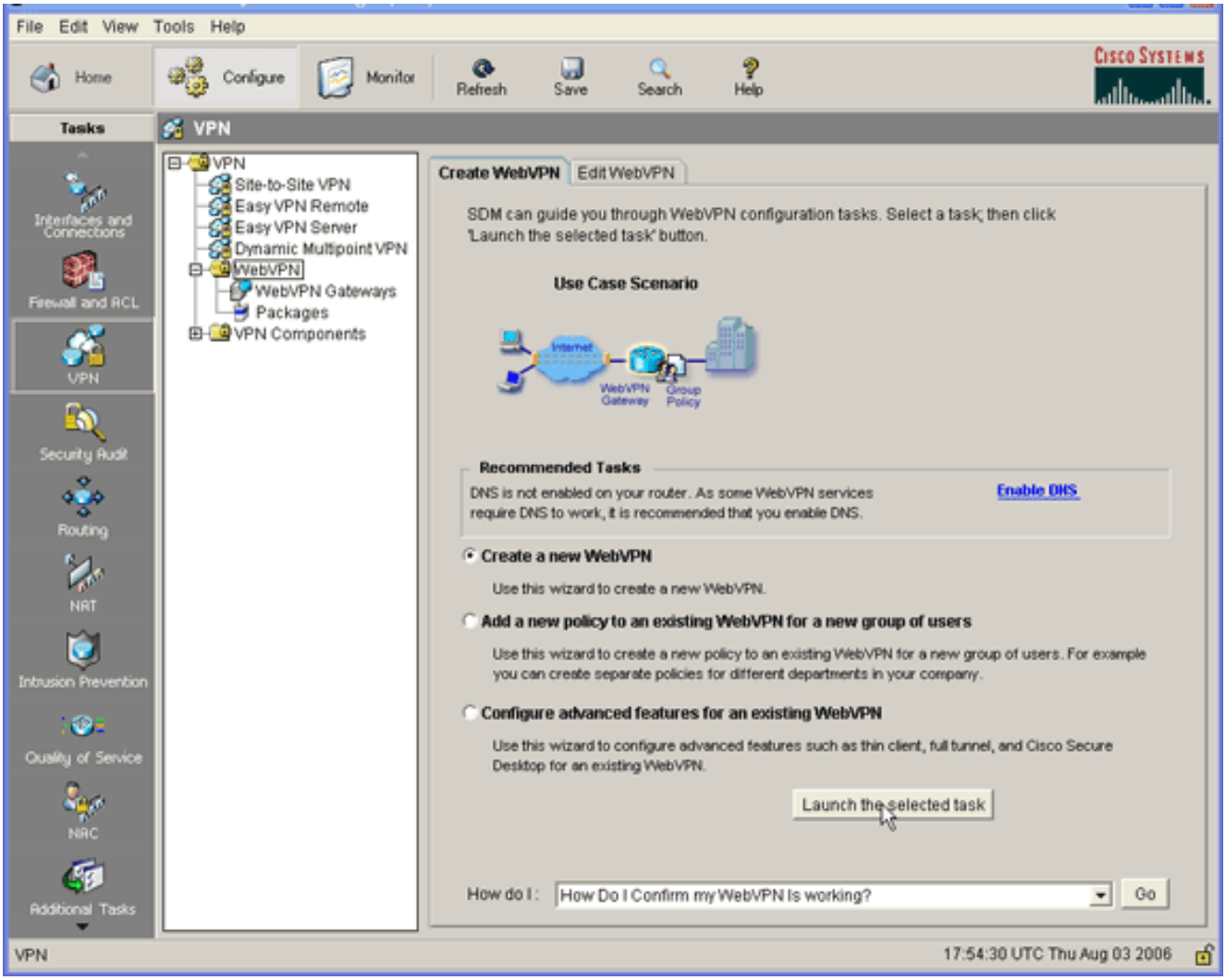

6. Clique em **Yes** e, em seguida, em **OK**.Um bem sucedido instala do pacote SVC é mostrado nesta
imagem:



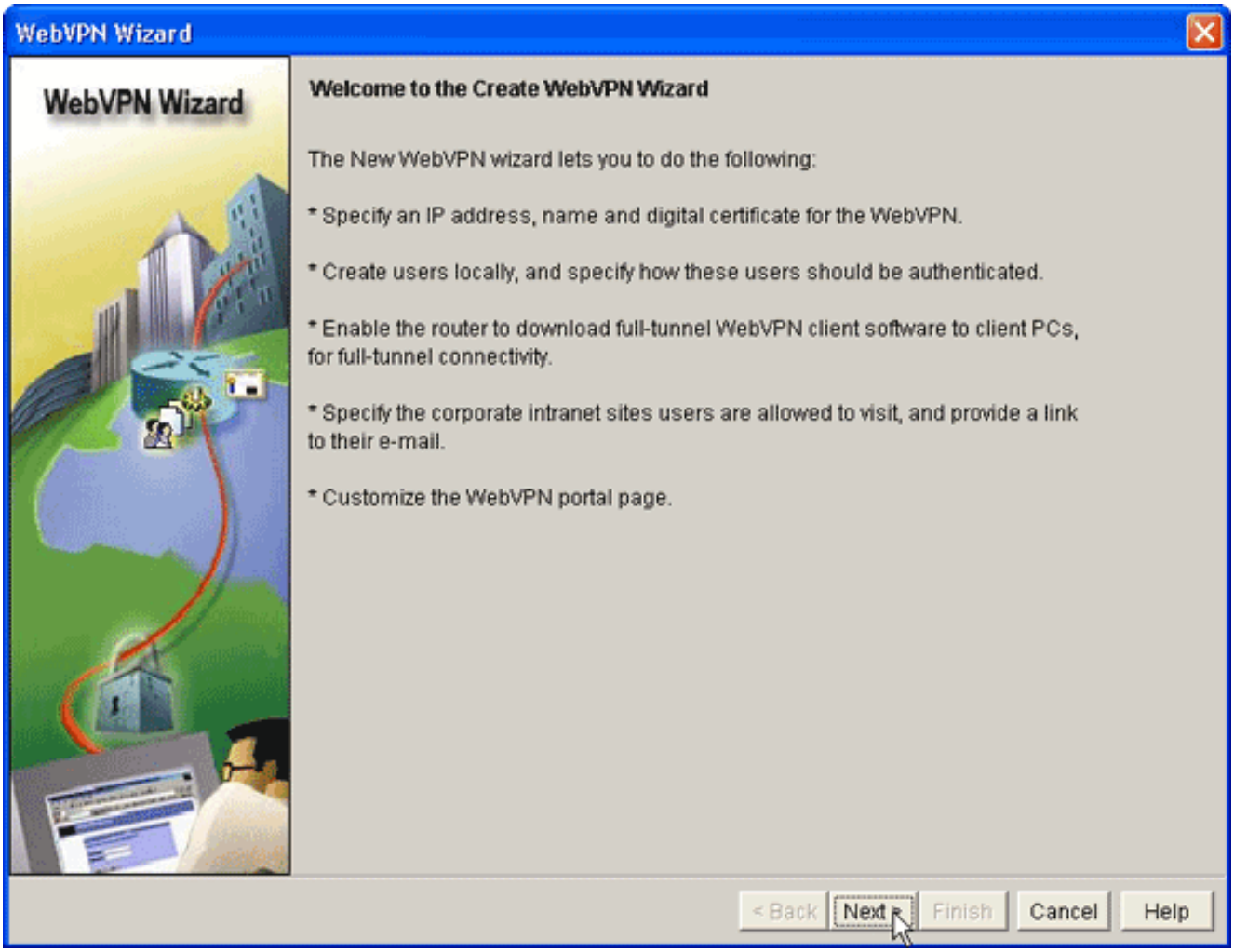

## Etapa 2. Configurar um contexto WebVPN e o gateway WebVPN com o assistente SDM

Termine estas etapas a fim configurar um contexto WebVPN e o gateway WebVPN:

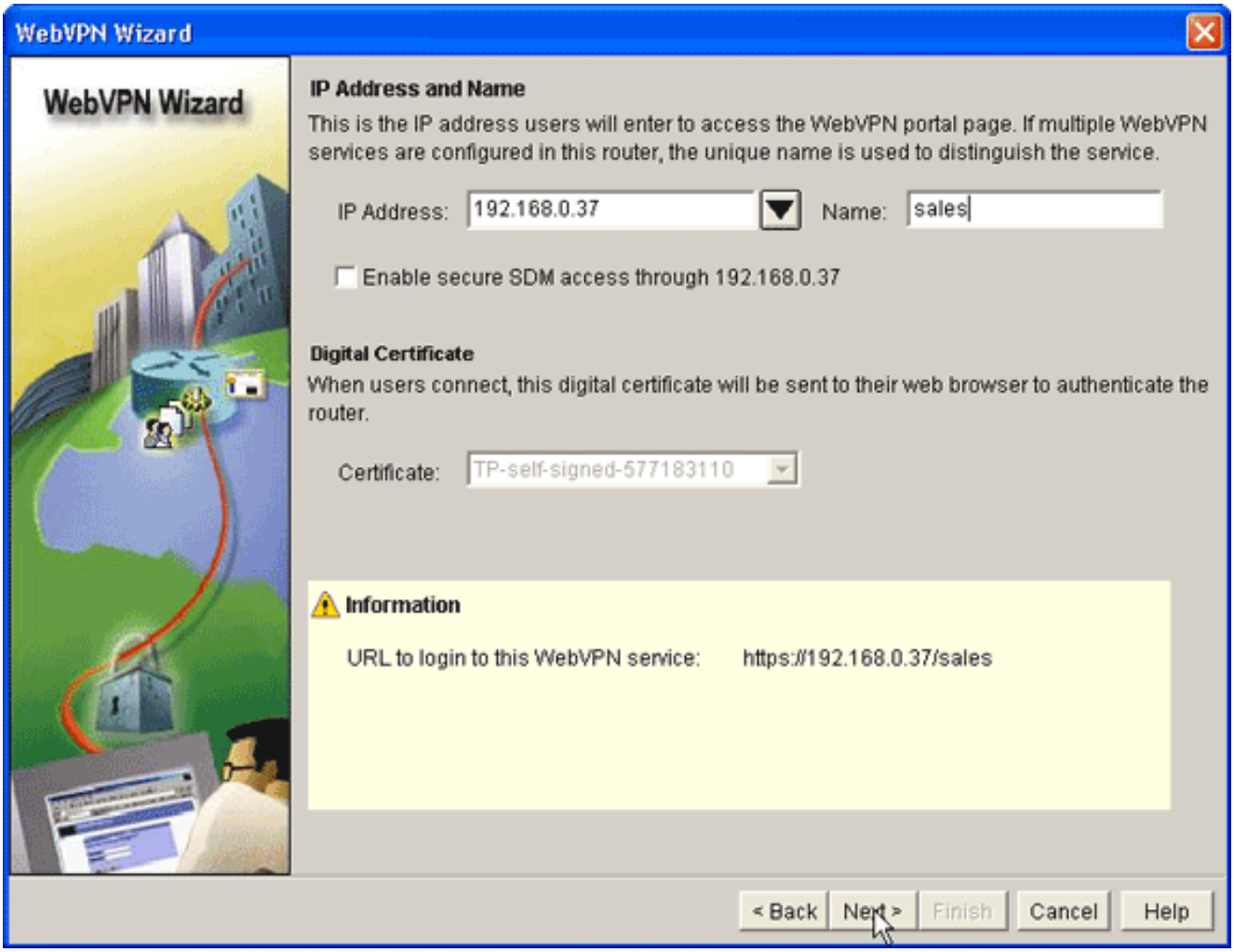
1. Depois que o SVC é instalado no roteador, o clique **configura**, e clica então o **VPN**.
2. Clique o **WebVPN**, e clique a aba da **criação WebVPN**.




3. Verifique a **criação um** botão de rádio **novo WebVPN**, e clique então o **lançamento a tarefa selecionada**.A caixa de diálogo do assistente WebVPN aparece.




4. Clique em Next.



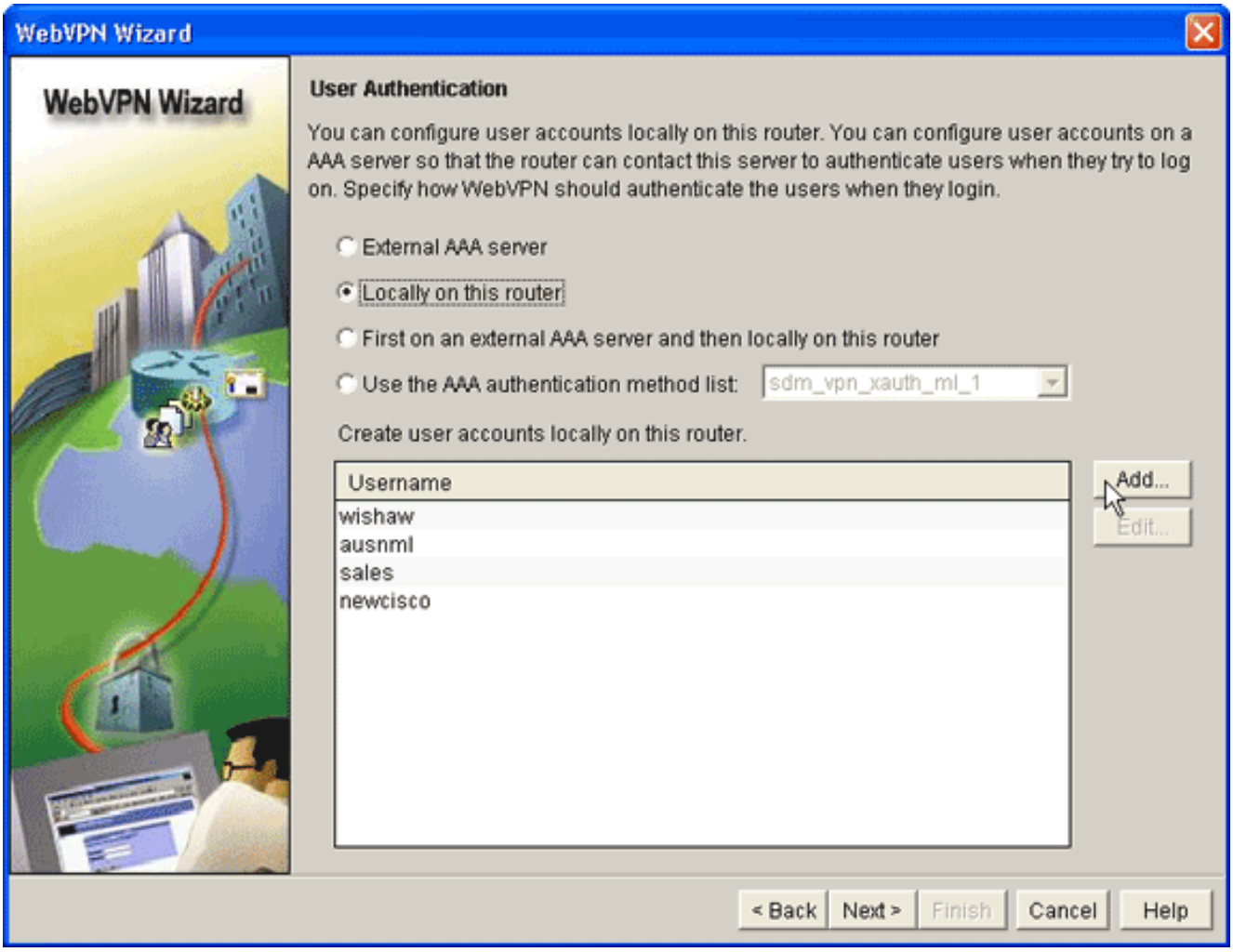

5. Incorpore o IP address do gateway novo WebVPN, e dê entrada com um nome exclusivo para este contexto WebVPN.Você pode criar contextos diferentes WebVPN para o mesmo IP address (gateway WebVPN), mas cada nome deve ser original. Este exemplo usa este endereço IP: *https://192.168.0.37/sales*
6. Clique em **Next** e prossiga para o Passo 3.

## Etapa 3. Configurar a base de dados de usuário para usuários SVC

Para autenticação, você pode utilizar um servidor AAA, usuários locais ou ambos. Este exemplo de configuração usa usuários criados localmente para a autenticação.

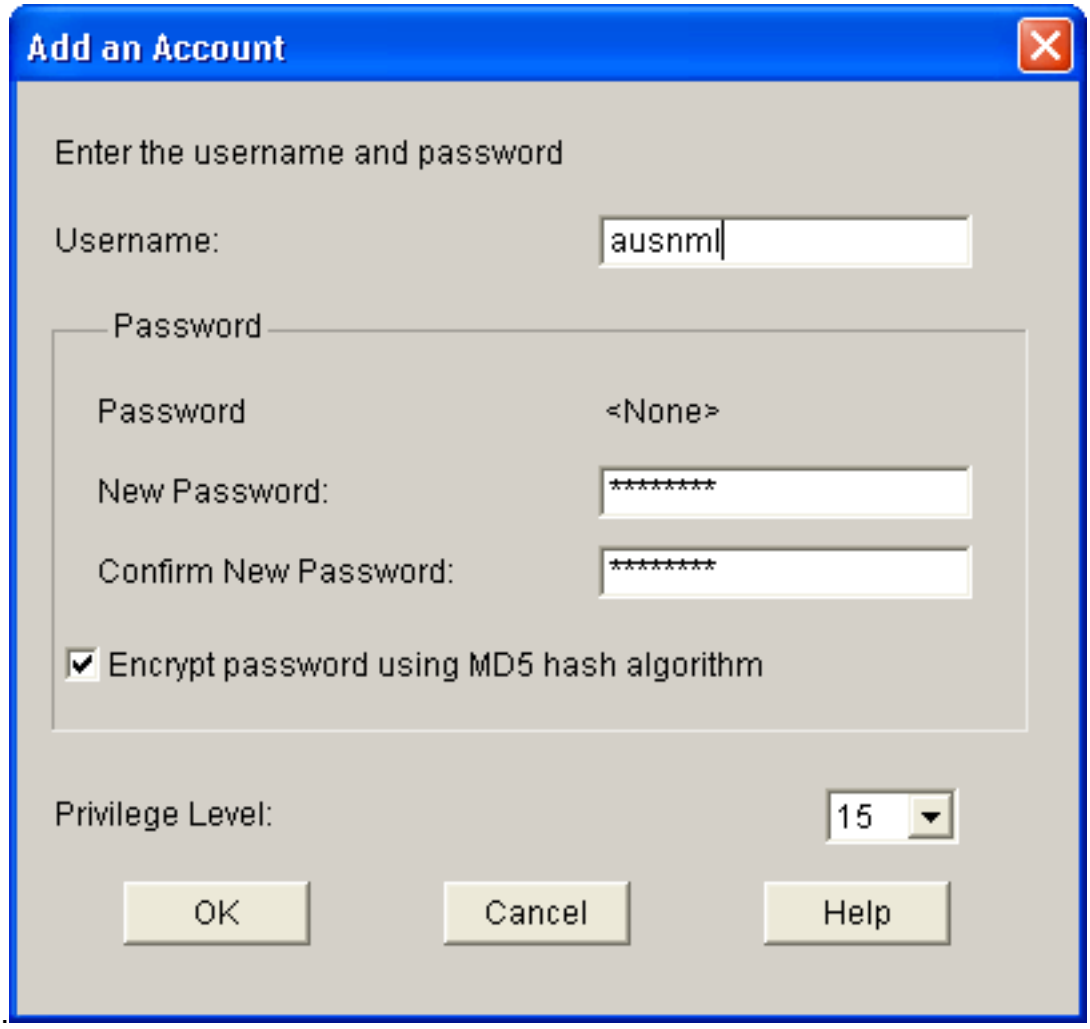
Termine estas etapas a fim configurar a base de dados de usuário para usuários SVC:

1. Depois que você termina etapa 2, clique **localmente sobre este** botão de rádio do **roteador** situado na caixa de diálogo da autenticação de usuário do assistente WebVPN.




Esta caixa de diálogo permite que você adicione usuários ao banco de dados local.

2. Clique em **Add** e insira as informações do




usuário.

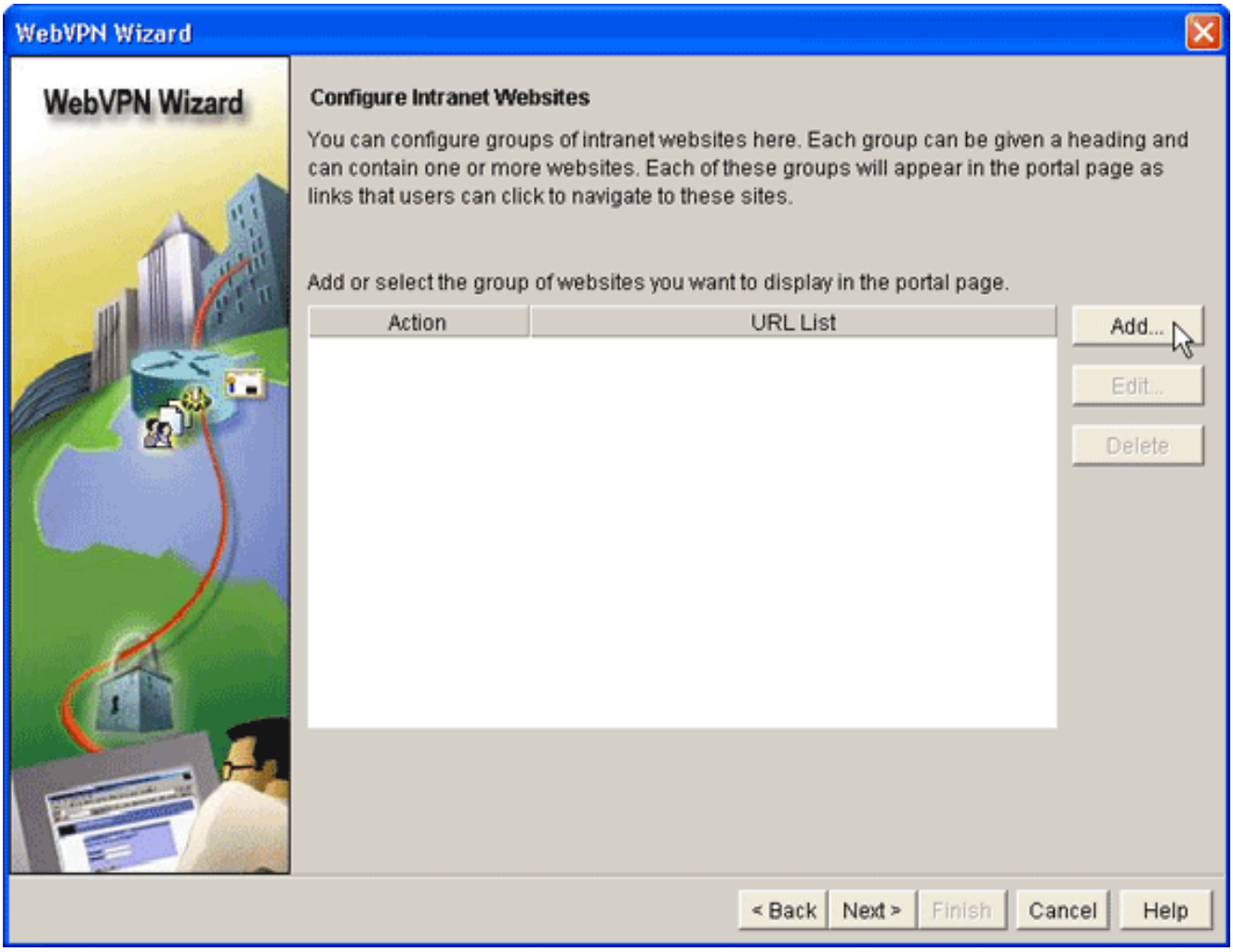
3. Clique em **OK** e adicione usuários a mais conforme o necessário.
4. Depois de adicionar os usuários necessários, clique em **Next** e prossiga para o Passo 4.

## Etapa 4. Configurar os recursos para expor aos usuários

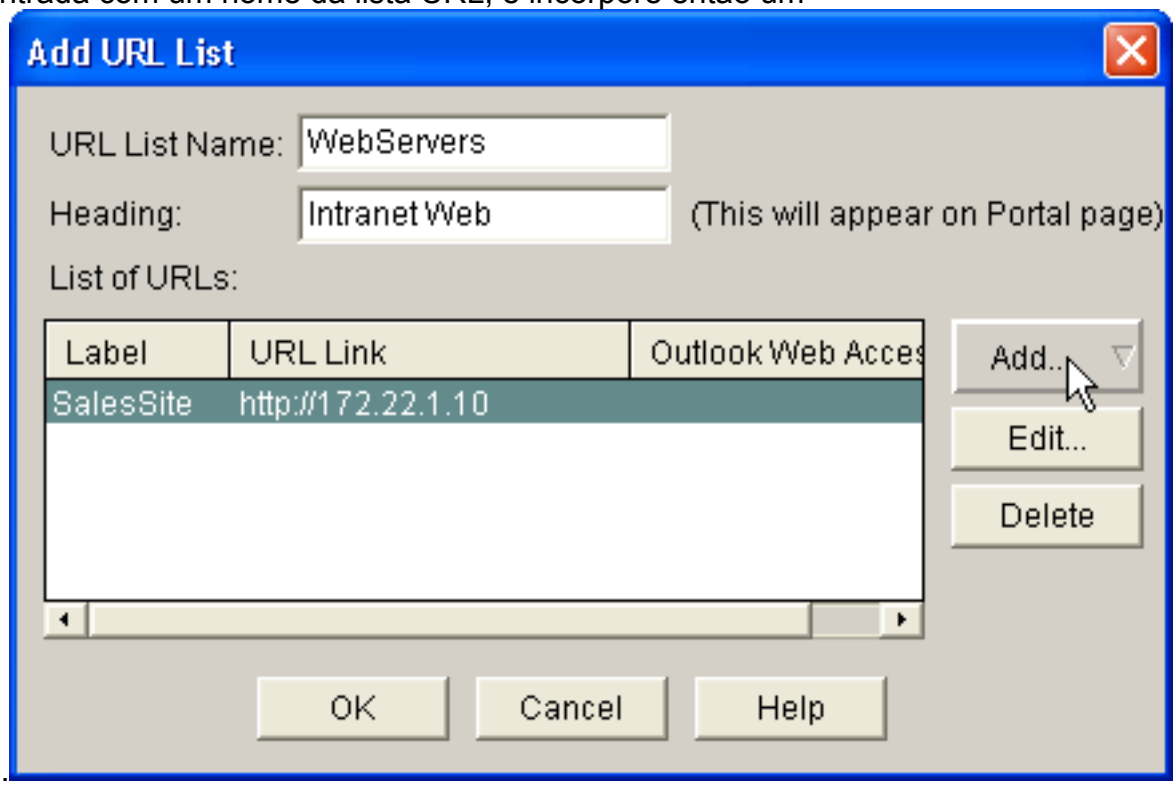
A caixa de diálogo do assistente dos Web site WebVPN do intranet configurar permite que você selecione os recursos do intranet que você quer expor a seus clientes SVC.

Termine estas etapas a fim configurar os recursos para expor aos usuários:

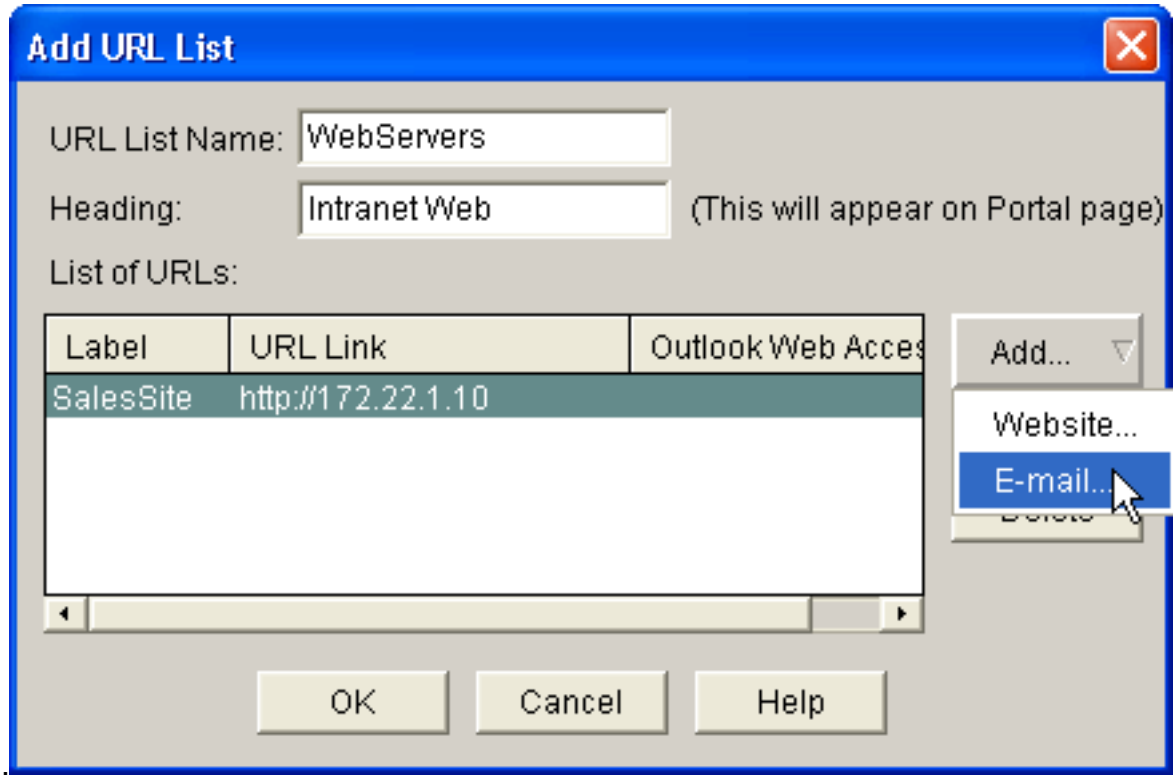
1. Depois que você termina etapa 3, clique o **botão Add** posicionado na caixa de diálogo dos Web site do intranet
   configurar.




2. Dê entrada com um nome da lista URL, e incorpore então um título.

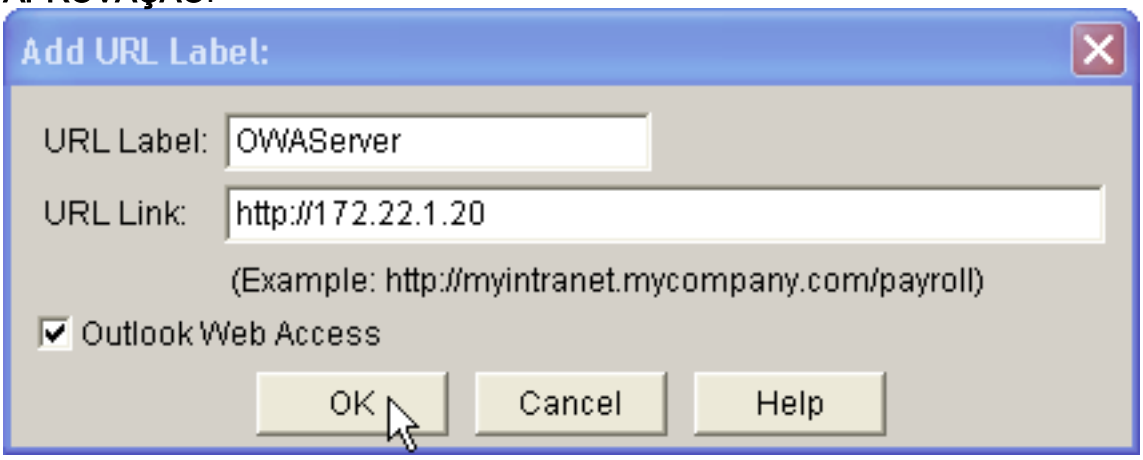



3. O clique **adiciona**, e escolhe o **Web site** adicionar os Web site que você quer expor a este cliente.
4. Incorpore a URL e a informação de link, e clique então a **APROVAÇÃO**.
5. Para adicionar o acesso aos serveres de câmbio OWA, o clique **adiciona** e escolhe o

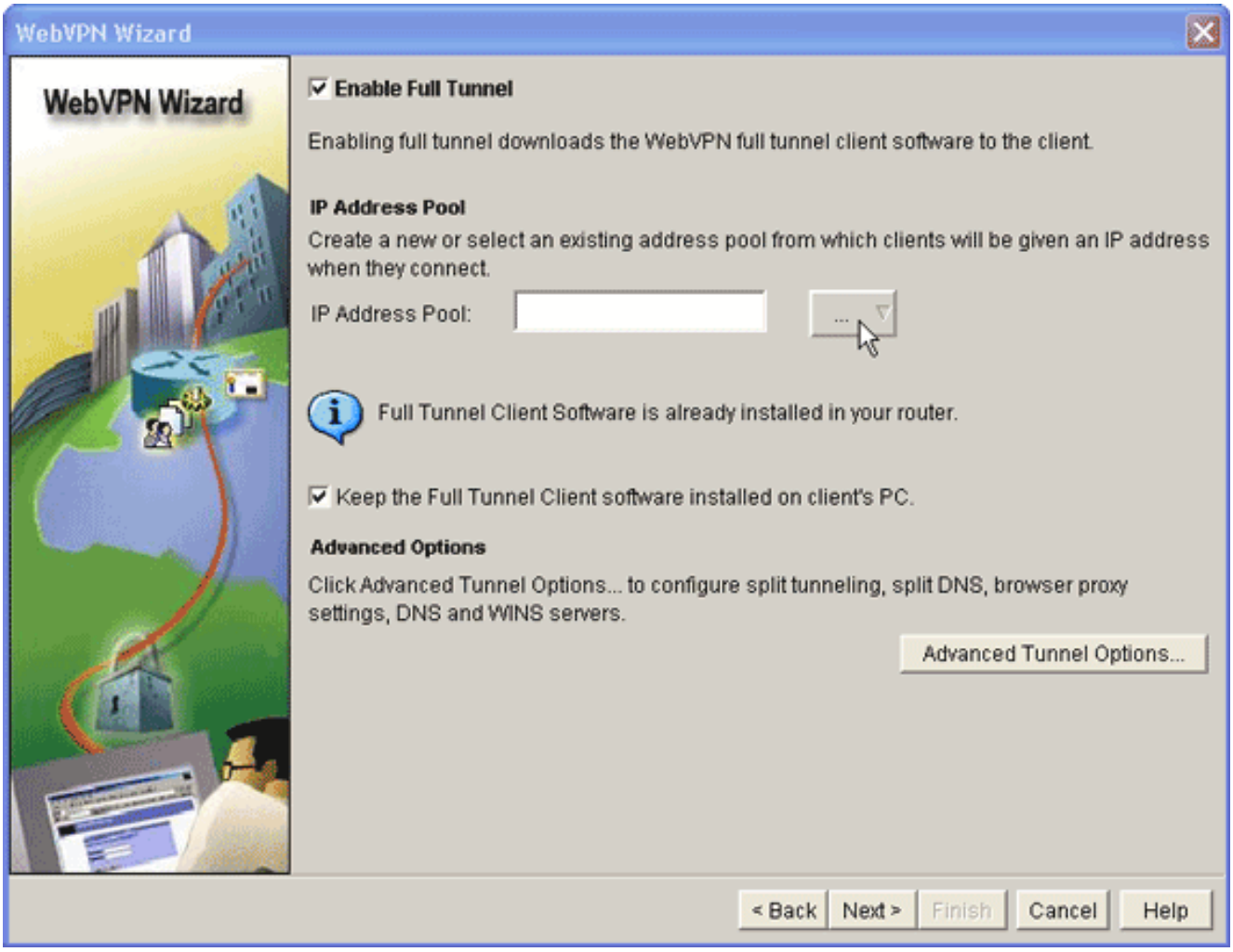



**email**.

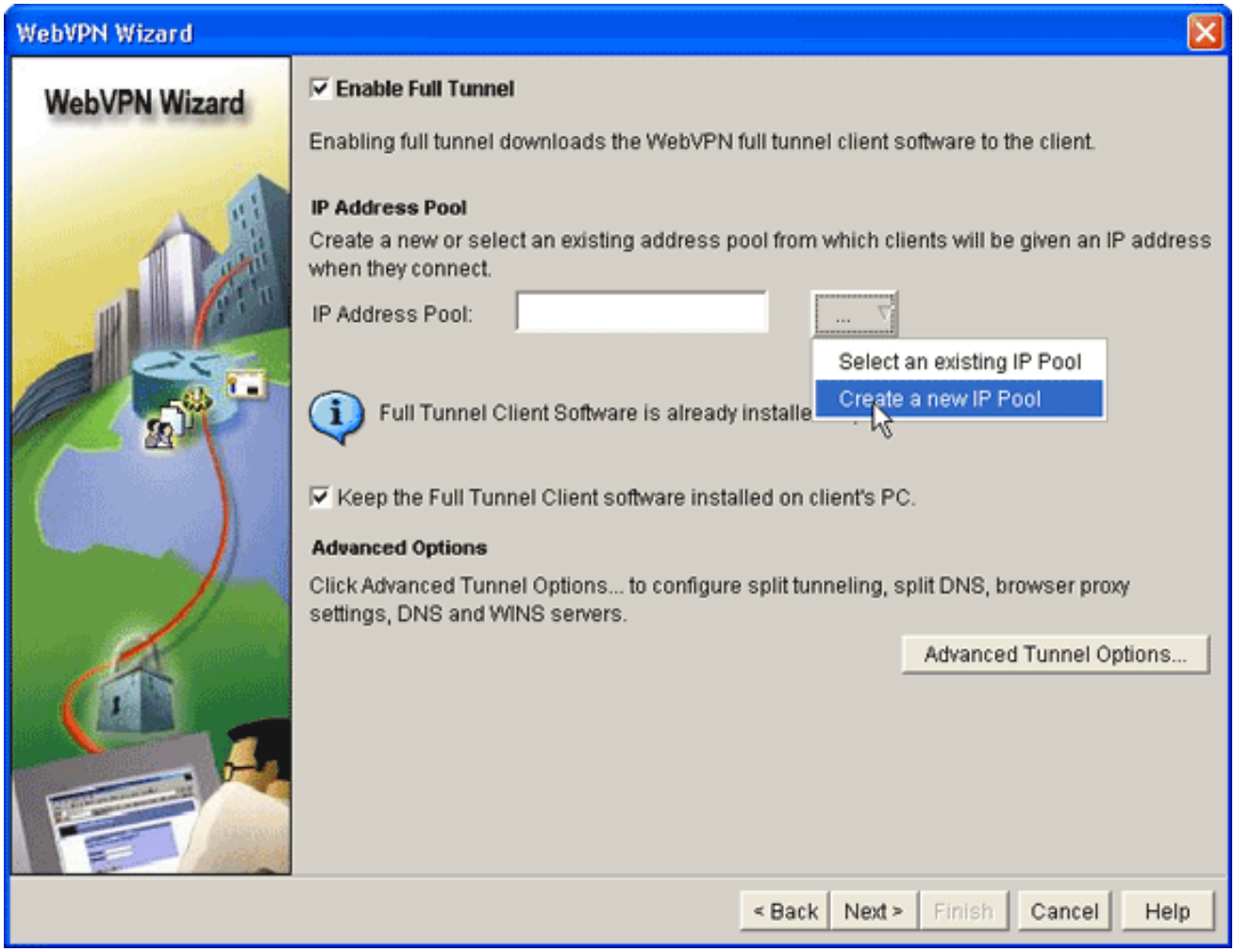
6. Verifique a caixa de verificação do **acesso à Web da probabilidade**, incorpore a etiqueta URL e a informação de link, e clique então a **APROVAÇÃO**.



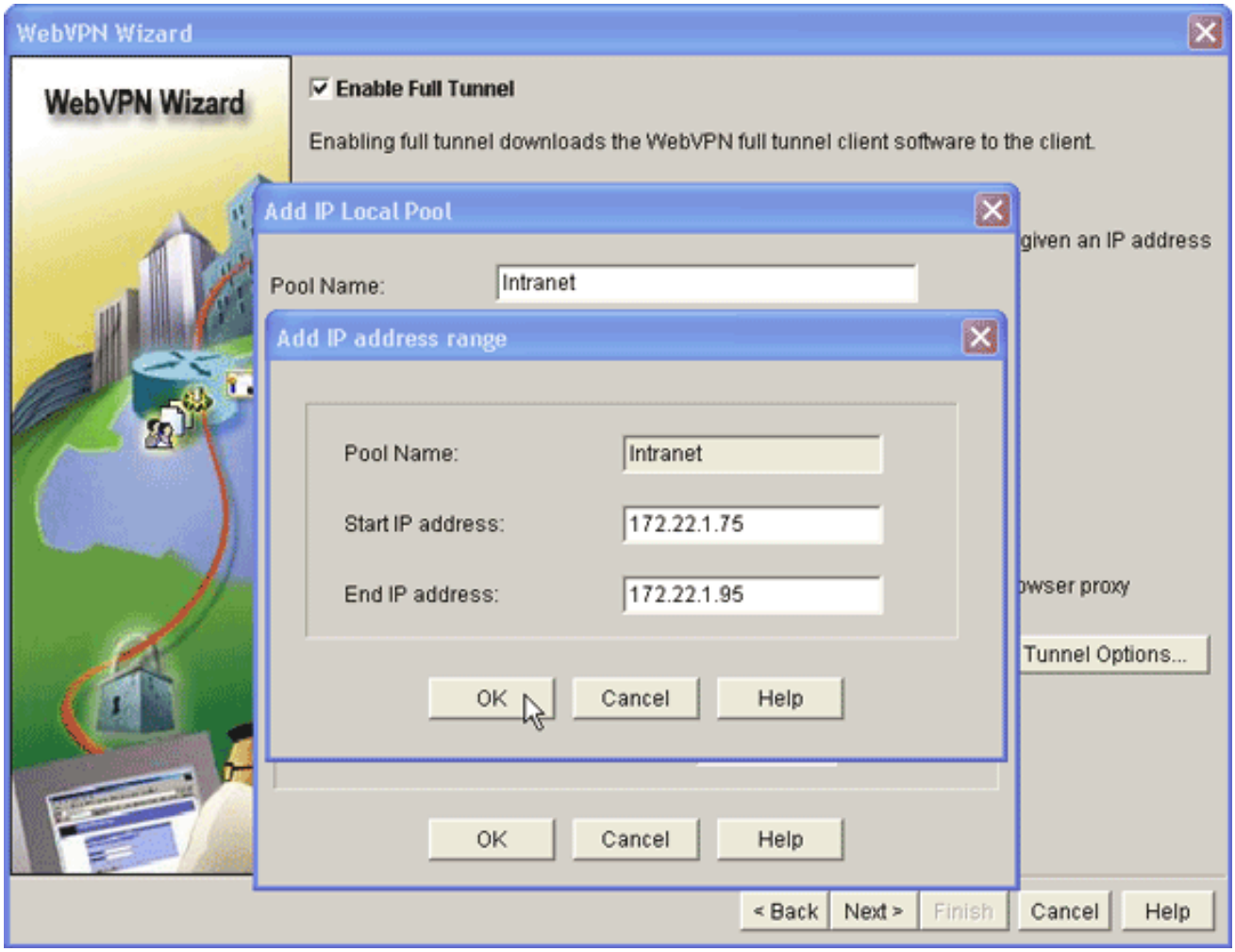

7. Depois que você adiciona os recursos desejados, clique a **APROVAÇÃO**, e clique-a então **em seguida**.A caixa de diálogo completa do túnel do assistente WebVPN aparece.



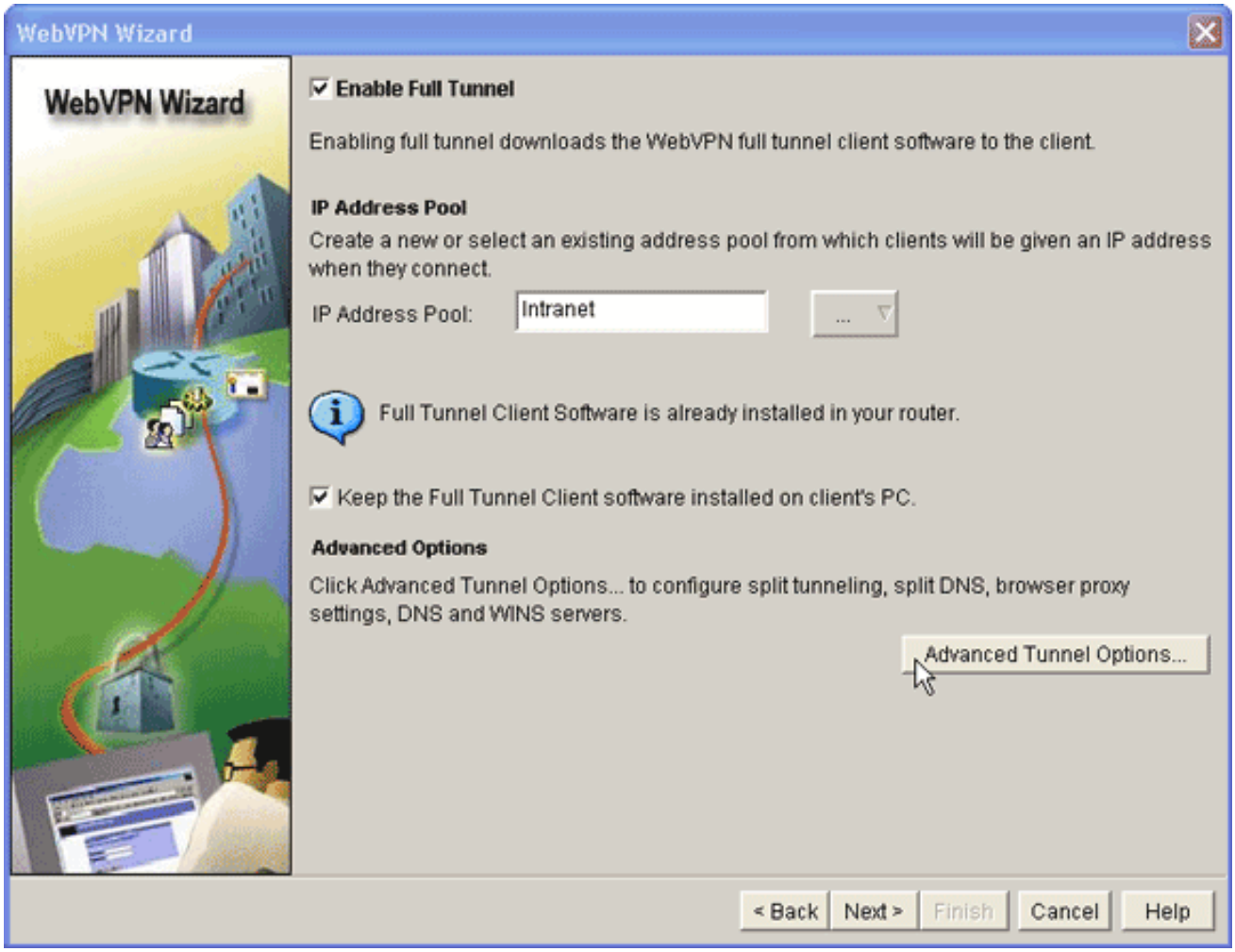

8. Certifique-se de que a caixa de verificação **Enable Full Tunnel** esteja marcada.
9. Crie um pool dos IP address que os clientes deste contexto WebVPN podem usar. O pool de endereços deve corresponder aos endereços disponíveis e roteáveis em sua intranet.
10. Clique as elipses (**...**) ao lado do campo do pool do IP address, e escolha **criam um IP pool novo**.



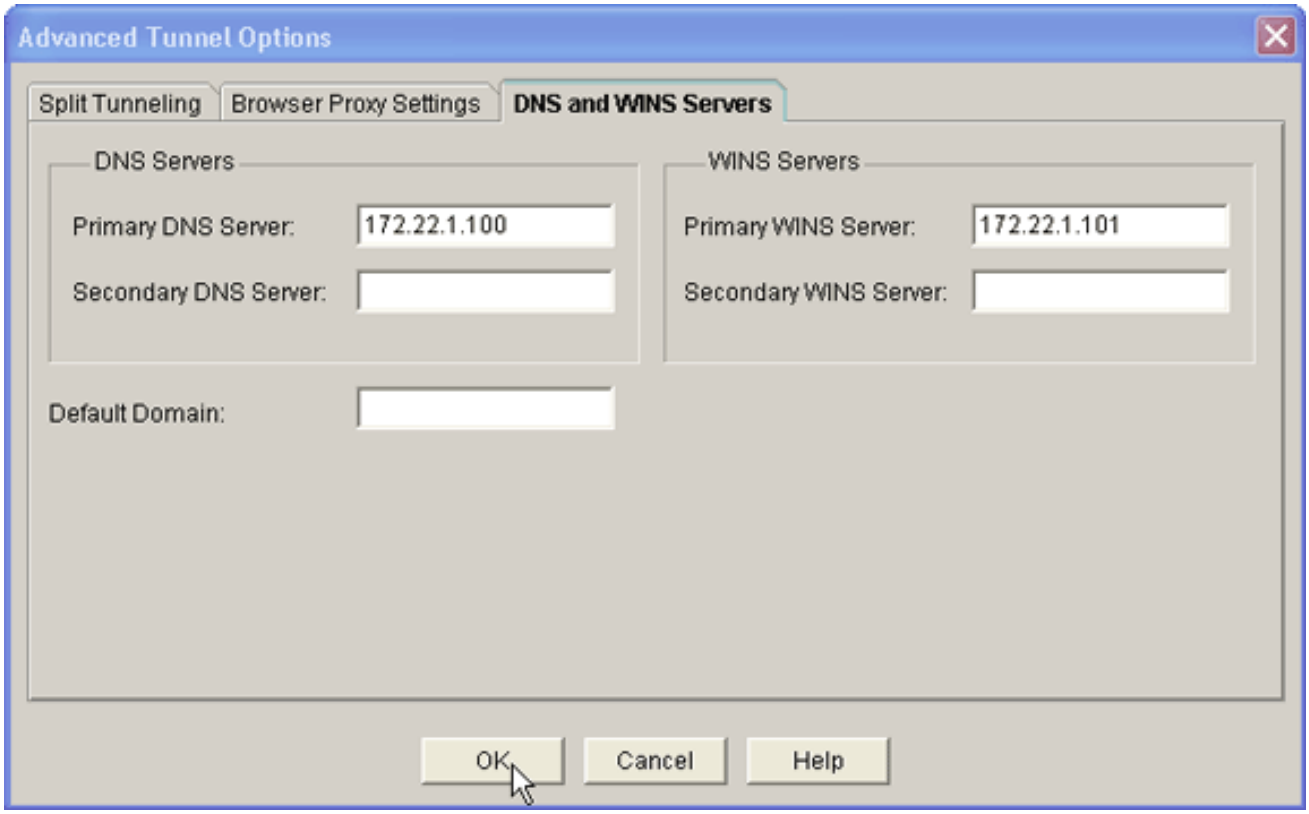

11. Na caixa de diálogo do conjunto local IP adicionar, dê entrada com um nome para o pool, e o clique
**adiciona**.



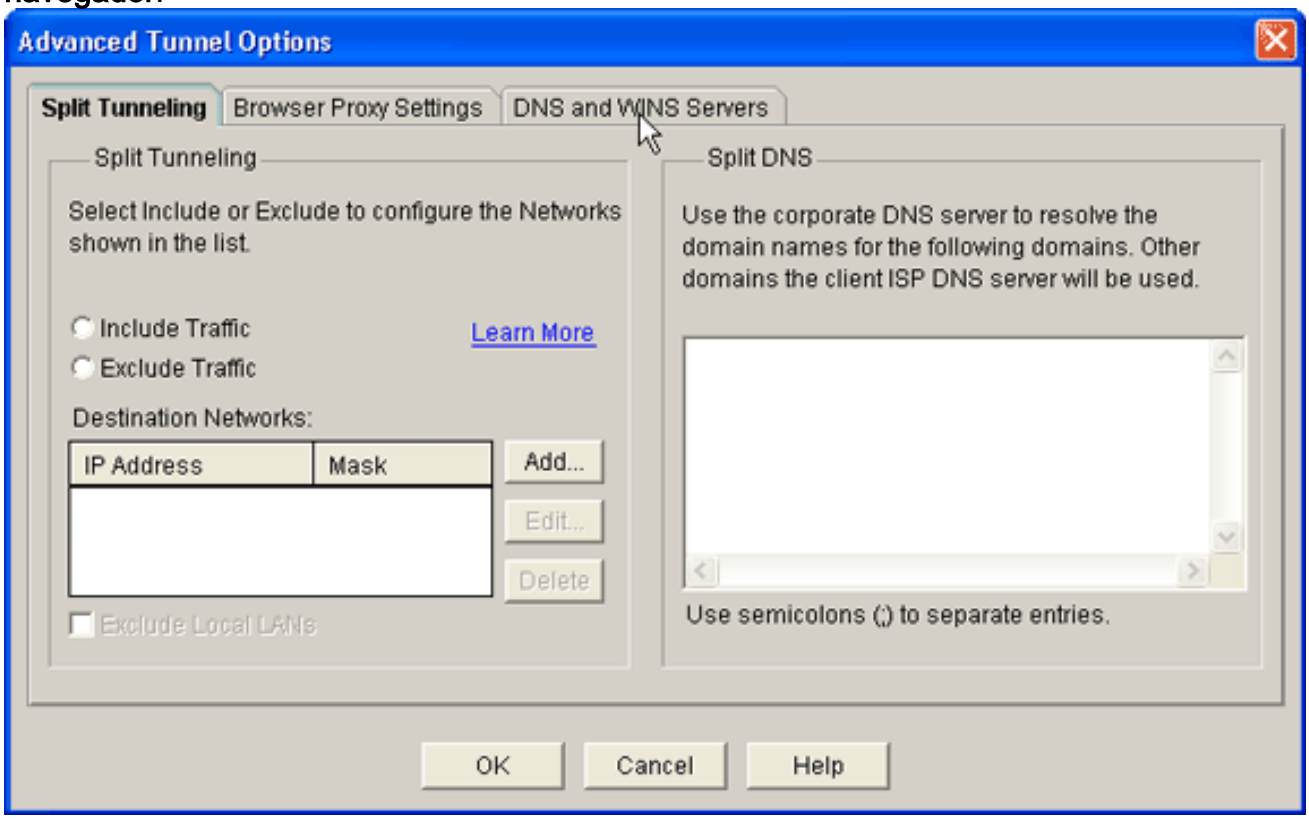

12. Na caixa de diálogo do intervalo de endereço IP adicionar, incorpore a escala do conjunto de endereços para os clientes SVC, e clique a **APROVAÇÃO**.**Nota:** O pool do IP address deve estar em uma escala de uma relação conectada diretamente ao roteador. Se você quer usar uma escala diferente do pool, você pode criar um endereço de loopback associado com seu pool novo para satisfazer esta exigência.
13. Clique em
**OK**.



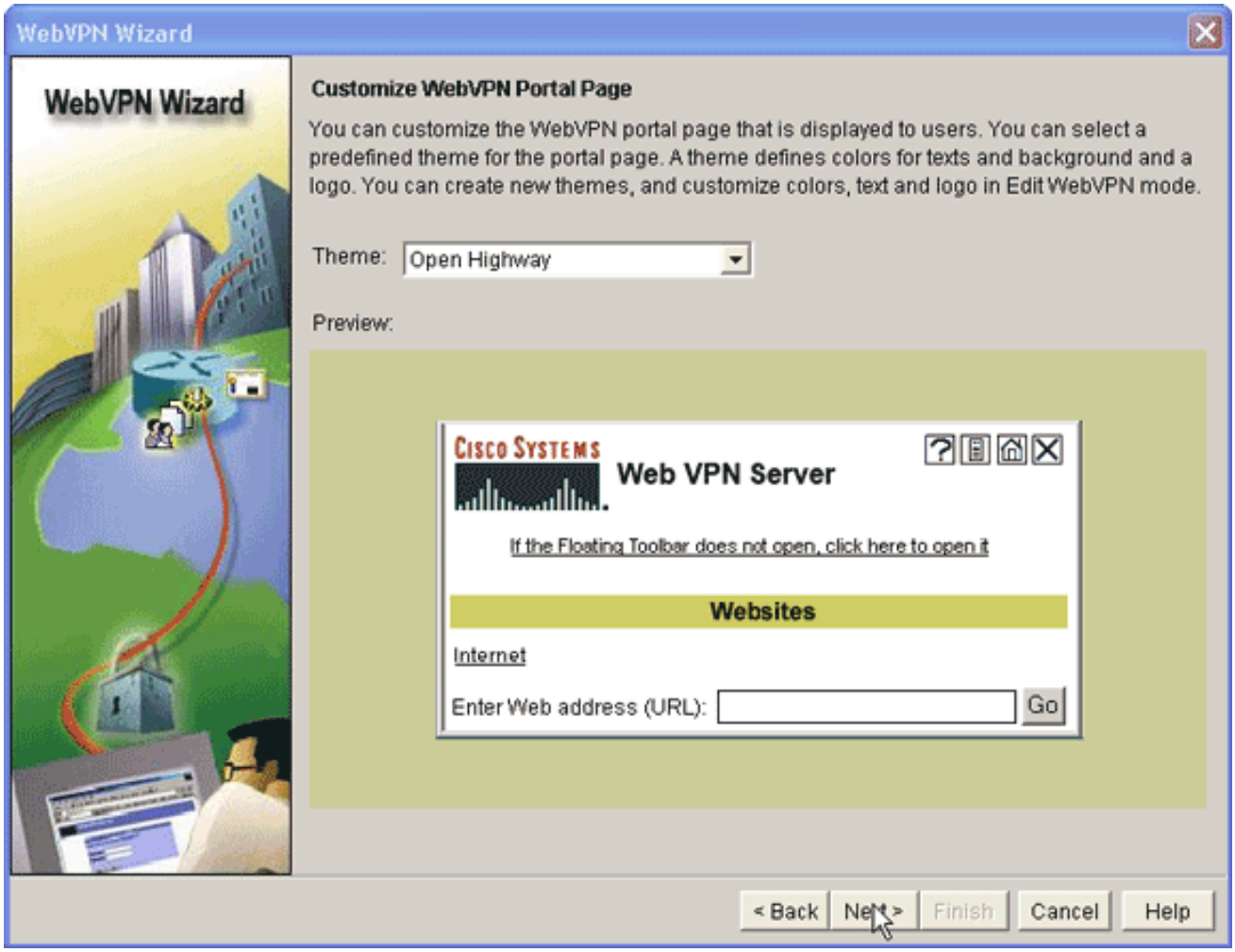

14. Se você quer seus clientes remotos armazenar permanentemente uma cópia do clique SVC o **mantimento o software do cliente completo do túnel instalou na** caixa de verificação do **PC do cliente**. Cancele esta opção para exigir o cliente transferir o software SVC cada vez que um cliente conecta.
15. Configure as opções avançadas do túnel, como tunelamento dividido, DNS dividido, configurações de proxy do navegador e servidores DNS e WINS. A Cisco recomenda que você configure pelo menos os servidores DNS e WINS.Para configurar opções avançadas do túnel, conclua estes passos:Clique no botão **>Advanced Tunnel Options**.



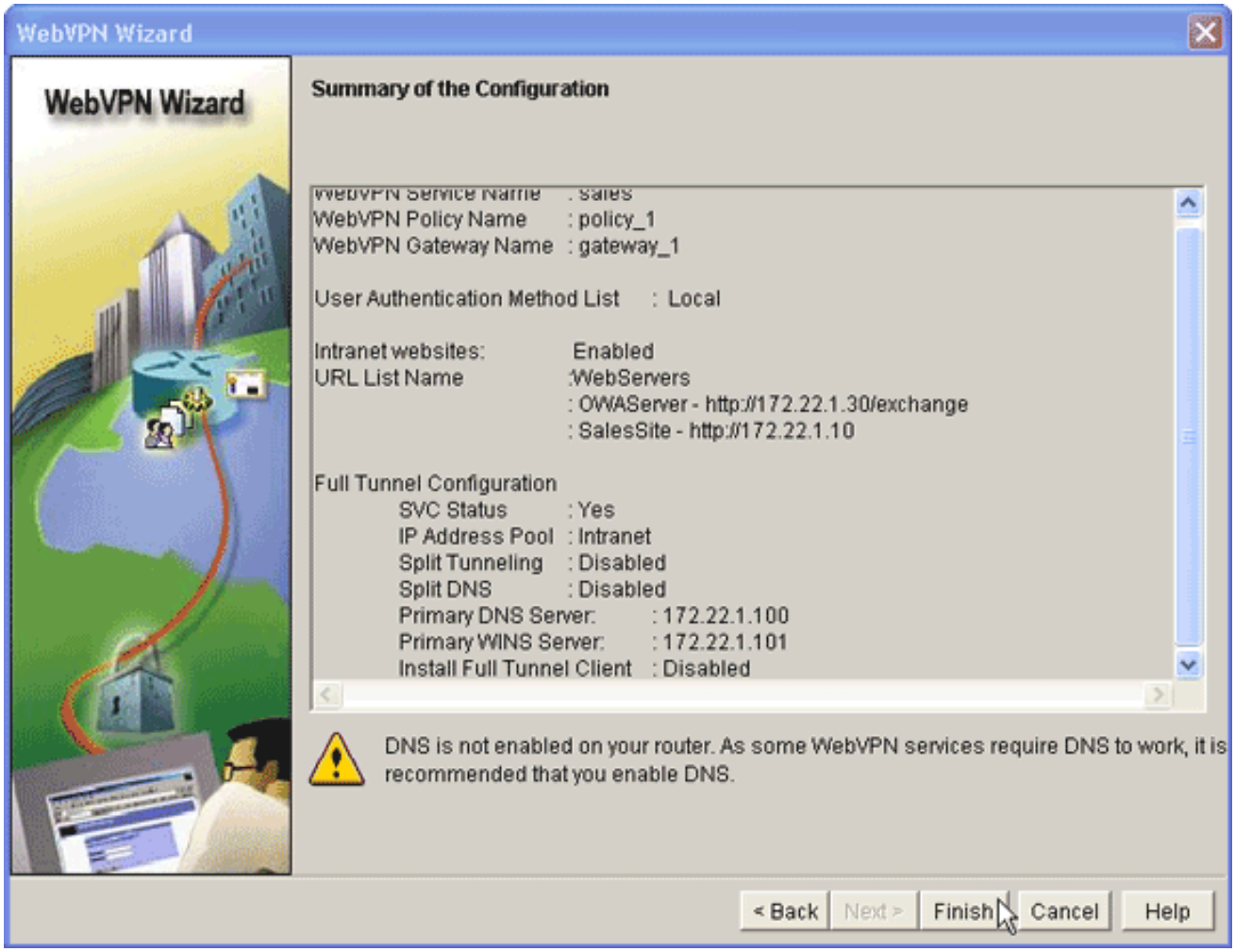

Clique na guia **DNS and WINS Servers** e insira os endereços IP primários dos servidores DNS e WINS.Para configurar ajustes do proxy do Split Tunneling e do navegador, clique a aba dos **ajustes do proxy do Split Tunneling** ou do **navegador**.



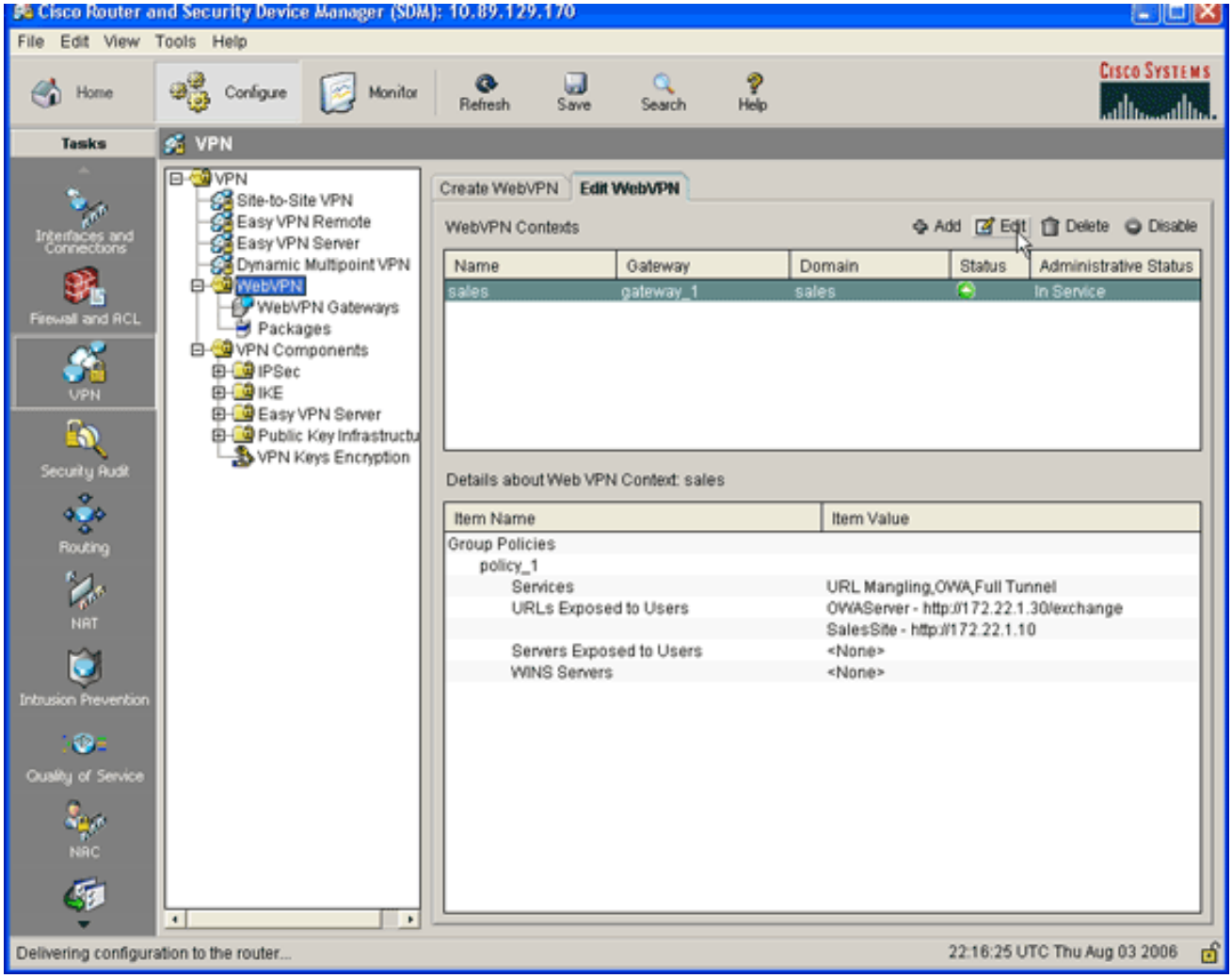

16. Após configurar as opções necessárias, clique **Next**.
17. Personalize a página portal WebVPN ou selecione os valores padrão.A página portal da personalização WebVPN permite que você personalize como a página portal WebVPN se publica a seus clientes.



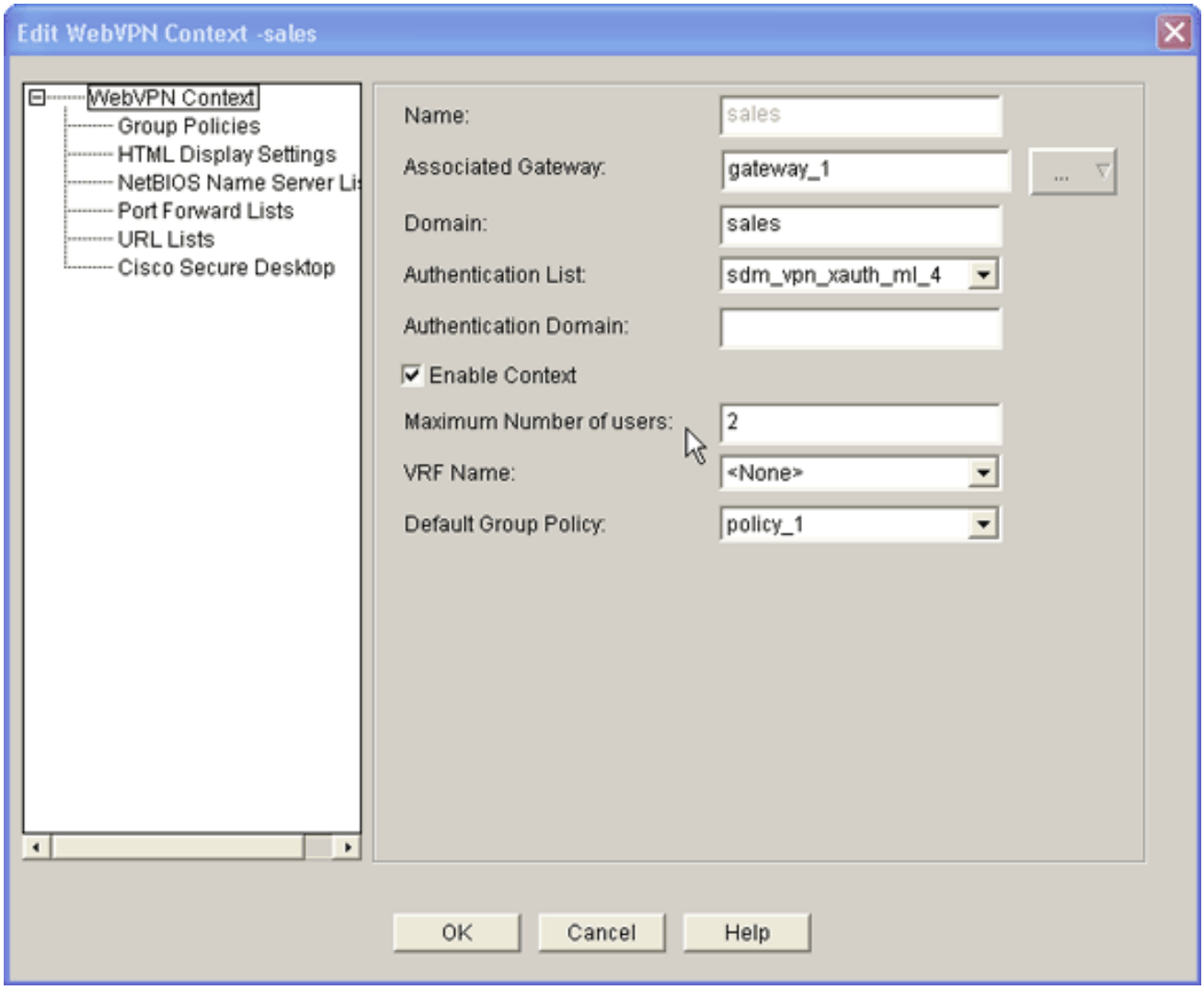

18. Depois que você configura a página portal WebVPN, clique **em seguida**, clique o **revestimento**, e clique então a **APROVAÇÃO**.O assistente WebVPN submete comandos da excursão ao roteador.
19. **APROVAÇÃO do** clique para salvar sua configuração.**Nota:** Se você recebe um Mensagem de Erro, a licença WebVPN pode estar incorreta. Um exemplo de mensagem de erro é mostrado nesta
imagem:




Para corrigir um problema de licença, conclua estes passos:Clique em **Configure** e clique em **VPN**.Expanda o **WebVPN**, e clique a aba da **edição WebVPN**.




Realce seu contexto recém-criado e clique no **botão Edit**.




No campo do Maximum Number of users, insira o número correto de usuários para sua licença.Clique em **OK** e, em seguida, clique em **OK**.Seus comandos são gravados no arquivo de configuração.Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

## Resultados

O ASDM cria estas configurações de linha de comando:

**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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

### Procedimento

Para testar sua configuração, entre em *http://192.168.0.37/sales em um* web browser SSL-permitido do cliente.

## Comandos

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para obter informações detalhadas sobre os **comandos show**, consulte Verificação da Configuração do WebVPN.

**Nota:** A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

# Troubleshooting

Use esta seção para resolver problemas de configuração.

## Problema de Conectividade SSL

**Problema:** Os clientes VPN SSL não conseguem se conectar ao roteador.

**Solução:** Endereços IP insuficientes no pool de endereços IP podem causar este problema. Aumente o número de endereços IP no pool de endereços IP no roteador para resolver este problema.

## Comandos para Troubleshooting

Vários **comandos clear** estão associados ao WebVPN. Para obter informações detalhadas sobre os comandos show, consulte Verificação da Configuração do WebVPN.

Vários **comandos debug** estão associados ao WebVPN. Para obter informações detalhadas sobre estes comandos, consulte Uso de Comandos de Depuração do WebVPN.

**Nota:** O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

# Informações Relacionadas

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Exemplo de Configuração de VPN SSL Sem Clientes (WebVPN) no Cisco IOS com SDM
- Exemplo de Configuração de VPN SSL com Thin-Client (WebVPN) no Cisco IOS com SDM
- Guia de Implantação de WebVPN e Convergência DMVPN
- Suporte Técnico e Documentação - Cisco Systems