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

Contents

Introdução

O Cliente VPN com SSL (SVC) fornece um túnel completo para comunicações seguras à rede interna corporativa. Você pode configurar o acesso em cada usuário ou pode criar contextos WebVPN diferentes nos quais você coloca um ou mais 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 VPN SSL nestes modos:

- VPN SSL sem cliente (WebVPN) — fornece um cliente remoto que requer um navegador da Web habilitado para SSL para acessar servidores Web HTTP ou HTTPS em uma rede local

corporativa (LAN). Além disso, a VPN SSL sem cliente fornece acesso à navegação de arquivos do Windows através do protocolo CIFS (Common Internet File System). O Outlook Web Access (OWA) é um exemplo de acesso HTTP.

Consulte VPN SSL Sem Clientes (WebVPN) no Cisco IOS com Exemplo de Configuração de SDM para saber mais sobre a VPN SSL Sem Clientes.

- Thin-Client SSL VPN (Port Forwarding) — Fornece um cliente remoto que faz download de um pequeno applet baseado em Java e permite acesso seguro para aplicações de Protocolo de Controle de Transmissão (TCP - Transmission Control Protocol) que usam números de porta estáticos. Point of presence (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), secure shell (ssh) e Telnet são exemplos de acesso seguro. Como os arquivos na máquina local são alterados, os usuários devem ter privilégios administrativos locais para usar esse método. Esse método de VPN SSL não funciona com aplicativos que usam atribuições de porta dinâmicas, como alguns aplicativos de protocolo de transferência de arquivos (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.

  Observação: o User Datagram Protocol (UDP) não é suportado.

- Cliente VPN SSL (Modo de túnel completo SVC)—Faz o download de um pequeno cliente para a estação de trabalho remota e permite acesso seguro total aos recursos em uma rede corporativa interna. Você pode fazer o download do SVC para uma estação de trabalho remota permanentemente ou pode remover o cliente depois que a sessão segura for fechada.

Este documento demonstra a configuração de um roteador Cisco IOS para uso por 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 dos roteadores listados na Introdução com uma imagem de Segurança avançada (12.4(6)T ou posterior)
- Cisco Security Device Manager (SDM) versão 2.3

  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 roteador

  Você pode usar um certificado autoassinado persistente ou uma Autoridade de Certificação (CA) externa para satisfazer esse requisito. Para obter mais informações sobre certificados com assinatura automática persistente, consulte Certificados com assinatura automática persistente.

Componentes Utilizados

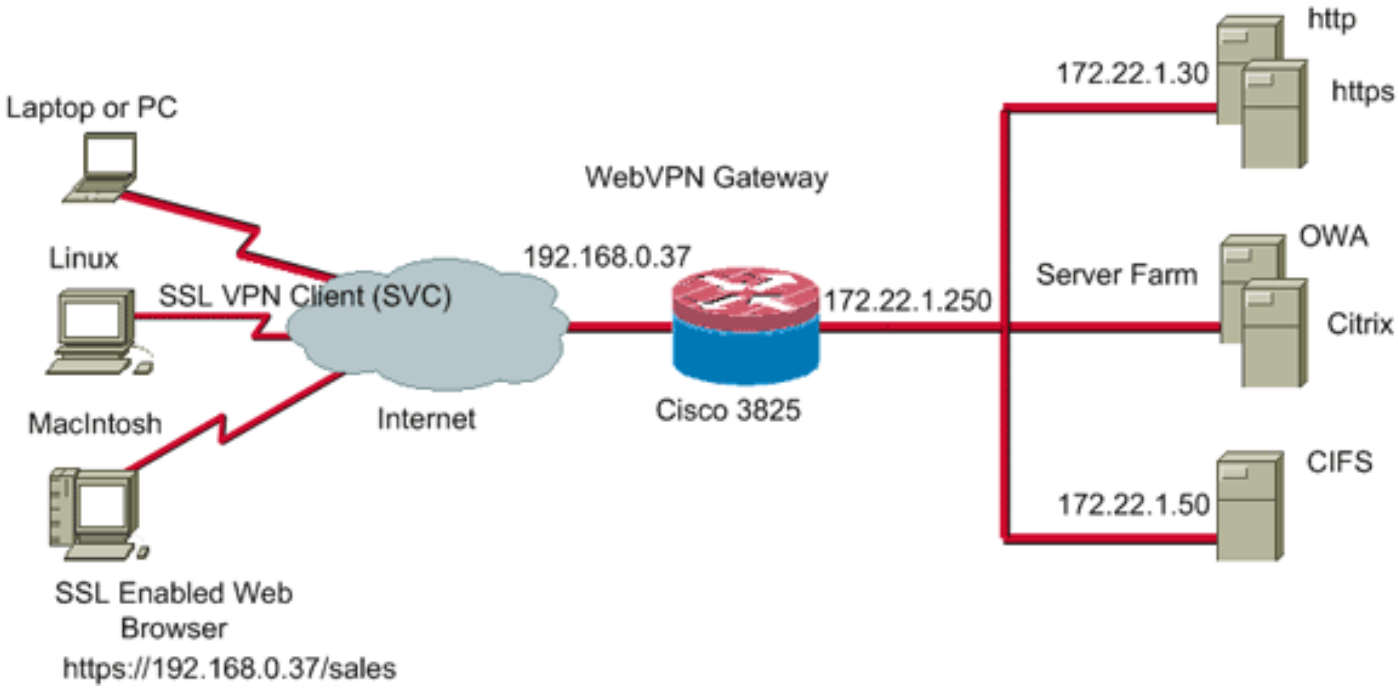
As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco IOS série 3825 com 12.4(9)T
- Security Device Manager (SDM) versão 2.3.1

Observação: as informações 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)

   Os roteadores com a licença de pacote de segurança apropriada já têm o aplicativo SDM carregado na memória flash. Consulte Download e Instalação do Cisco Router e do Security Device Manager (SDM) para obter e configurar o software.

2. Faça o download de uma cópia do SVC para o PC de gerenciamento.

   Você pode obter uma cópia do arquivo do pacote SVC em Download de Software: Cisco SSL VPN Client (somente clientes registrados) . Você deve ter uma conta CCO válida com um contrato de serviço.

3. Defina a data, a hora e o fuso horário corretos e configure um certificado digital no roteador.

Conventions

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

Informações de Apoio

O SVC é inicialmente carregado no roteador do gateway WebVPN. Cada vez que o cliente se conecta, uma cópia do SVC é dinamicamente transferida para o PC. Para alterar esse comportamento, configure o roteador para permitir que o software permaneça permanentemente no computador cliente.

Configurar o SVC no IOS

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

Conclua estes passos para configurar o SVC no roteador IOS:

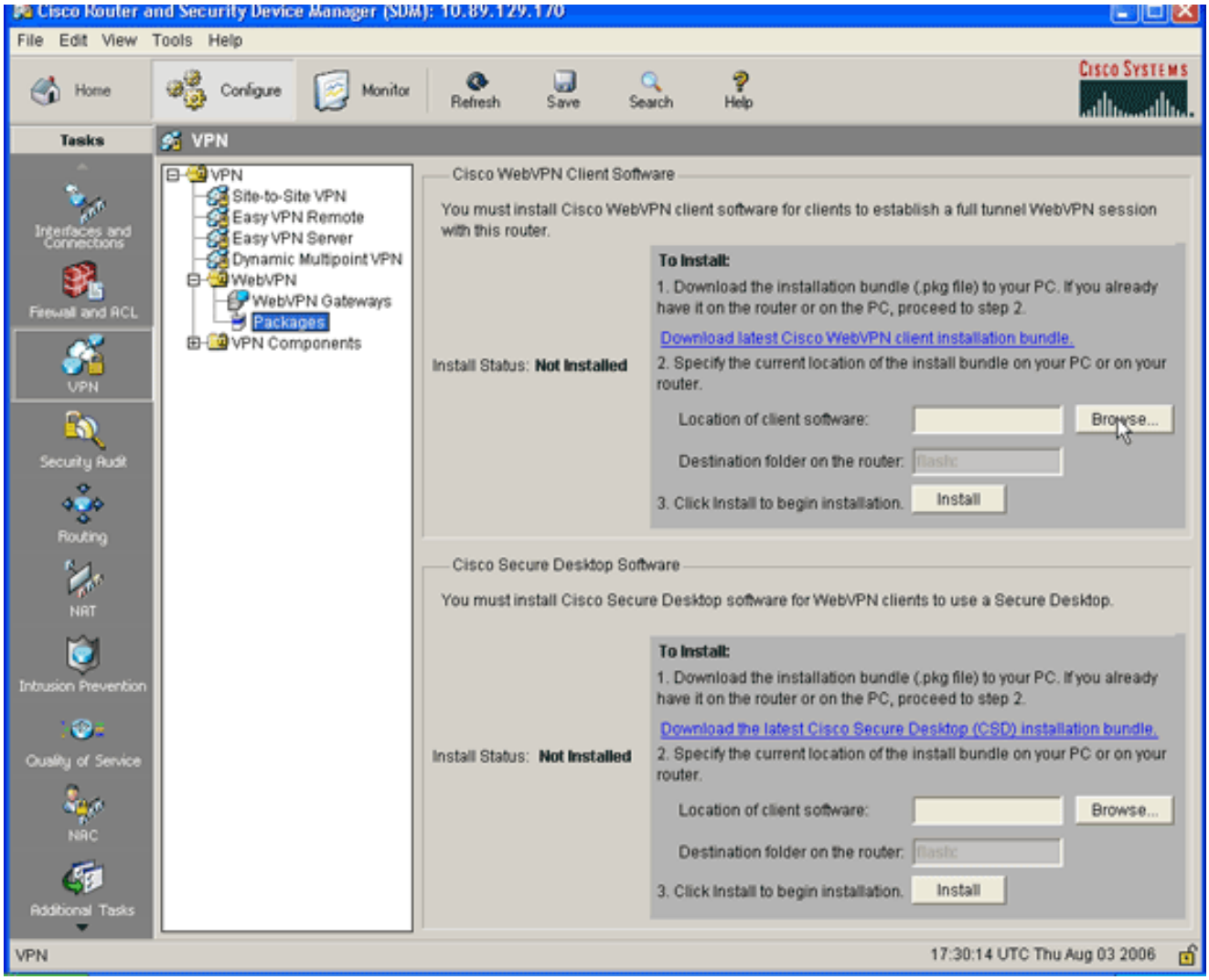
1. Instalar e ativar o software SVC no roteador IOS
2. Configurar um Contexto WebVPN e o Gateway WebVPN com o Assistente de SDM
3. Configurar o banco de dados de usuários para usuários do SVC
4. Configurar os recursos para expor aos usuários

Etapa 1. Instalar e ativar o software SVC no roteador IOS

Conclua estas etapas para instalar e ativar o software SVC no roteador IOS:

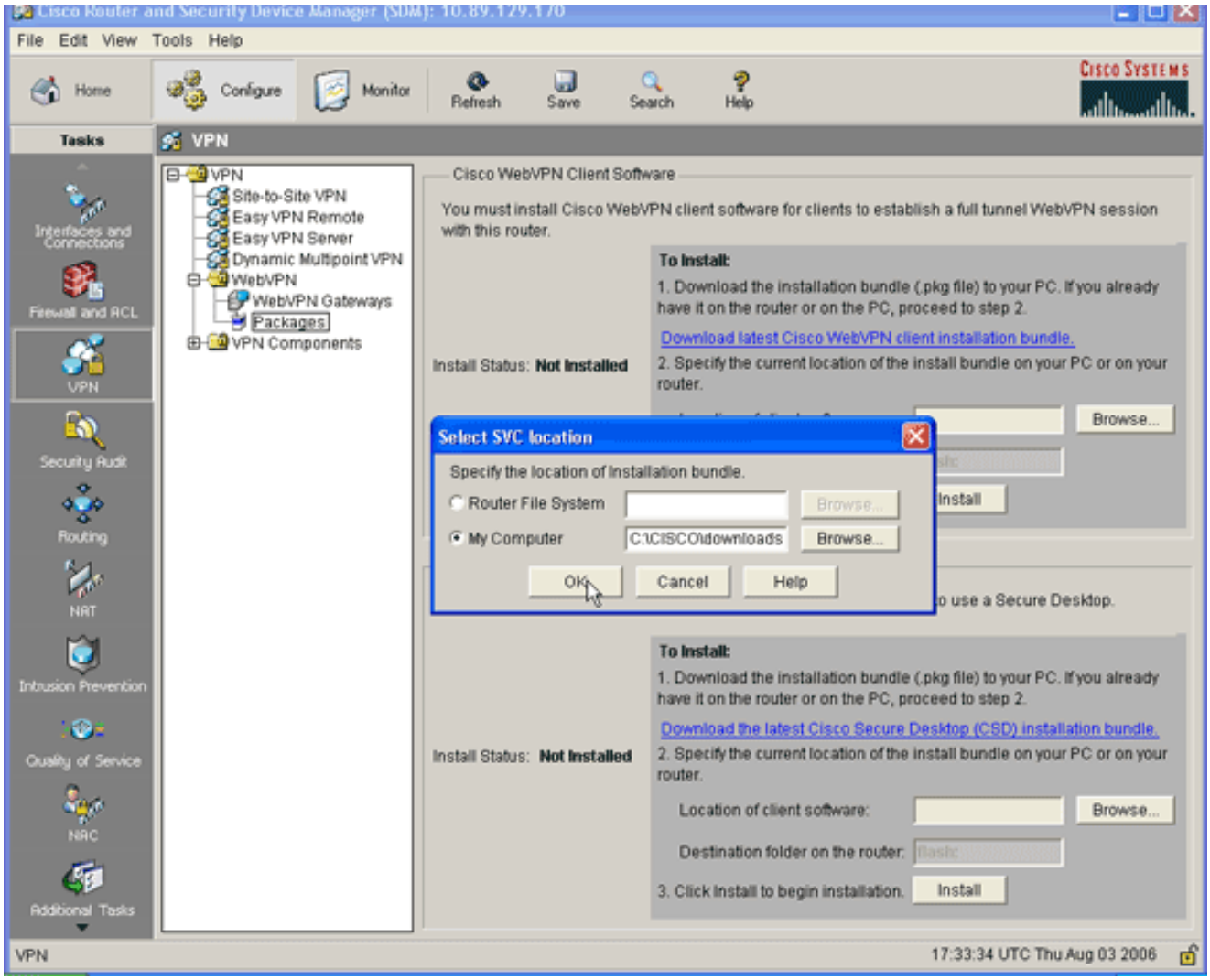
1. Abra o aplicativo SDM, clique em Configure e em VPN.

2. Expanda WebVPN e escolha Packages.



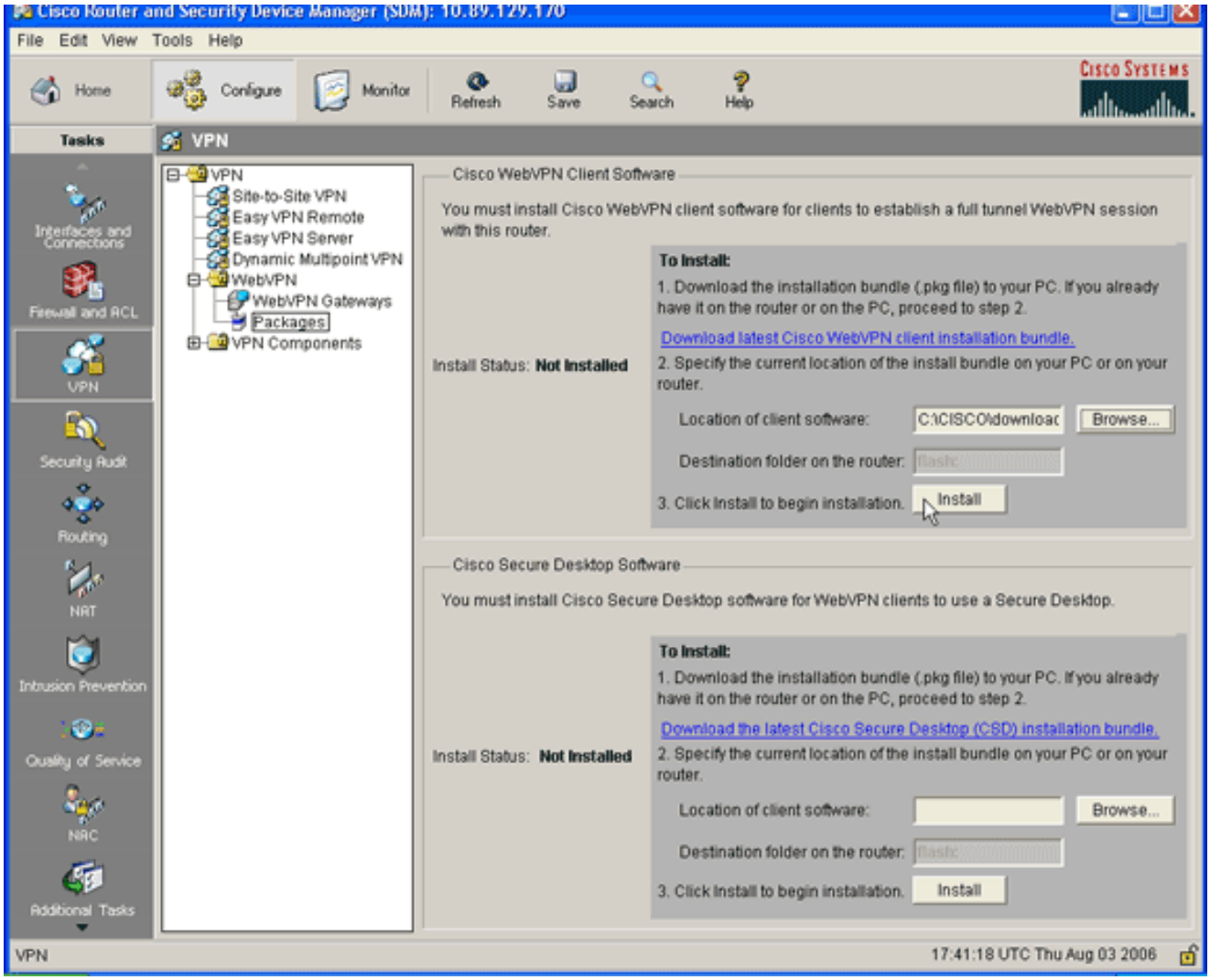
3. Na área Cisco WebVPN Client Software, clique no botão Browse.

   A caixa de diálogo Selecionar local do SVC é exibida.



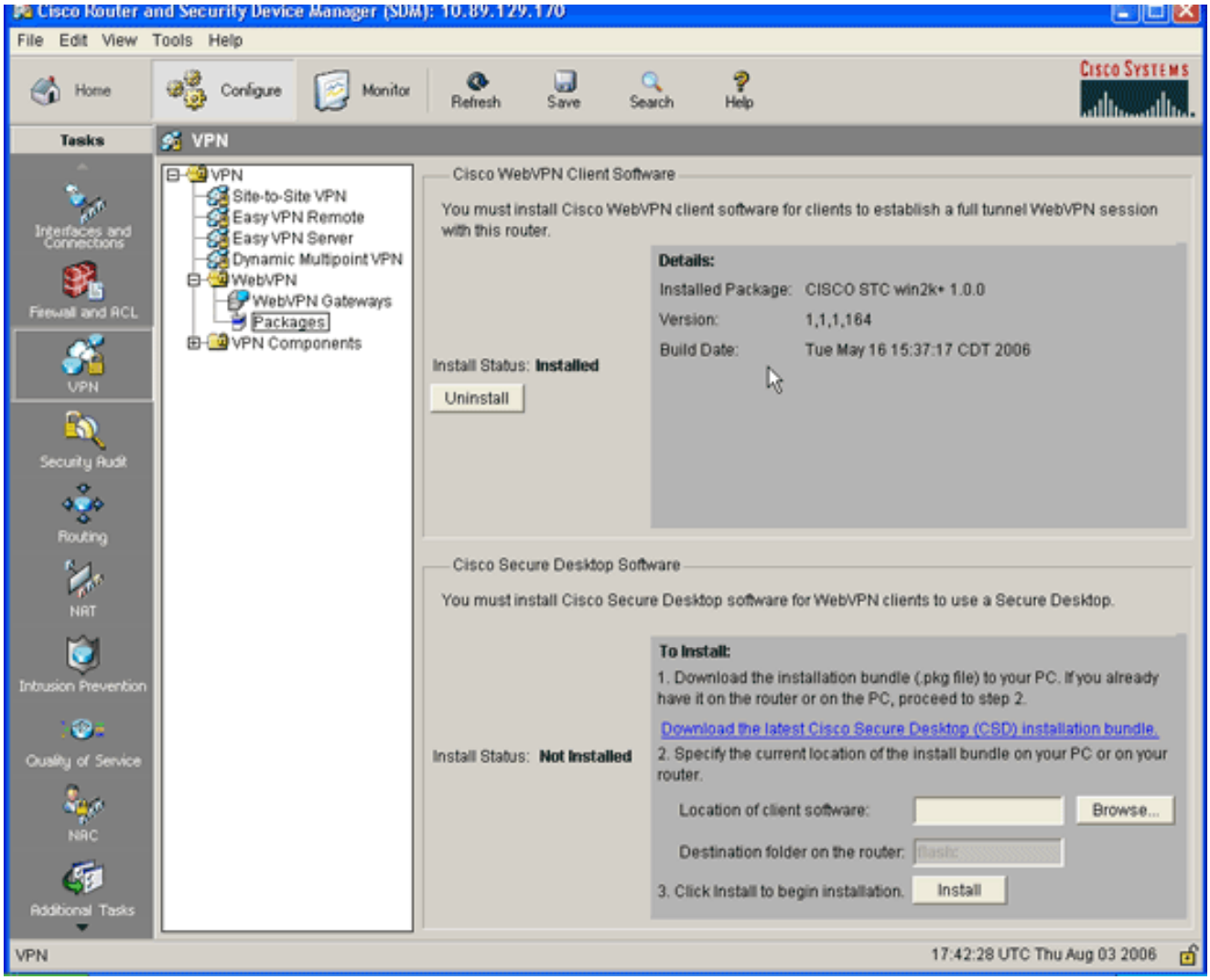
4. Clique no botão de opção Meu computador e, em seguida, clique em Procurar para localizar o pacote SVC no seu PC de gerenciamento.

5. Clique em OK e, em seguida, clique no botão Install.



6. Clique em Yes e, em seguida, em OK.

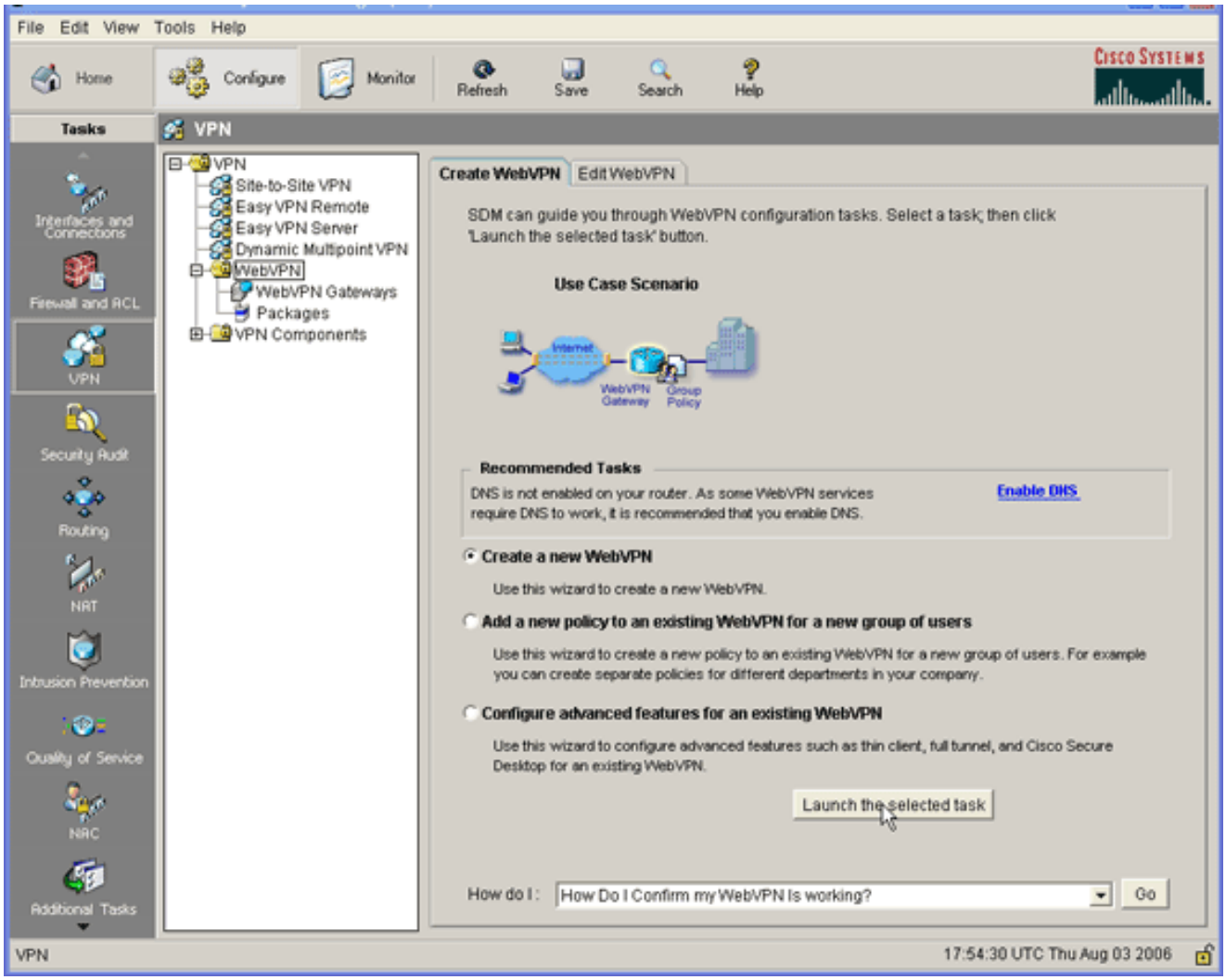
   Uma instalação bem-sucedida do pacote SVC é mostrada nesta imagem:



Etapa 2. Configurar um Contexto WebVPN e o Gateway WebVPN com o Assistente de SDM

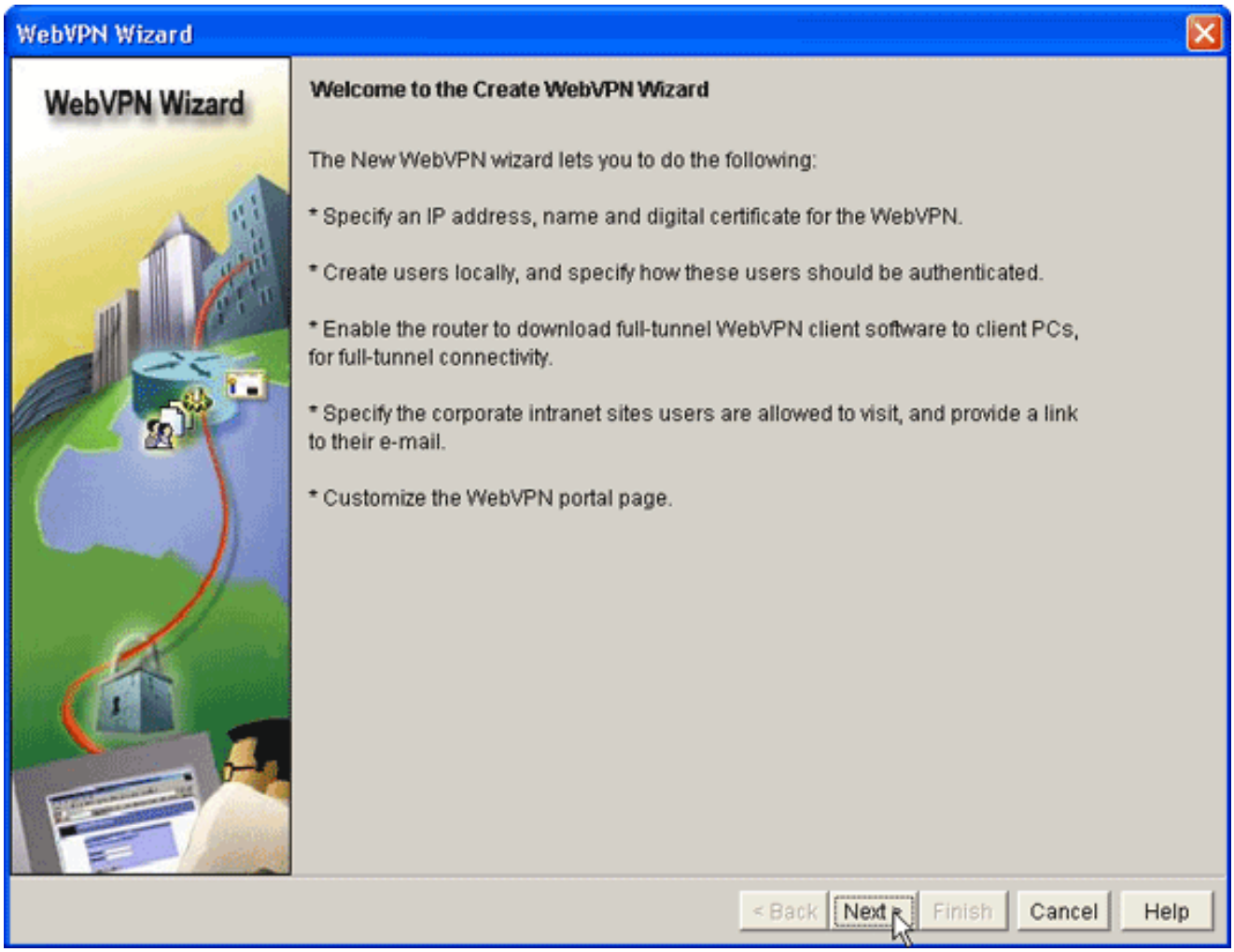
Conclua estas etapas para configurar um contexto WebVPN e um gateway WebVPN:

1. Depois que o SVC estiver instalado no roteador, clique em Configure e em VPN.
2. Clique em WebVPN e clique na guia Create WebVPN.

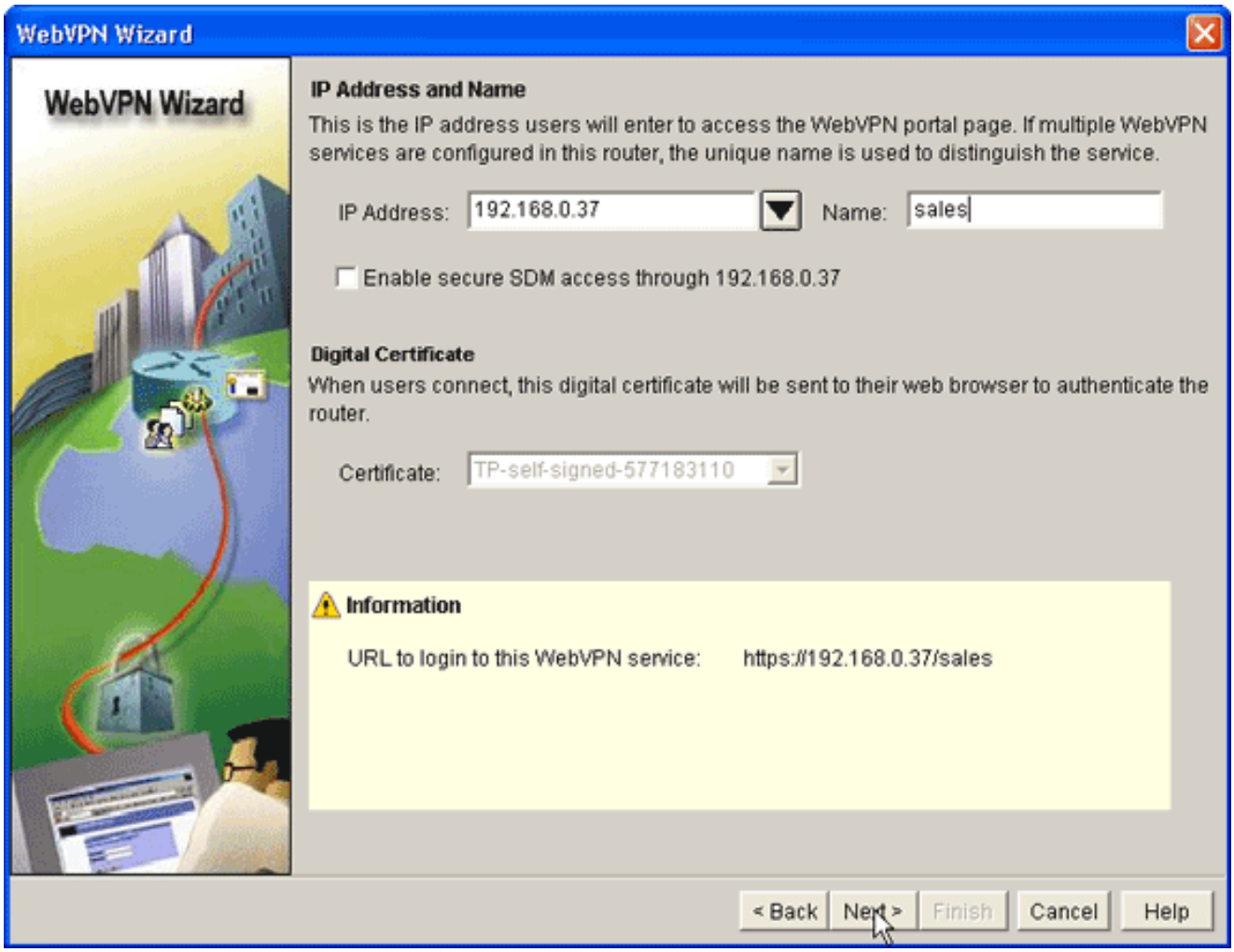


3. Marque o botão de opção Create a New WebVPN e clique em Launch the seleted task.

   A caixa de diálogo WebVPN Wizard é exibida.



4. Clique em Next.



5. Insira o endereço IP do novo gateway WebVPN e insira um nome exclusivo para este contexto WebVPN.

   Você pode criar contextos WebVPN diferentes para o mesmo endereço IP (gateway WebVPN), mas cada nome deve ser exclusivo. Este exemplo usa este endereço IP: https://192.168.0.37/sales

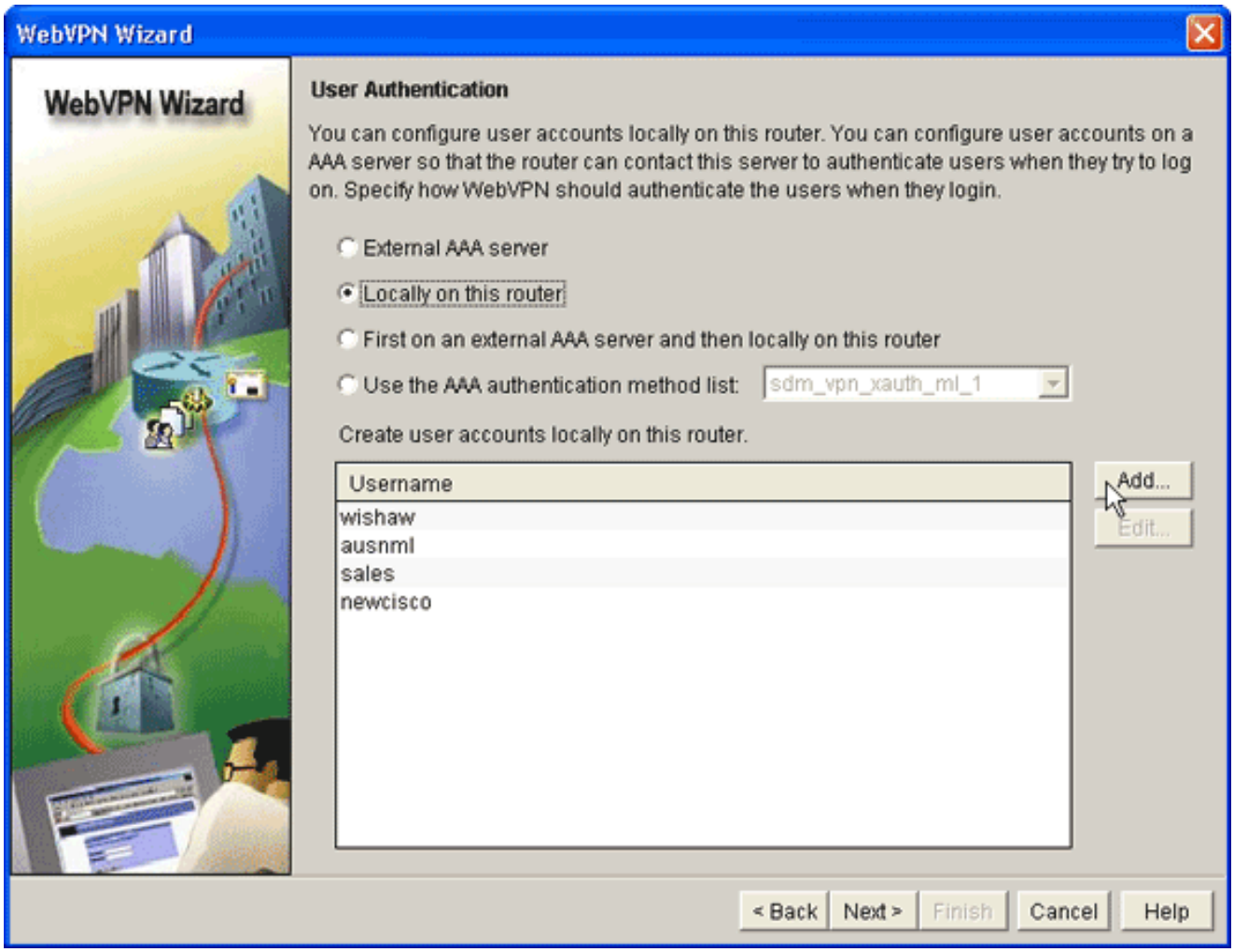
6. Clique em Next e prossiga para o Passo 3.

Etapa 3. Configurar o banco de dados de usuários para usuários do SVC

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

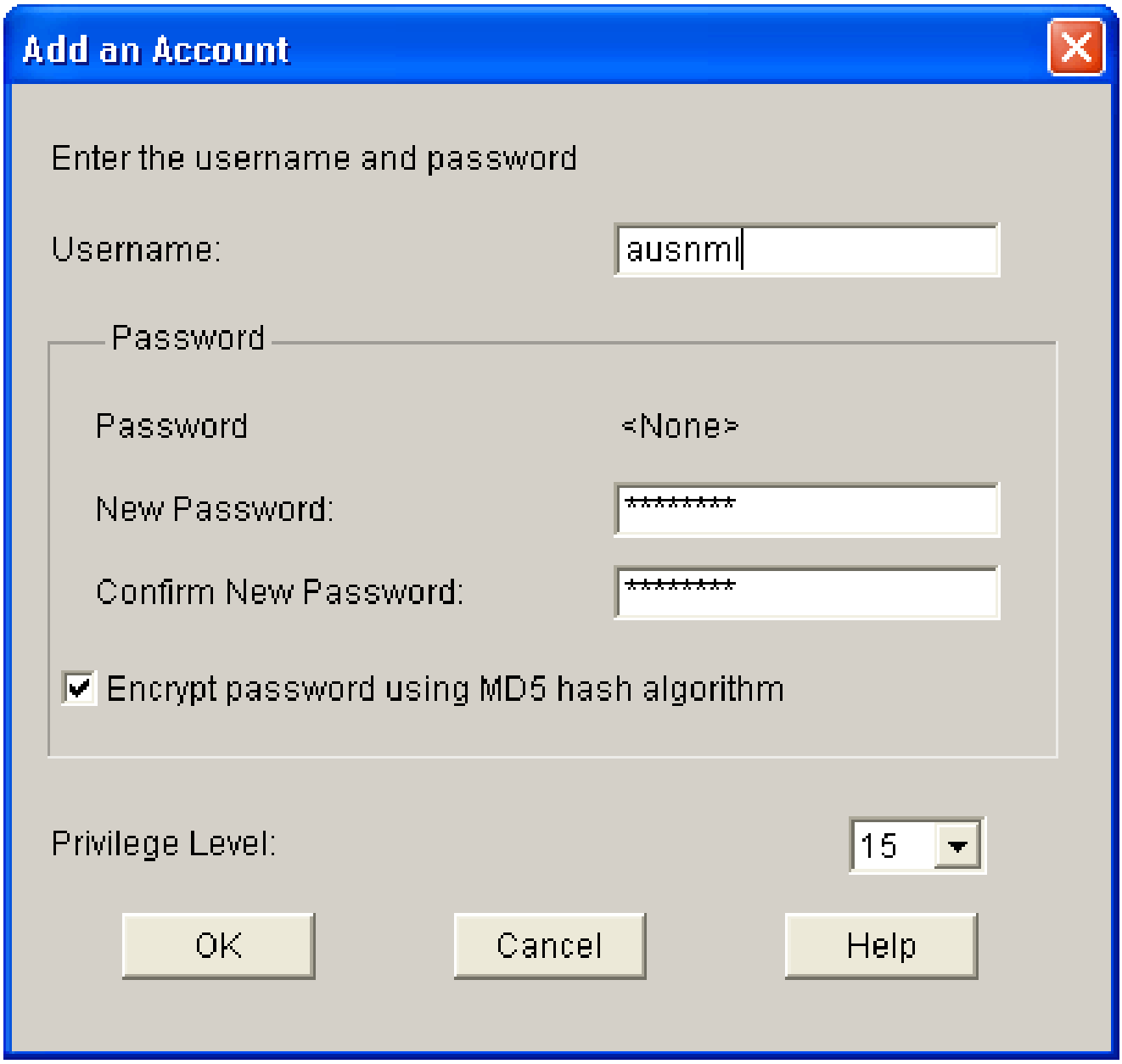
Conclua estas etapas para configurar o banco de dados de usuários para usuários do SVC:

1. Após concluir a Etapa 2, clique no botão de opção Locally on this router localizado na caixa de diálogo User Authentication do WebVPN Wizard.



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

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



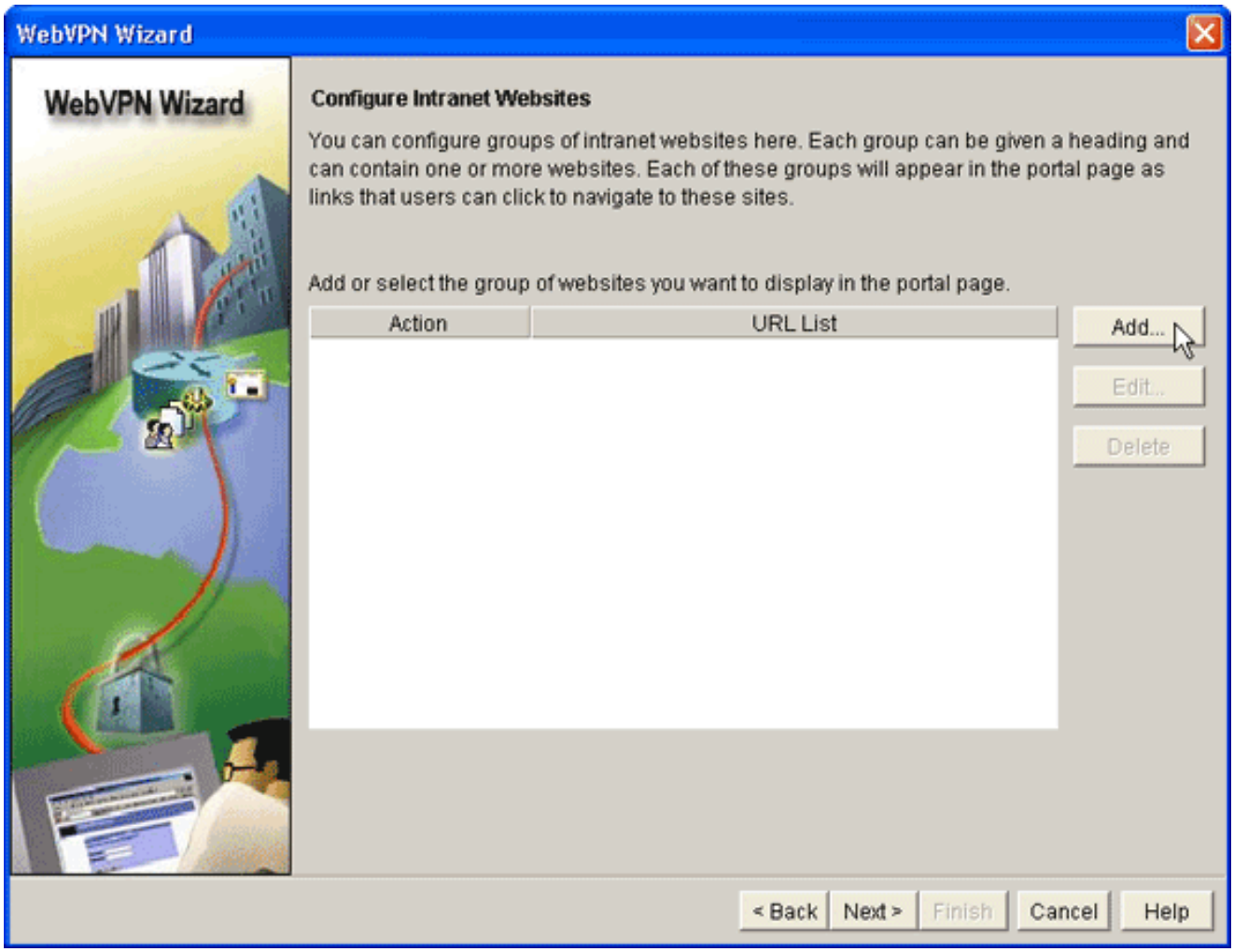
3. Clique em OK e adicione usuários a mais conforme o necessário.
4. Depois de adicionar os usuários necessários, clique em Next e prossiga para o Passo 4.

Etapa 4. Configurar os recursos para expor aos usuários

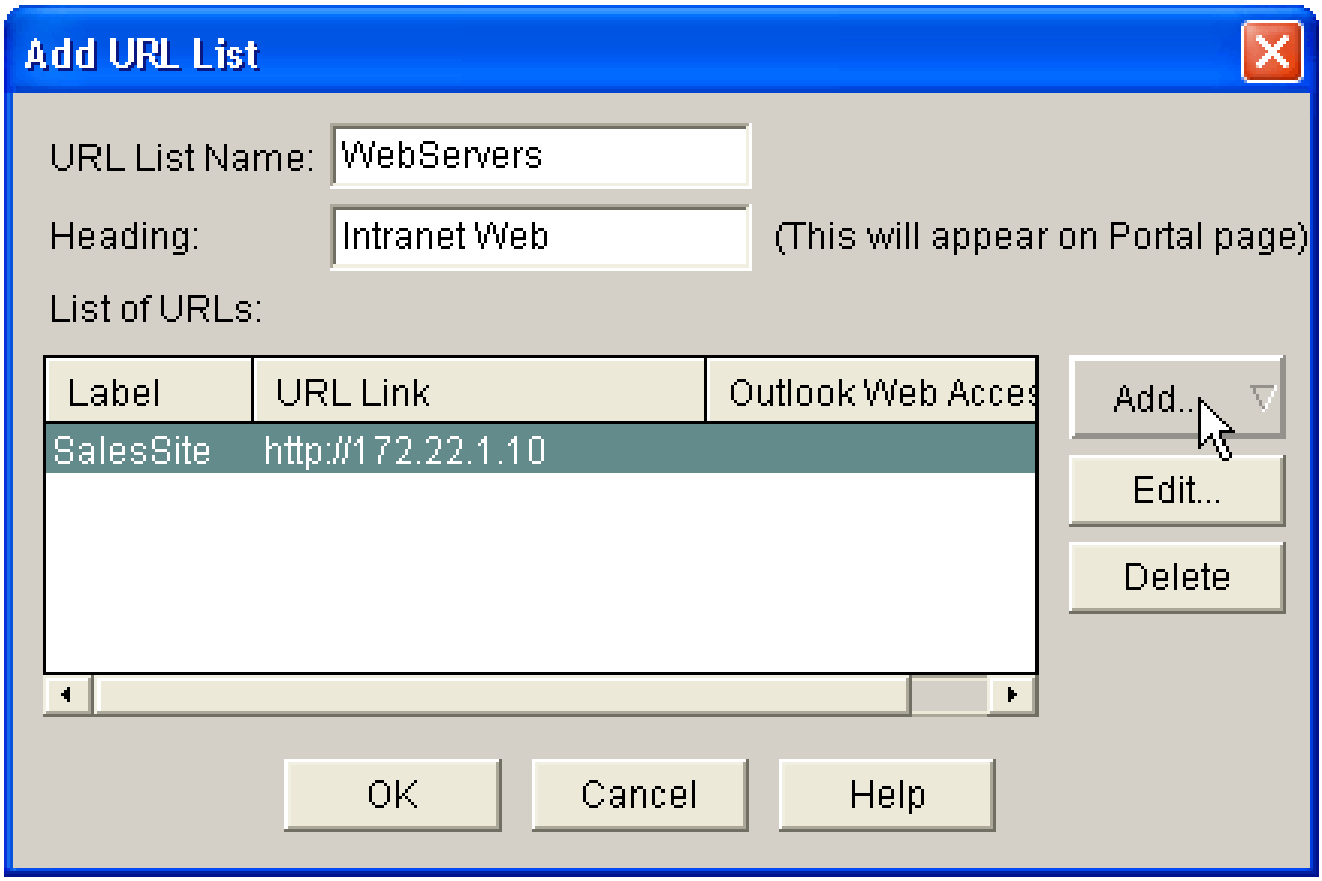
A caixa de diálogo Configure Intranet Websites WebVPN Wizard permite selecionar os recursos da intranet que você deseja expor aos seus clientes SVC.

Conclua estas etapas para configurar os recursos a serem expostos aos usuários:

1. Após concluir a Etapa 3, clique no botão Add localizado na caixa de diálogo Configure Intranet Websites.



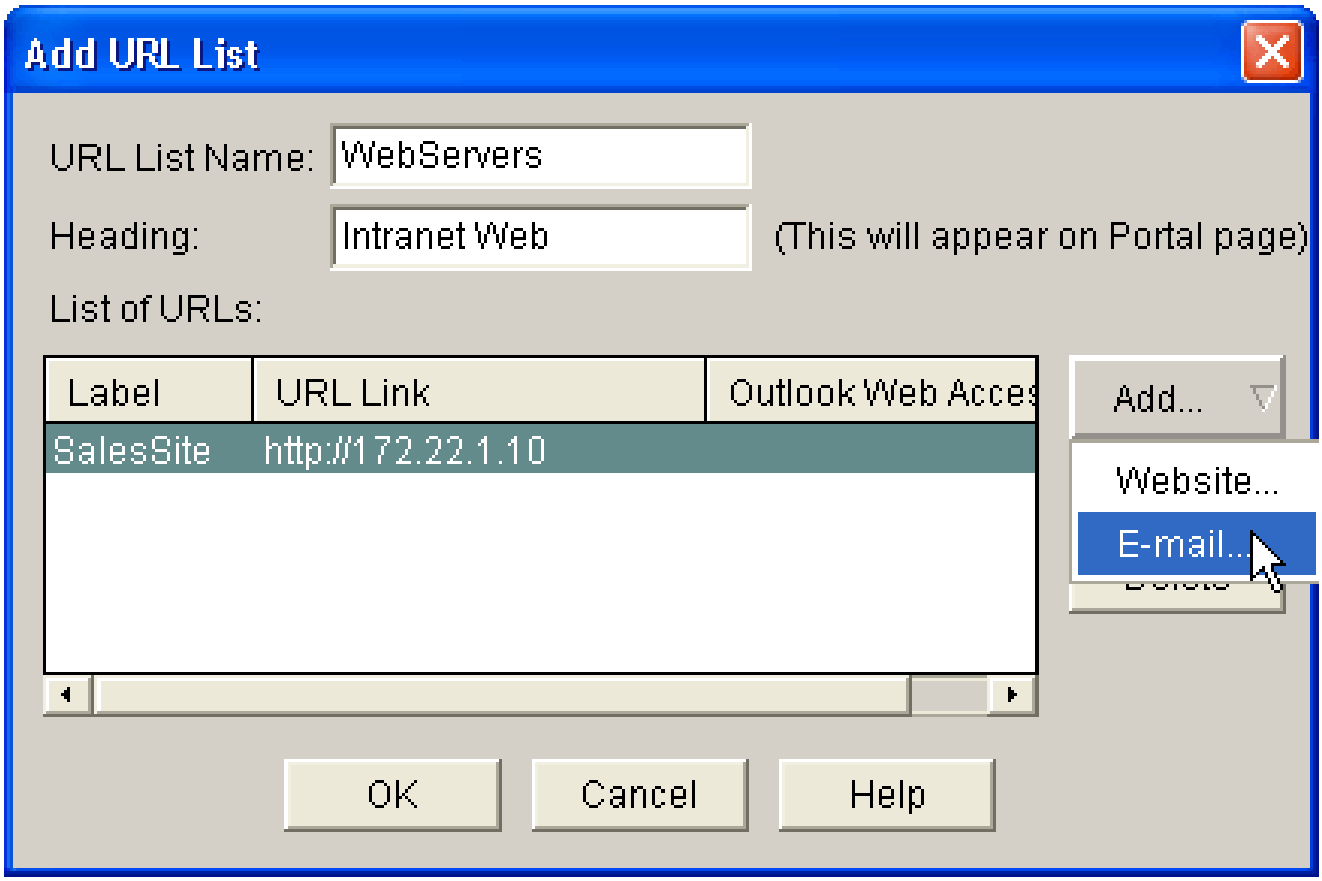
2. Insira um nome de lista de URL e, em seguida, insira um cabeçalho.



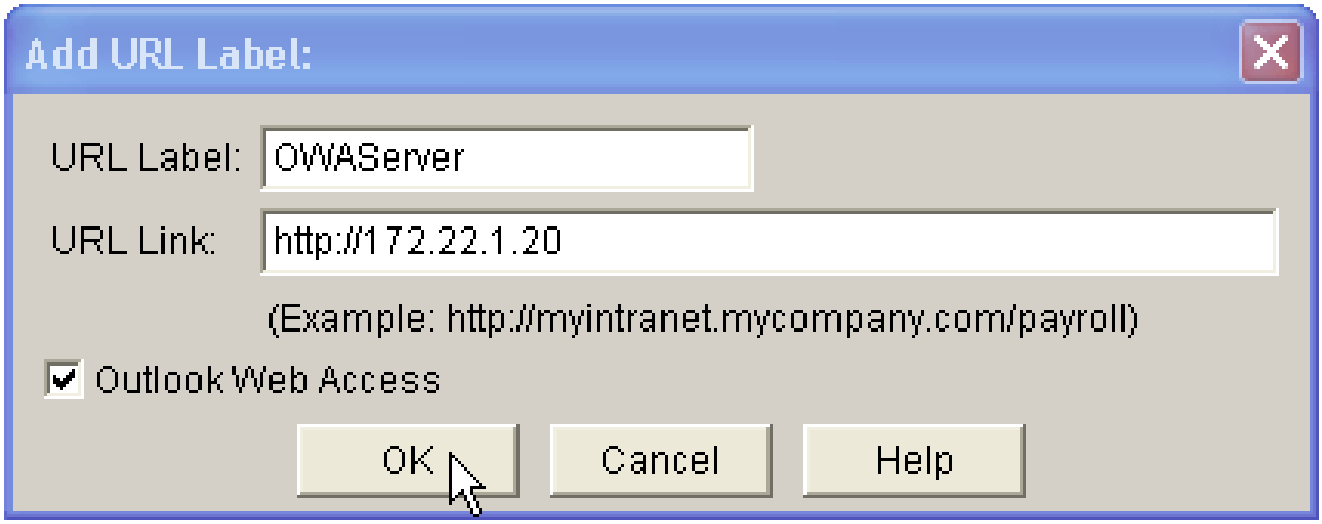
3. Clique em Adicionar e escolha Site para adicionar os sites que você deseja expor a este cliente.

4. Insira a URL e as informações do link e clique em OK.

5. Para adicionar acesso aos servidores Exchange do OWA, clique em Adicionar e escolha E-mail.

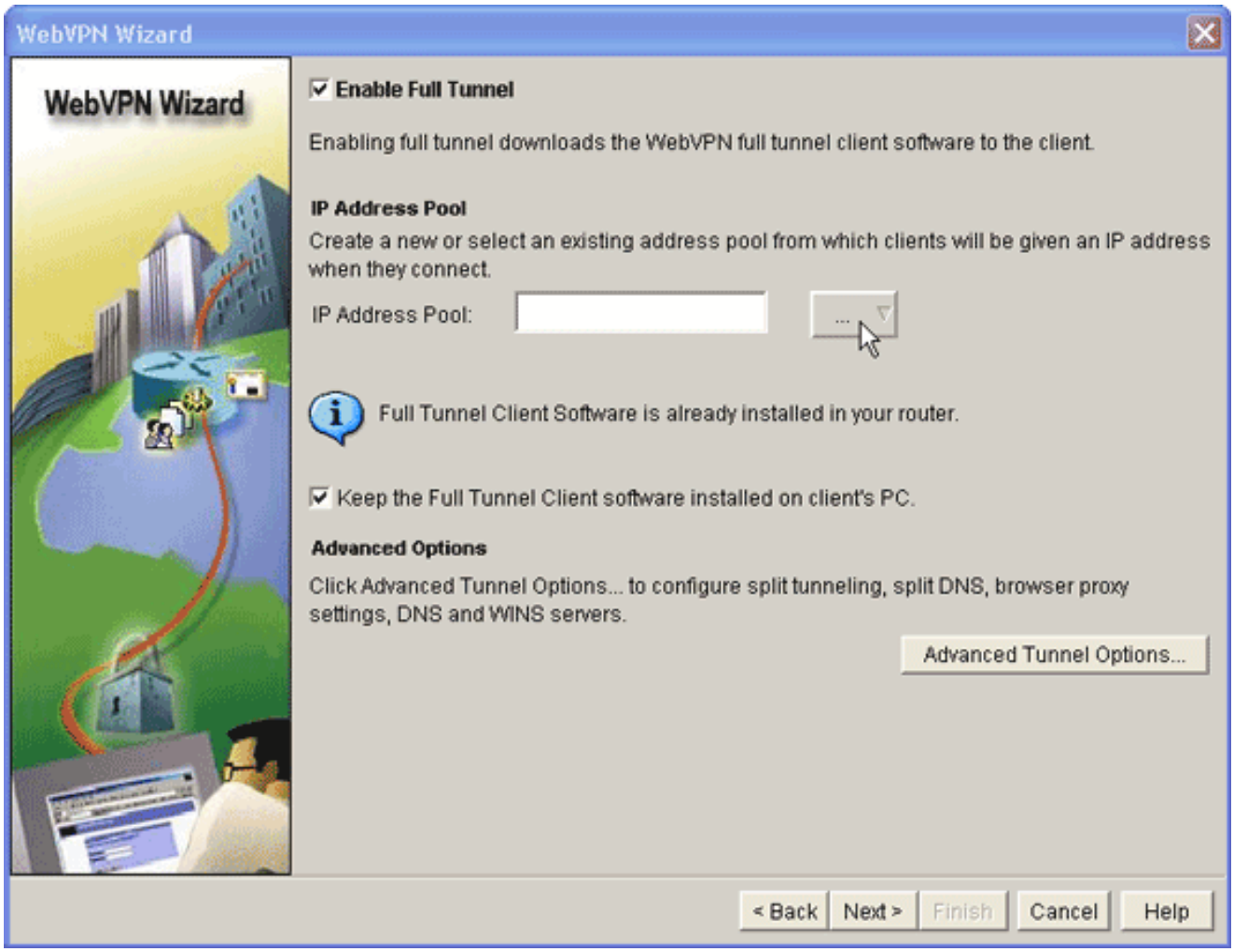


6. Marque a caixa de seleção Outlook Web Access, insira o rótulo da URL e as informações de link e clique em OK.

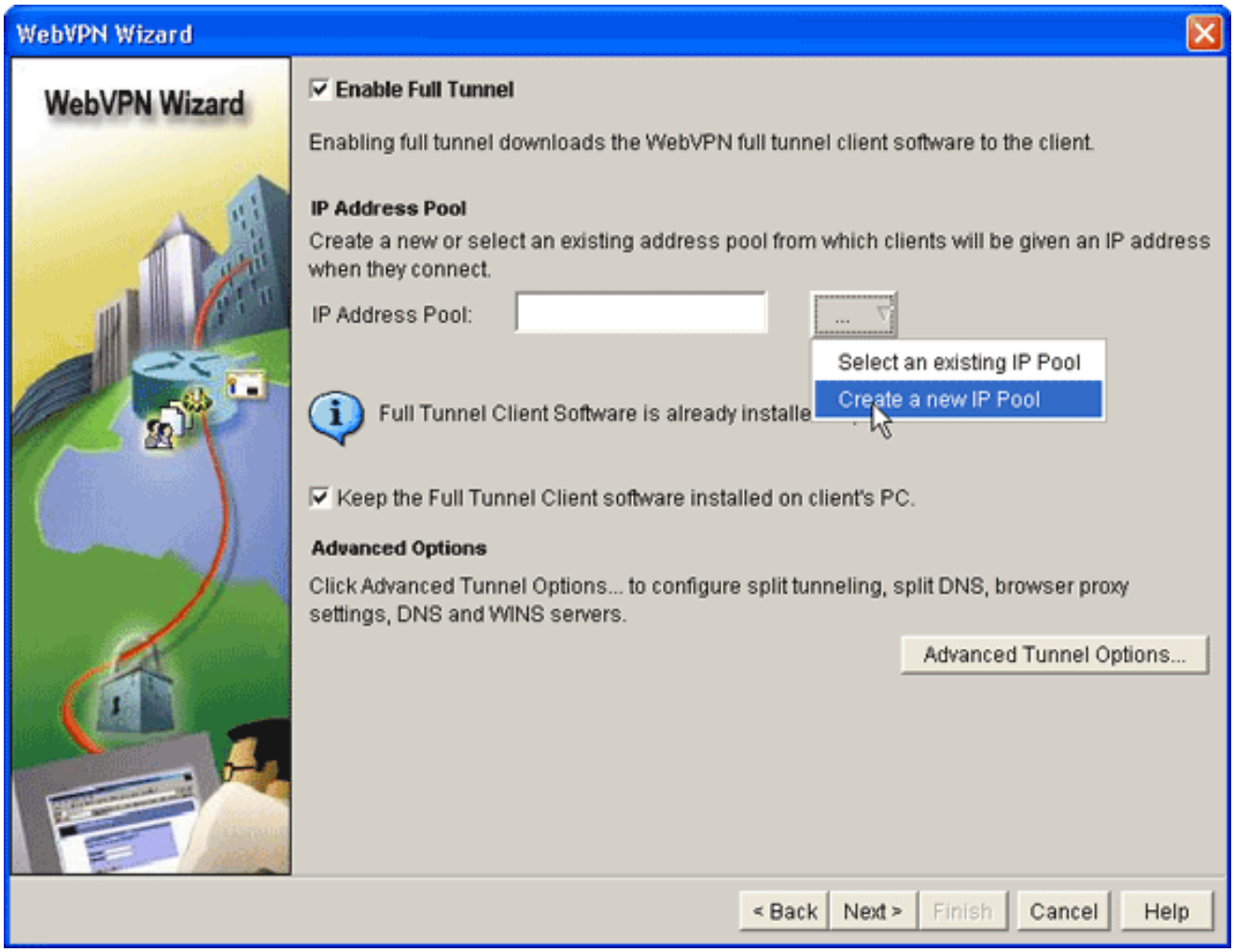


7. Depois de adicionar os recursos desejados, clique em OK e em Avançar.

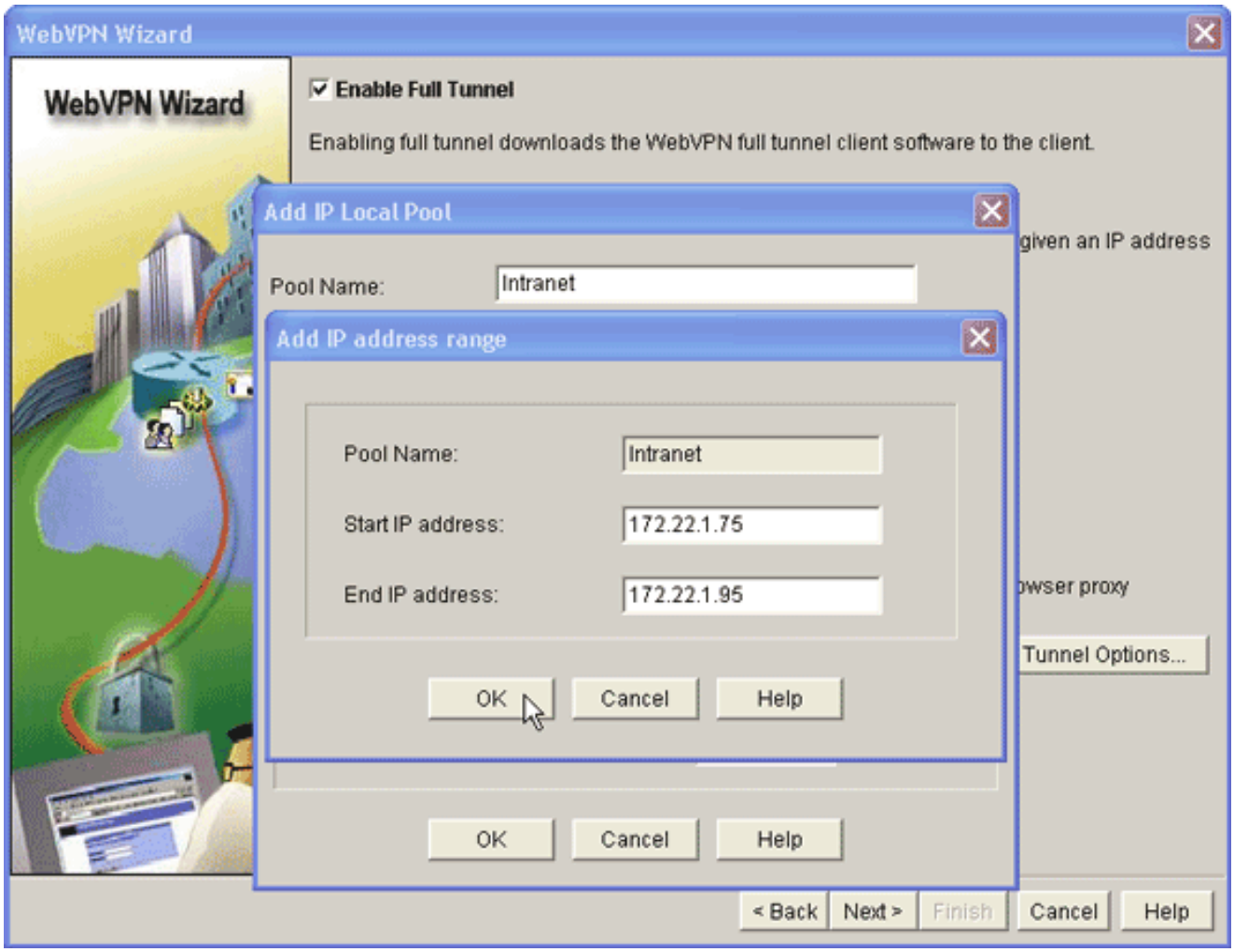
   A caixa de diálogo de túnel completo do Assistente WebVPN é exibida.



8. Certifique-se de que a caixa de verificação Enable Full Tunnel esteja marcada.
9. Crie um pool de endereços IP que os clientes deste contexto WebVPN possam usar. O pool de endereços deve corresponder aos endereços disponíveis e roteáveis em sua intranet.
10. Clique nas reticências (...) ao lado do campo IP Address Pool e escolha Create a new IP pool.



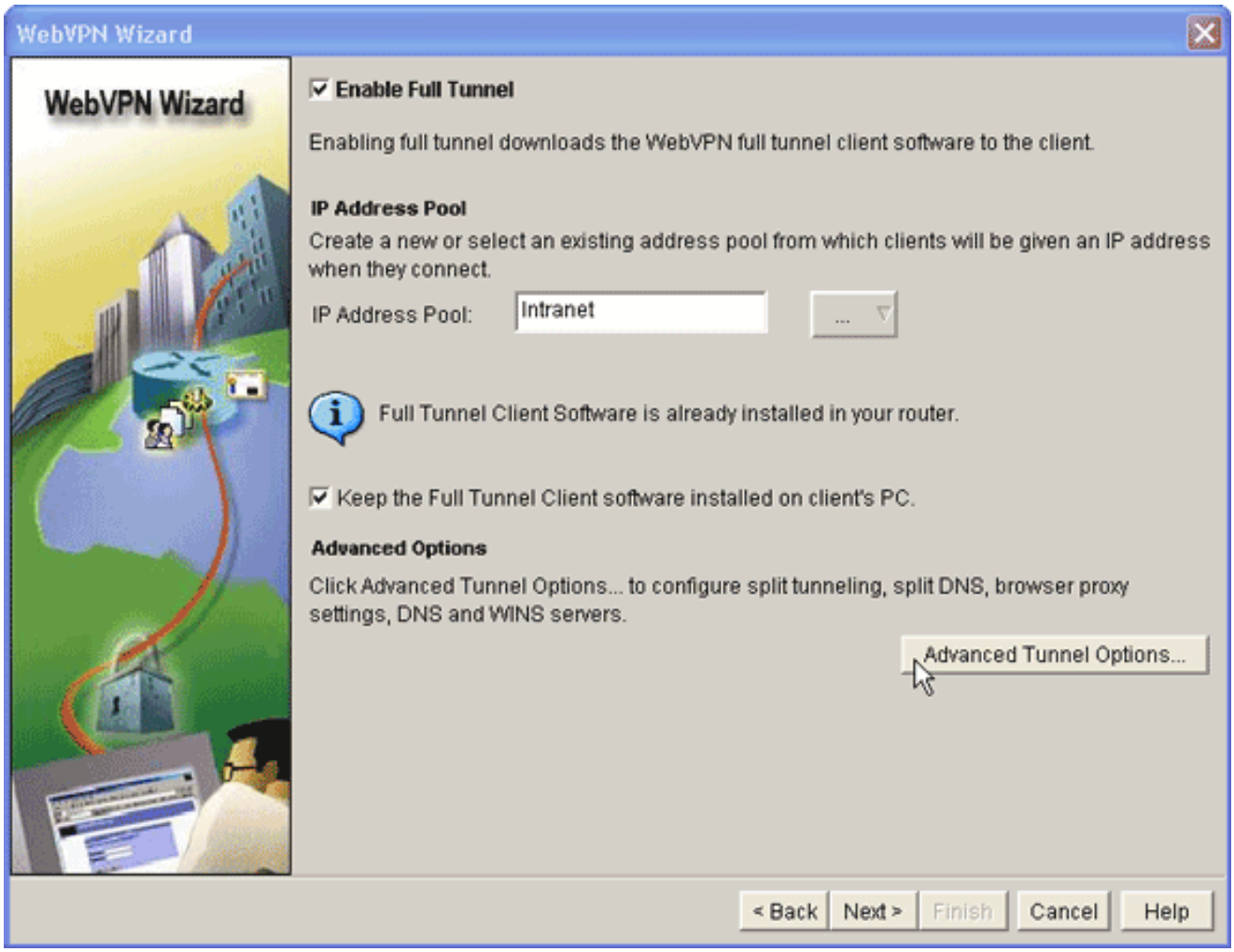
11. Na caixa de diálogo Add IP Local Pool, digite um nome para o pool e clique em Add.



12. Na caixa de diálogo Add IP address range (Adicionar intervalo de endereços IP), insira o intervalo de pool de endereços para os clientes SVC e clique em OK.

    Observação: o pool de endereços IP deve estar em um intervalo de uma interface diretamente conectada ao roteador. Se quiser usar um intervalo de pool diferente, você pode criar um endereço de loopback associado ao novo pool para satisfazer esse requisito.

13. Click OK.

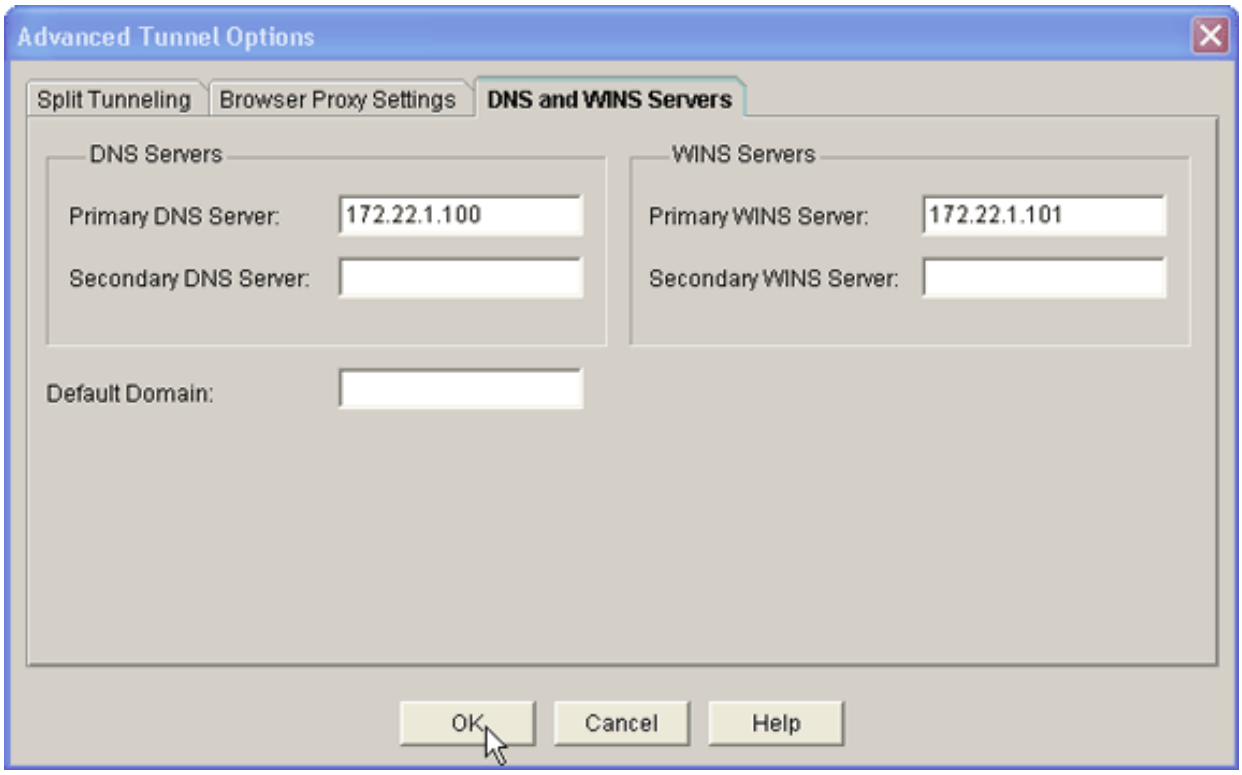


14. Se desejar que seus clientes remotos armazenem permanentemente uma cópia do SVC, clique na caixa de seleção Keep the Full Tunnel Client Software installed on client's PC. Desmarque essa opção para exigir que o cliente baixe o software SVC sempre que um cliente se conectar.

15. Configure opções de túnel avançadas, como encapsulamento dividido, DNS dividido, configurações de proxy do navegador e servidores DNS e WNS. A Cisco recomenda que você configure pelo menos os servidores DNS e WINS.

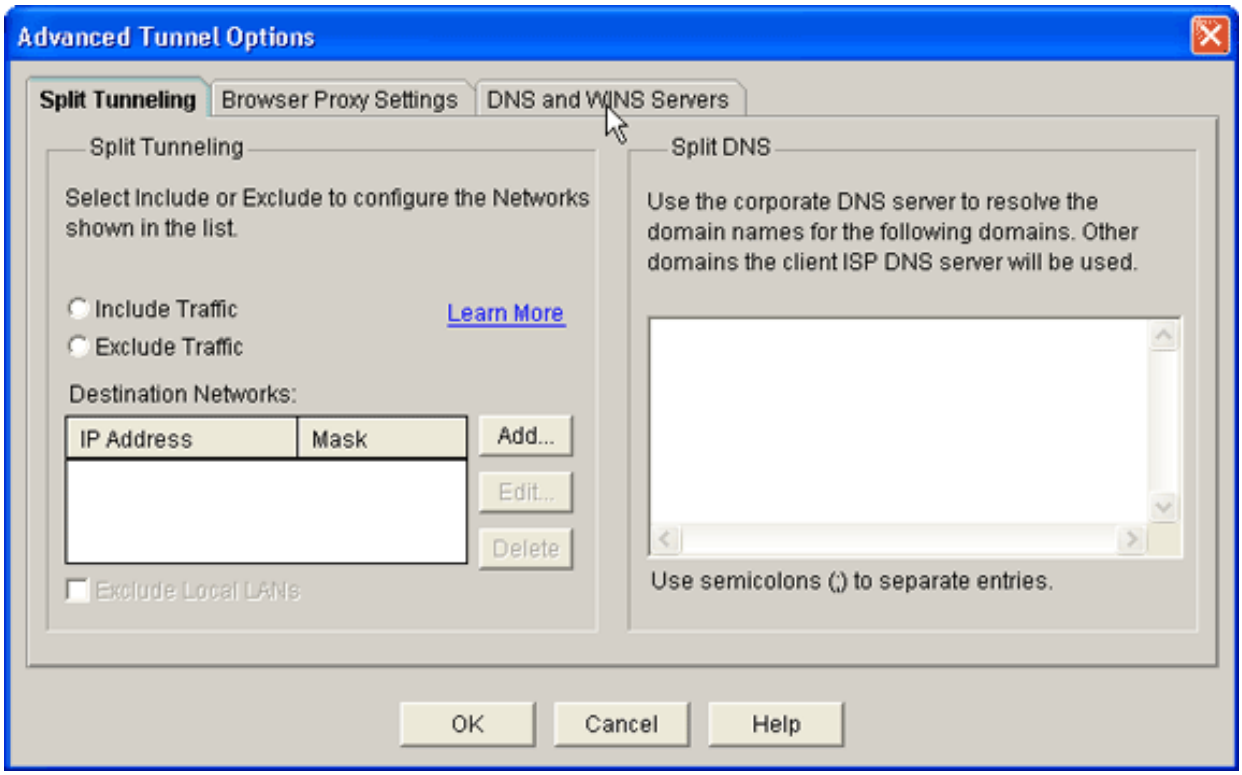
    Para configurar opções avançadas do túnel, conclua estes passos:

    a. Clique no botão >Advanced Tunnel Options.



b. Clique na guia DNS and WINS Servers e insira os endereços IP primários dos servidores DNS e WINS.

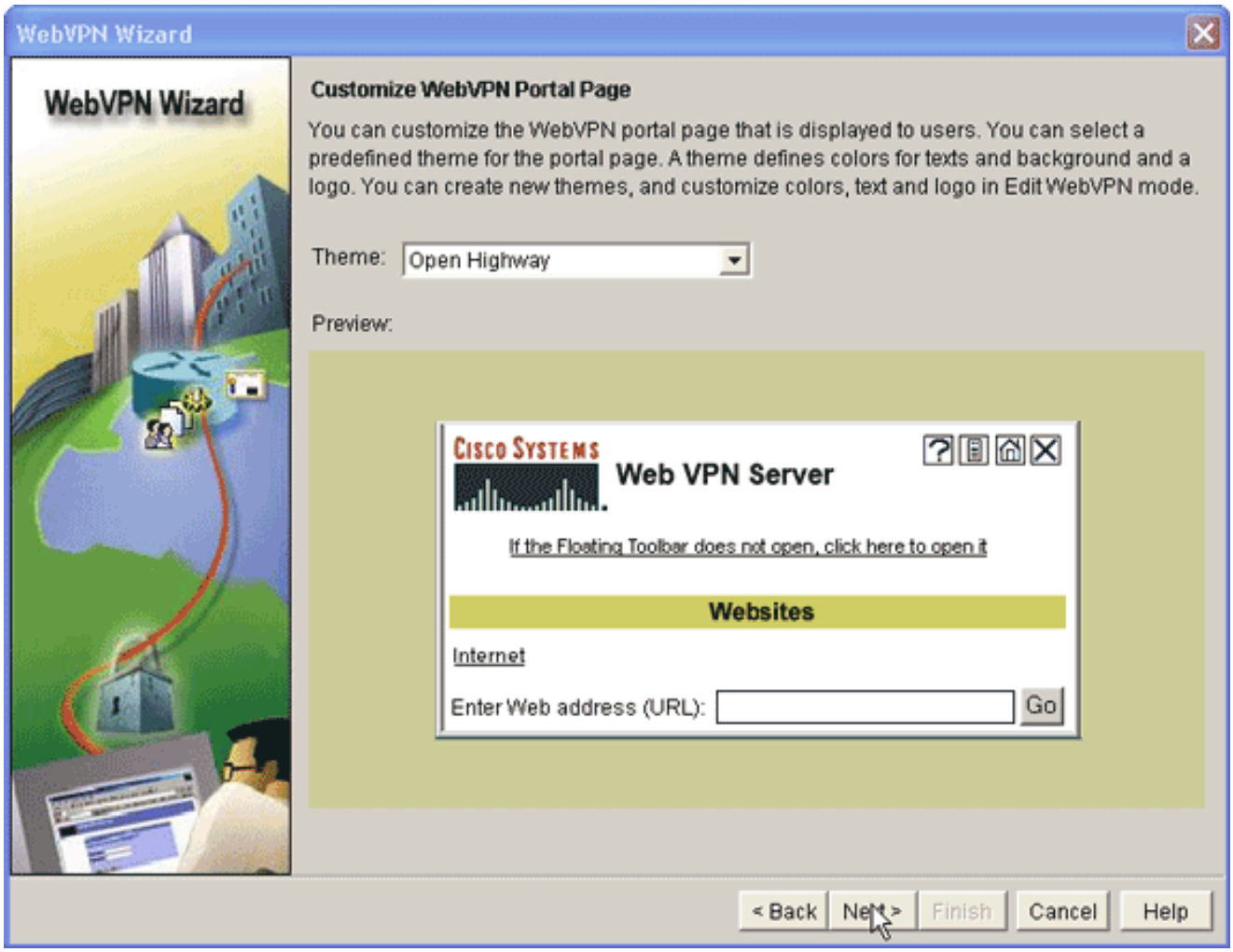
c. Para configurar o tunelamento dividido e as configurações de proxy do navegador, clique na guia Tunelamento dividido ou Configurações de proxy do navegador.



16. Após configurar as opções necessárias, clique Next.

17. Personalize a página do portal WebVPN ou selecione os valores padrão.

A página Personalizar portal WebVPN permite personalizar como a página do portal WebVPN aparece para seus clientes.

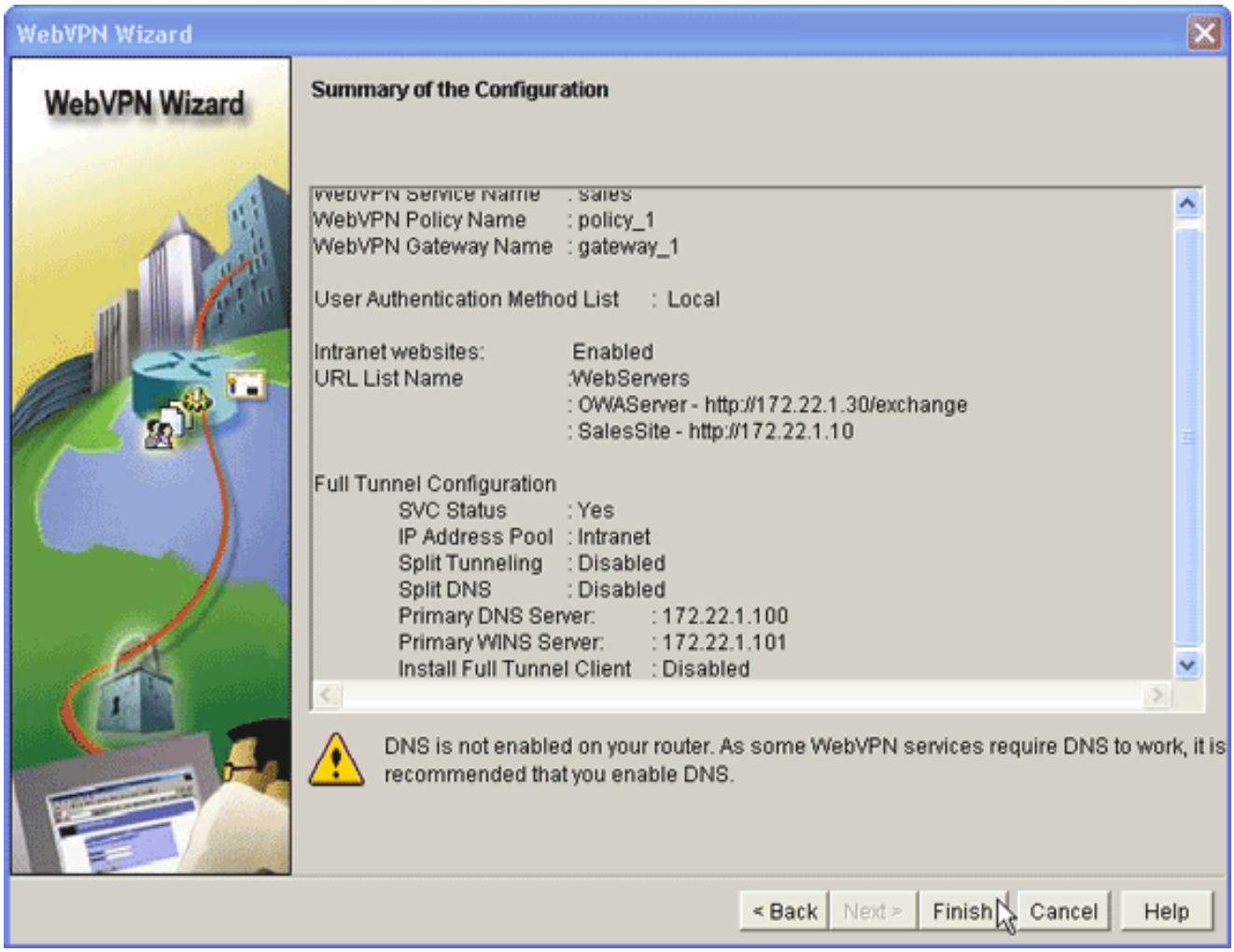


18. Depois de configurar a página do portal WebVPN, clique em Next, clique em Finish e, em seguida, clique em OK.

    O WebVPN Wizard envia comandos de tour ao roteador.

19. Clique em OK para salvar sua configuração.

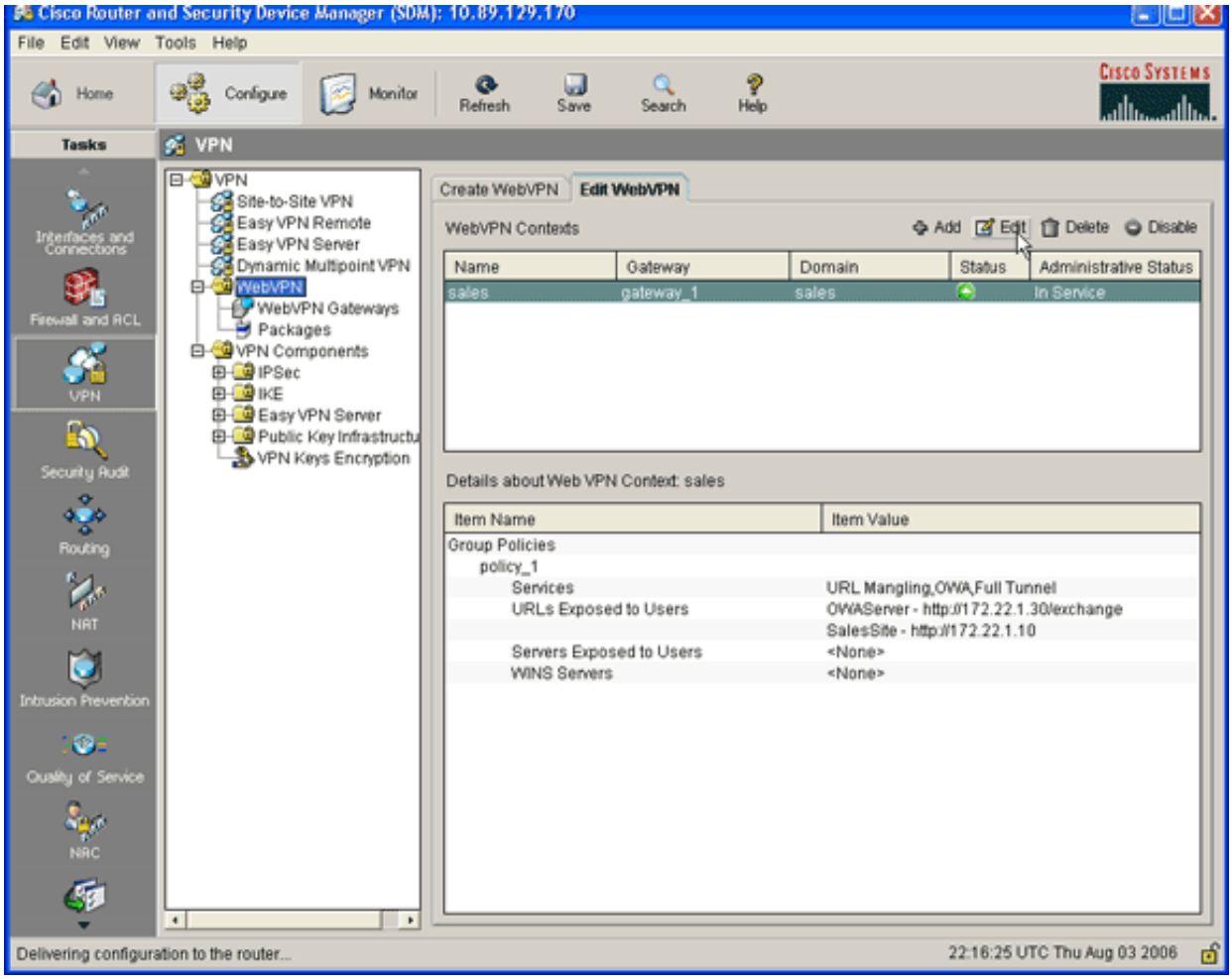
    Observação: se você receber uma mensagem de erro, a licença WebVPN pode estar incorreta. Um exemplo de mensagem de erro é mostrado nesta imagem:



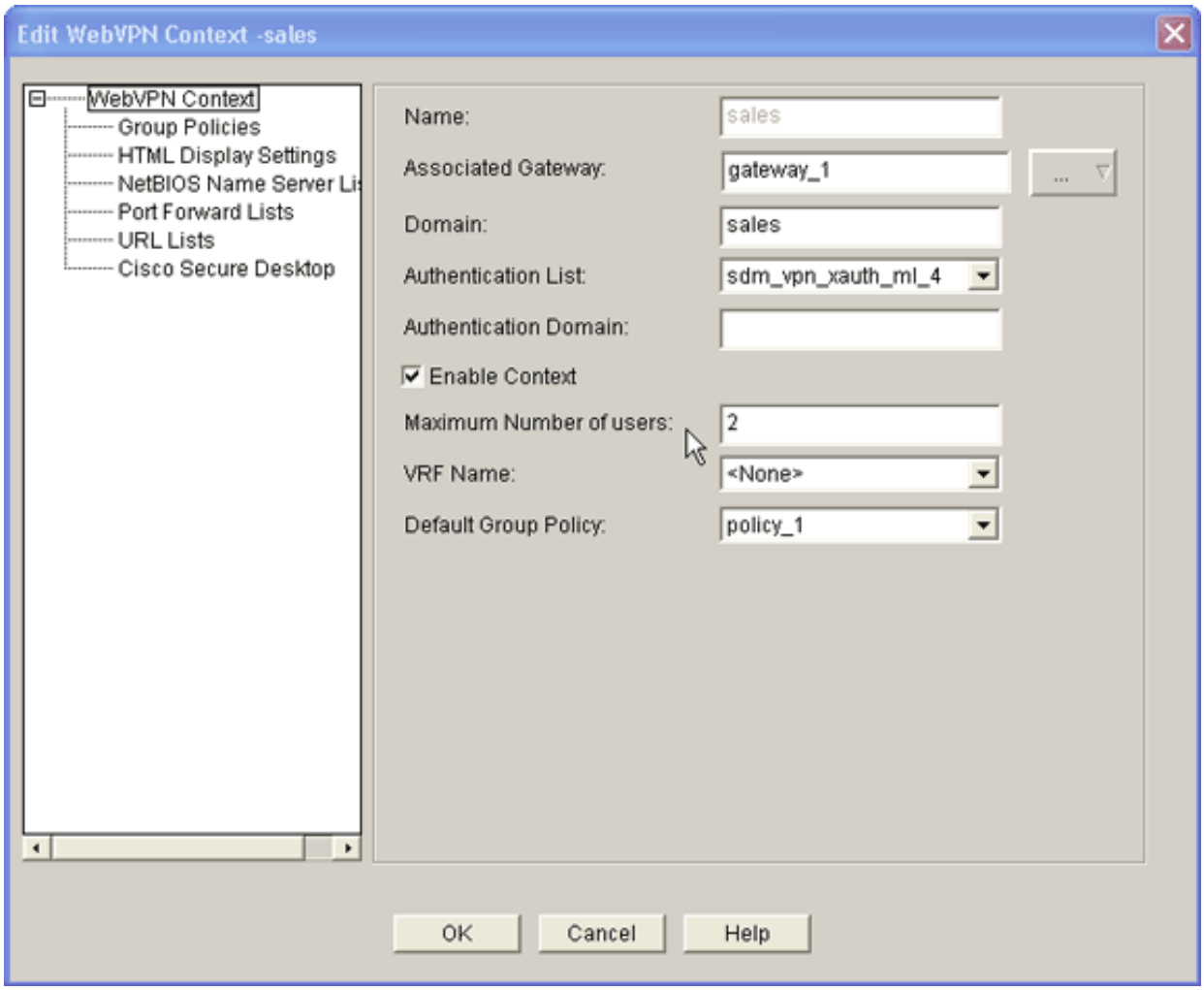
Para corrigir um problema de licença, conclua estes passos:

a. Clique em Configure e clique em VPN.

b. Expanda WebVPN e clique na guia Edit WebVPN.



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



d. No campo do Maximum Number of users, insira o número correto de usuários para sua licença.

e. Clique em OK e, em seguida, clique em OK.

Seus comandos são gravados no arquivo de configuração.

f. 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
<#root> 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, insira http://192.168.0.37/sales em um navegador da Web do cliente habilitado para SSL.

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.

Observação: a Output Interpreter Tool (somente 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 esse 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.

Observação: o uso dos comandos debug pode afetar adversamente o 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.