Configurar o Cisco IOS SSL VPN Thin-Client (WebVPN) com SDM

Contents

Introduction

A tecnologia de VPN SSL Thin-Client pode ser usada para permitir acesso seguro para aplicativos que usam portas estáticas. Exemplos são Telnet (23), SSH (22), POP3 (110), IMAP4 (143) e SMTP (25). O Thin-Client pode ser orientado por usuários, por políticas ou ambos. O acesso pode ser configurado usuário por usuário ou podem ser criadas políticas de grupo que incluem um ou mais usuários. A tecnologia de VPN SSL pode ser configurada em três modos principais: VPN SSL sem cliente (WebVPN), VPN SSL thin-client (encaminhamento de portas) e Cliente VPN SSL (modo de túnel completo SVC).

1. VPN SSL sem cliente (WebVPN):

Um cliente remoto precisa apenas de um navegador da Web habilitado para SSL para acessar servidores da Web habilitados para http ou https na LAN corporativa. O acesso também está disponível para procurar arquivos do Windows com o CIFS (Common Internet File System). Um bom exemplo de acesso http é o cliente Outlook Web Access (OWA).

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

2. VPN SSL Thin-Client (encaminhamento de portas)

Um cliente remoto deve baixar um miniaplicativo baseado em Java para acesso seguro de aplicativos TCP que usam números de porta estática. UDP não é suportado. Os exemplos incluem acesso a POP3, SMTP, IMAP, SSH e Telnet. O usuário precisa de privilégios administrativos locais porque as alterações são feitas em arquivos na máquina local. Esse método de VPN SSL não funciona com aplicativos que usam atribuições de porta dinâmicas, por exemplo, vários aplicativos FTP.

3. Cliente VPN SSL (Modo de túnel completo SVC):

O SSL VPN Client faz o download de um pequeno cliente para a estação de trabalho remota e permite acesso completo e seguro aos recursos na rede corporativa interna. O SVC pode ser baixado permanentemente para a estação remota ou pode ser removido após o término da sessão segura.

Consulte SSL VPN Client (SVC) no IOS usando o Exemplo de Configuração de SDM para saber mais sobre o SSL VPN Client.

Este documento demonstra uma configuração simples para o Thin-Client SSL VPN em um roteador Cisco IOS®. A VPN SSL Thin-Client é executada nestes roteadores Cisco IOS:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 e 2851 Series Routers
- Roteadores Cisco séries 3725, 3745, 3825, 3845, 7200 e 7301

Prerequisites

Requirements

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

Requisitos para o roteador Cisco IOS

- Qualquer um dos roteadores listados carregados com SDM e uma imagem avançada do IOS versão 12.4(6)T ou posterior
- Estação de gerenciamento carregada com SDMA Cisco envia novos roteadores com uma cópia pré-instalada do SDM. Se o roteador não tiver o SDM instalado, você poderá obter o software em Download de software - Cisco Security Device Manager. Você deve possuir uma conta CCO com um contrato de serviço. Consulte Configurar o Roteador com Gerenciador de Dispositivos de Segurança para obter instruções detalhadas.

Requisitos para computadores clientes

- Os clientes remotos devem ter privilégios administrativos locais; não é obrigatório, mas é altamente sugerido.
- Os clientes remotos devem ter Java Runtime Environment (JRE) versão 1.4 ou superior.
- Navegadores clientes remotos: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 ou Firefox 1.0
- Cookies ativados e pop-ups permitidos em clientes remotos

Componentes Utilizados

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

- Imagem do Cisco Advanced Enterprise Software 12.4(9)T
- Roteador de serviços integrados Cisco 3825
- Cisco Router and Security Device Manager (SDM) versão 2.3.1

The information in this document was created from the devices in a specific lab environment. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). If your network is live, make sure that you understand the potential impact of any command. Os endereços IP usados para essa configuração são provenientes do espaço de endereço RFC 1918. Eles não são legais na Internet.

Conventions

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

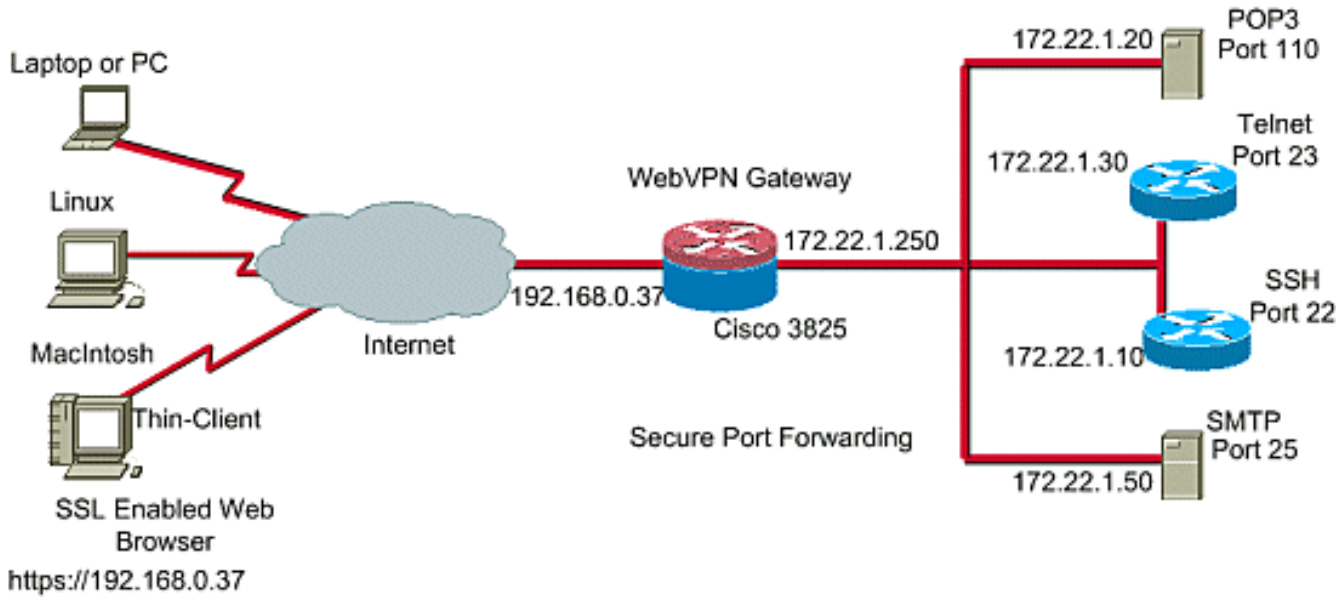
Configurar

Tarefa

Esta seção contém as informações necessárias para configurar os recursos descritos neste documento.

Diagrama de Rede

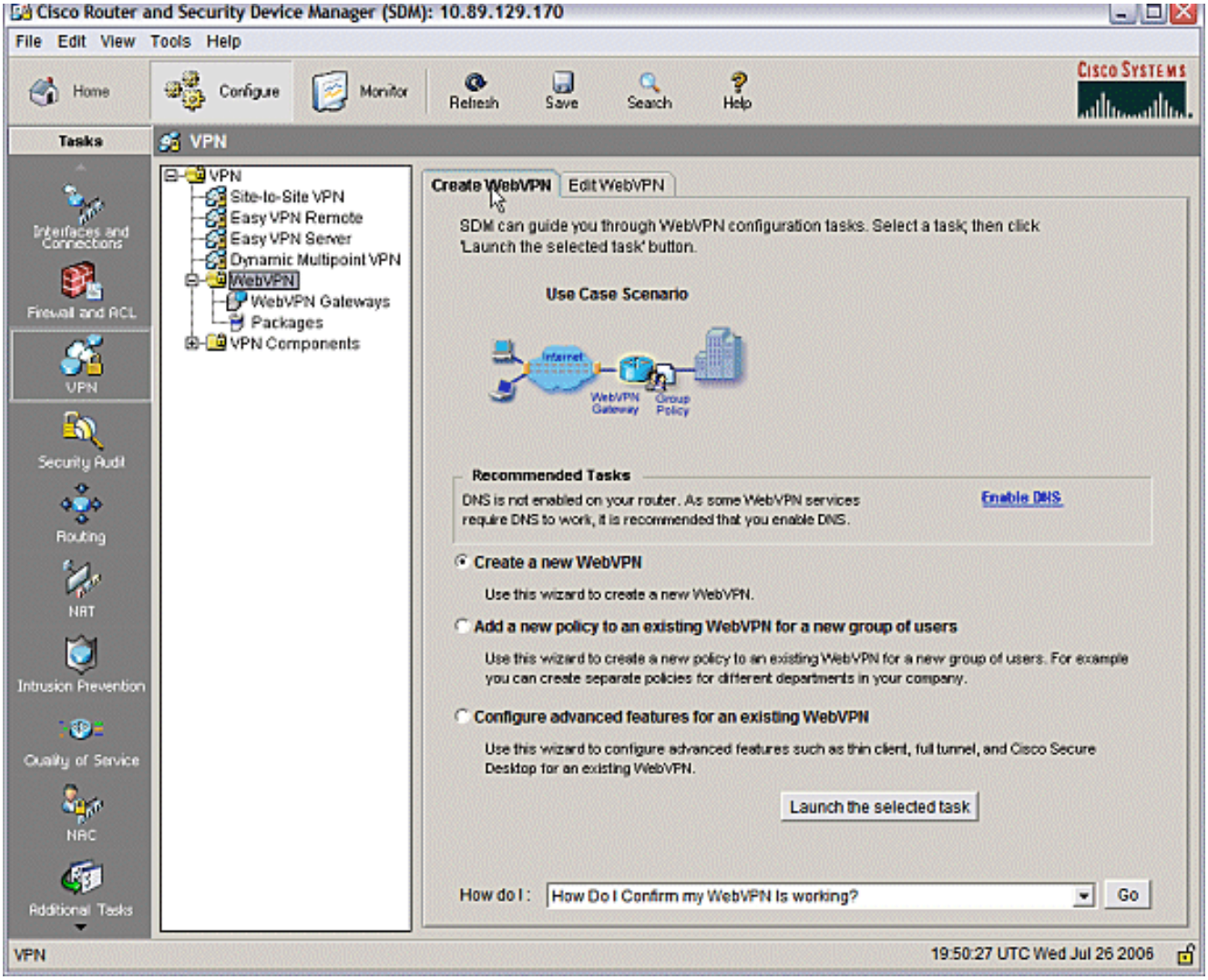
Este documento utiliza a seguinte configuração de rede:



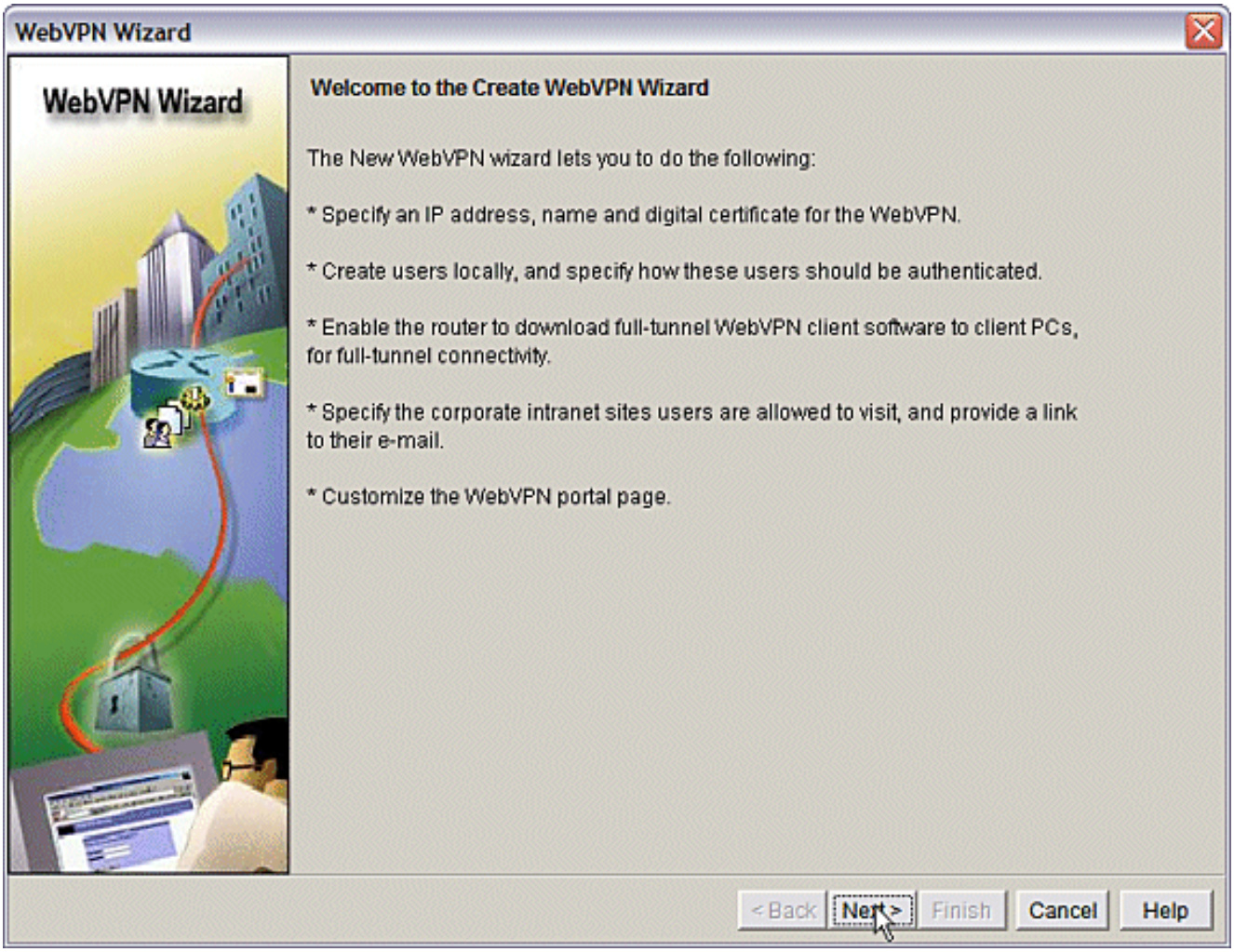
Configurar a VPN SSL Thin-Client

Use o Assistente fornecido na interface do Gerenciador de dispositivos de segurança (SDM) para configurar a VPN SSL Thin-Client no Cisco IOS ou configure-a na Interface de linha de comando (CLI) ou manualmente no aplicativo SDM. Este exemplo usa o Assistente.

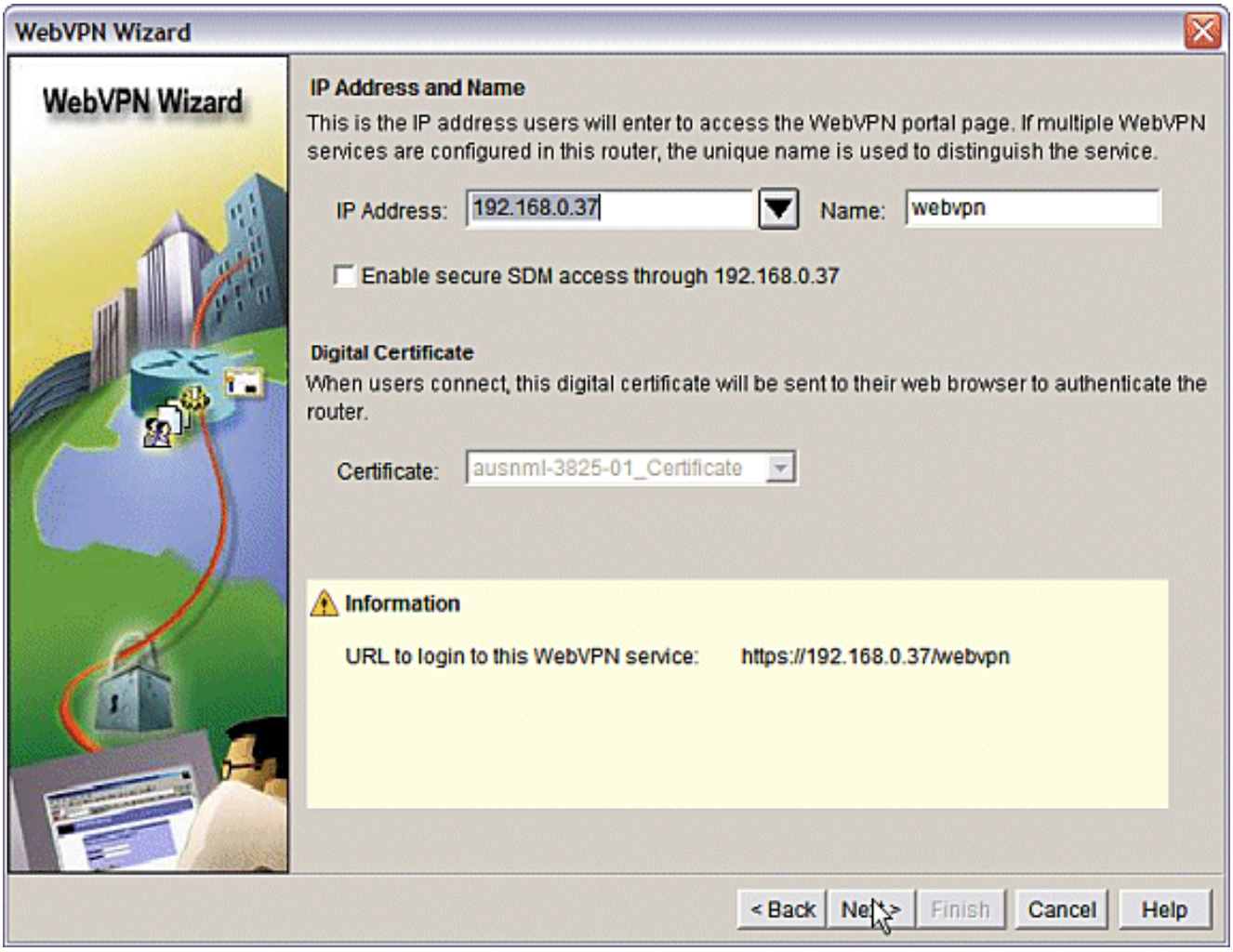
1. Escolha a guia **Configurar**.No painel de navegação, escolha **VPN > WebVPN**.Clique na guia **Create WebVPN**.Clique no botão de opção ao lado de **Create a new WebVPN**.Clique no botão **Iniciar a tarefa selecionada**.



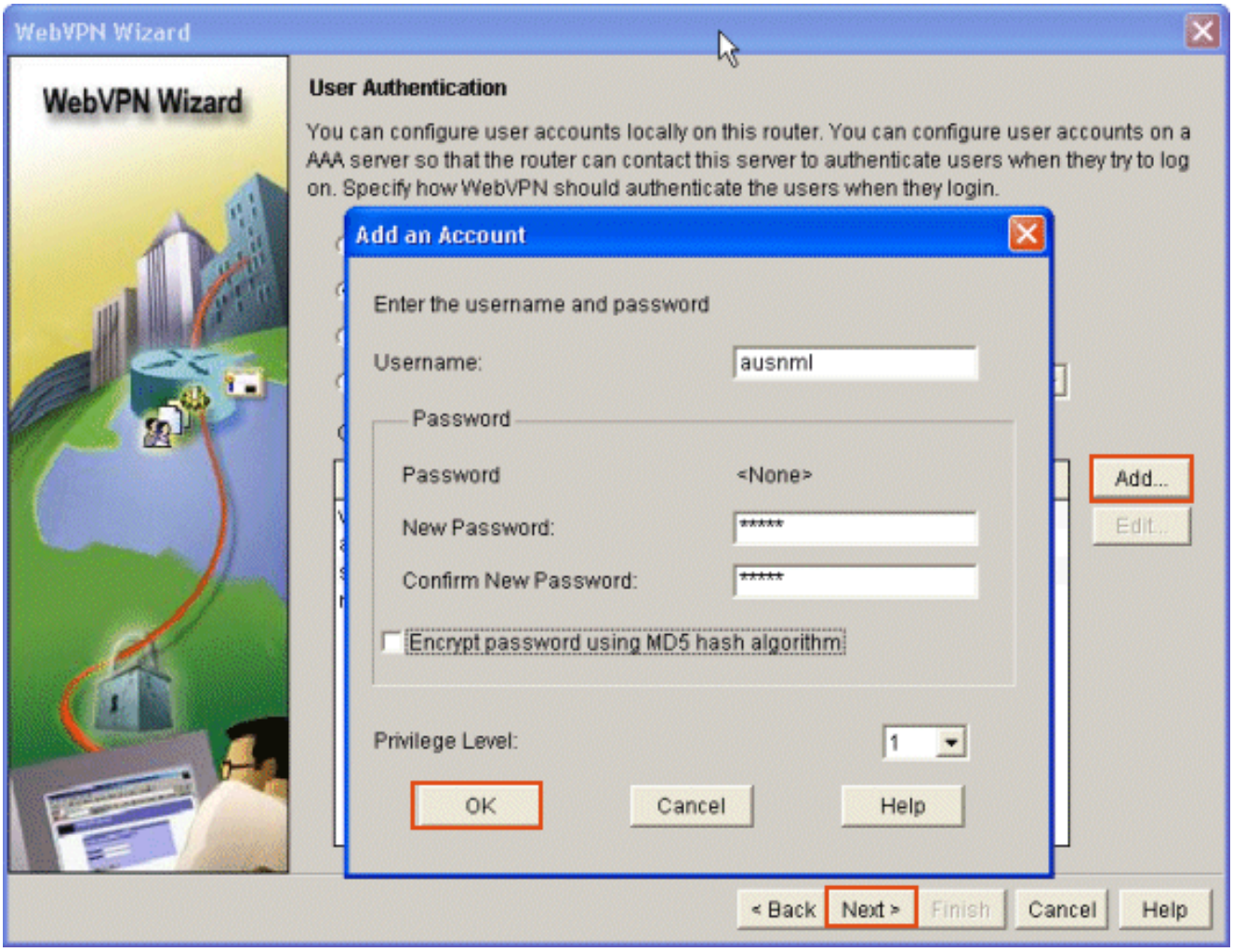
2. O WebVPN Wizard é iniciado. Clique em Next.



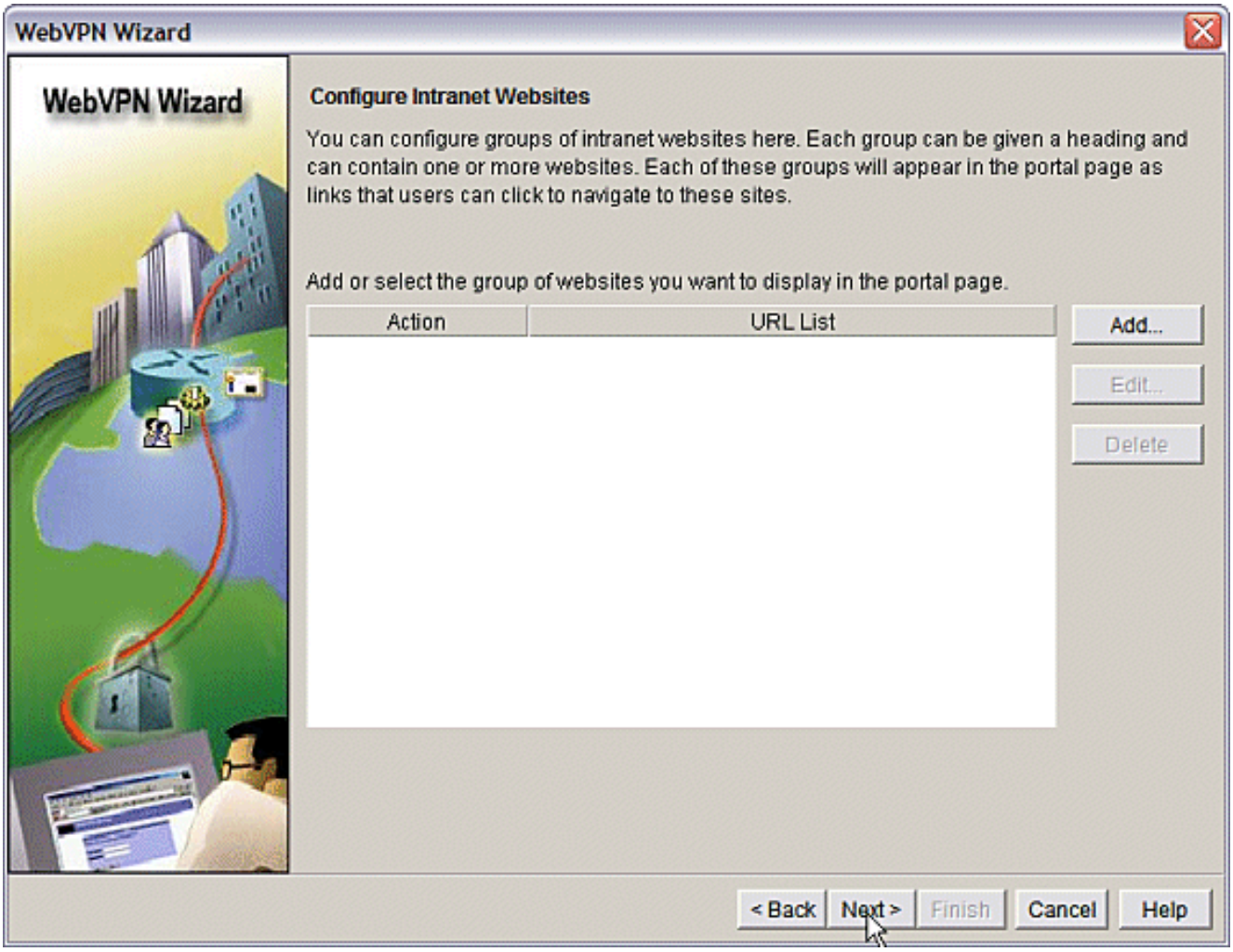
Insira o endereço IP e um nome exclusivo para este gateway WebVPN. Clique em Next.



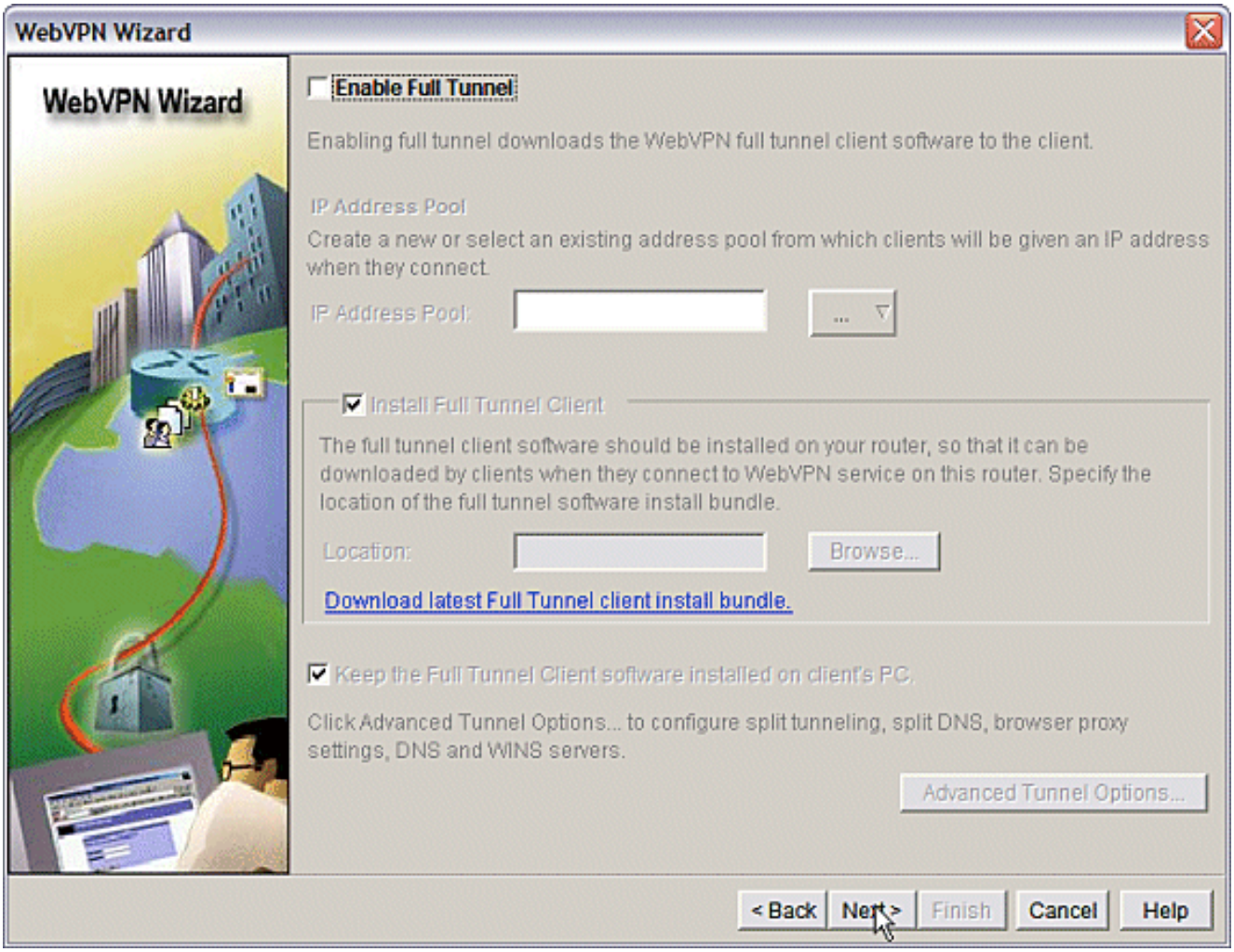
3. A tela Autenticação de usuário permite a oportunidade de fornecer a autenticação de usuários. Essa configuração usa uma conta criada localmente no roteador. Você também pode usar um servidor de Autenticação, Autorização e Auditoria (AAA).Para adicionar um usuário, clique em **Adicionar**.Digite as informações do usuário na tela Adicionar uma conta e clique em **OK**.Clique em **Next (Avançar)** na tela User Authentication (Autenticação de usuário).



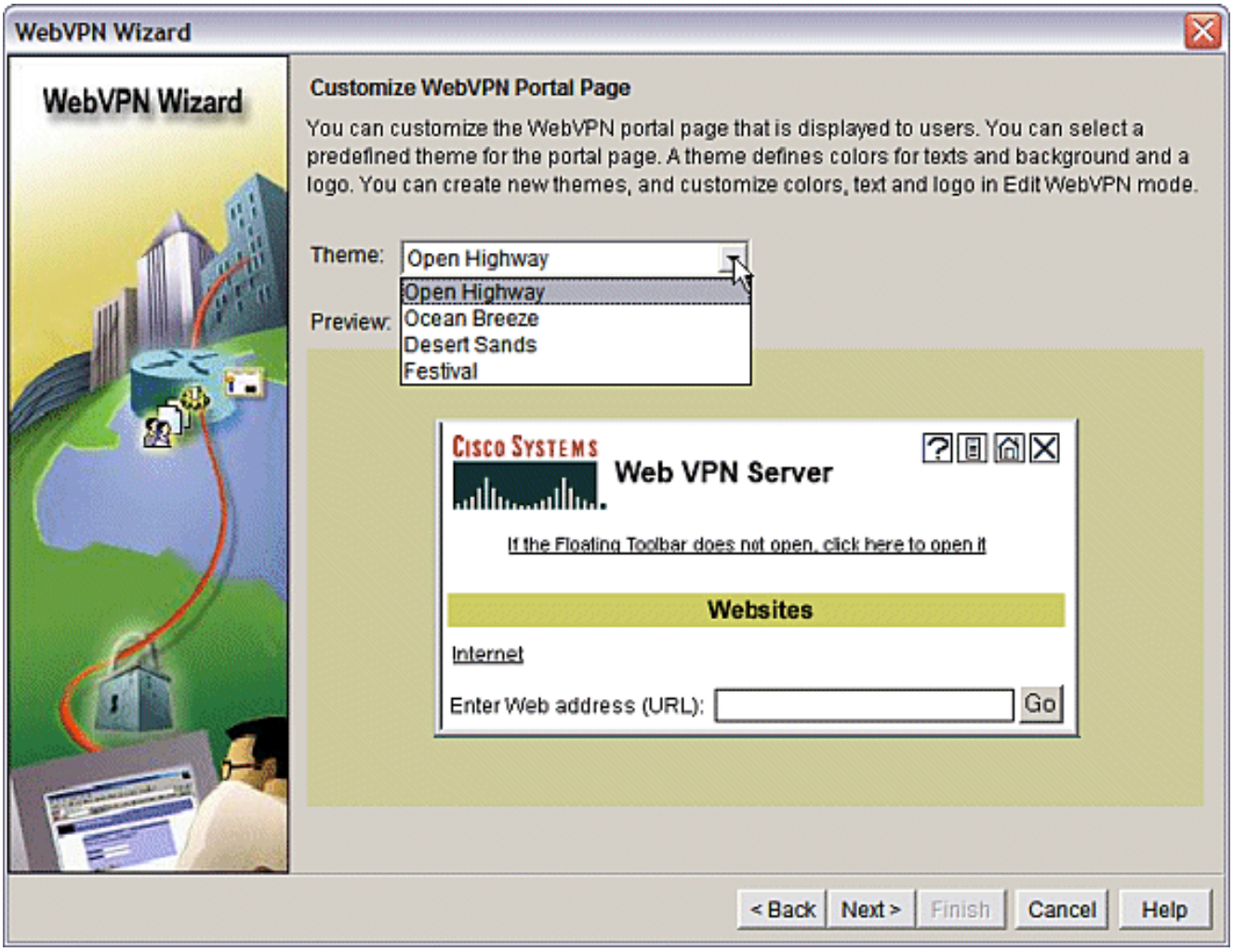
A tela WebVPN Wizard permite a configuração de sites da Intranet, mas essa etapa é omitida porque o Port-Forwarding é usado para esse acesso de aplicativo. Se quiser permitir acesso a sites, use as configurações de VPN SSL Cliente ou Cliente Completo, que não estão no escopo deste
documento.



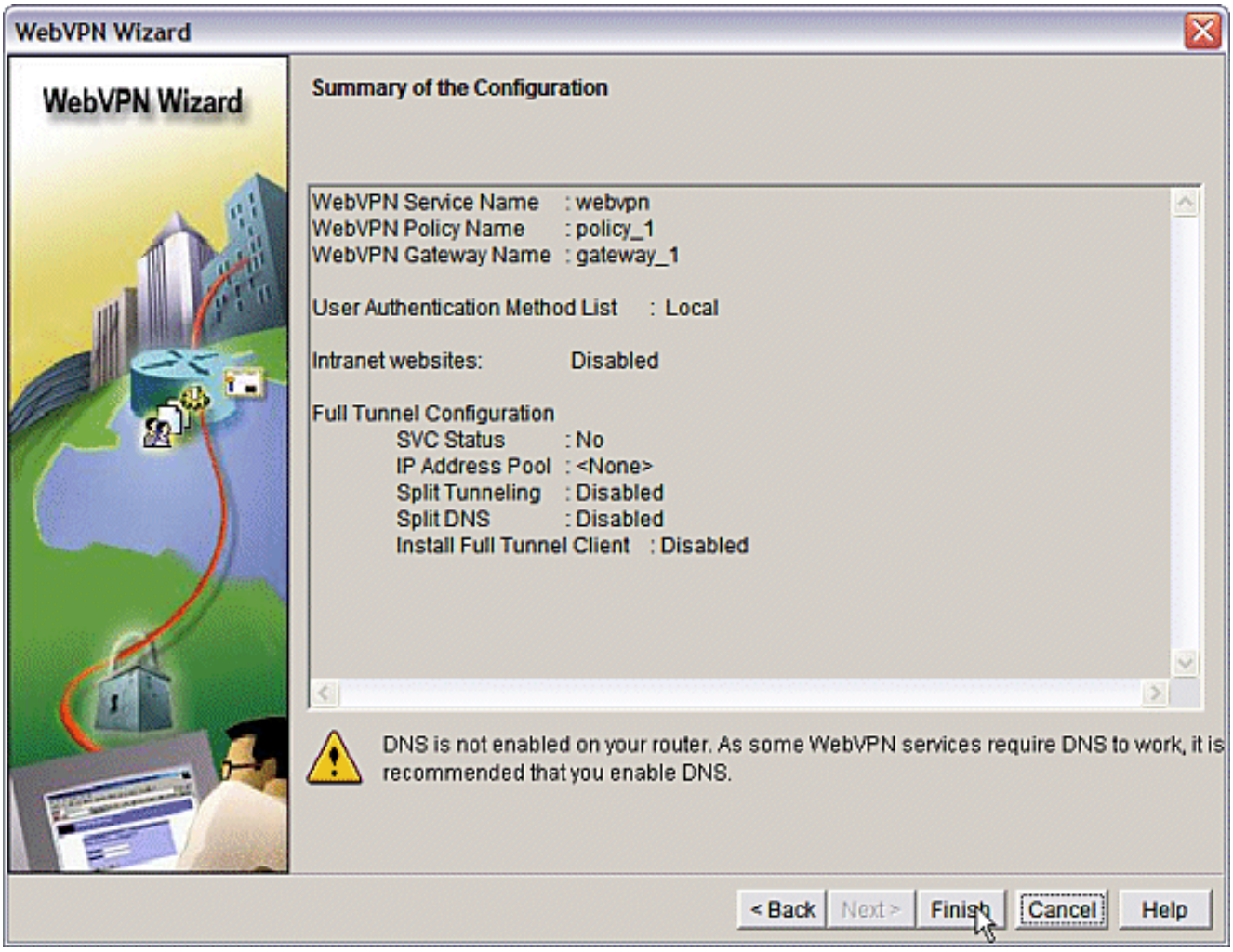
Clique em Next. O Assistente exibe uma tela que permite a configuração do cliente de Túnel Completo. Isso não se aplica ao Thin-Client SSL VPN (Port Forwarding).Desmarque **Ativar túnel completo**. Clique em
Next.



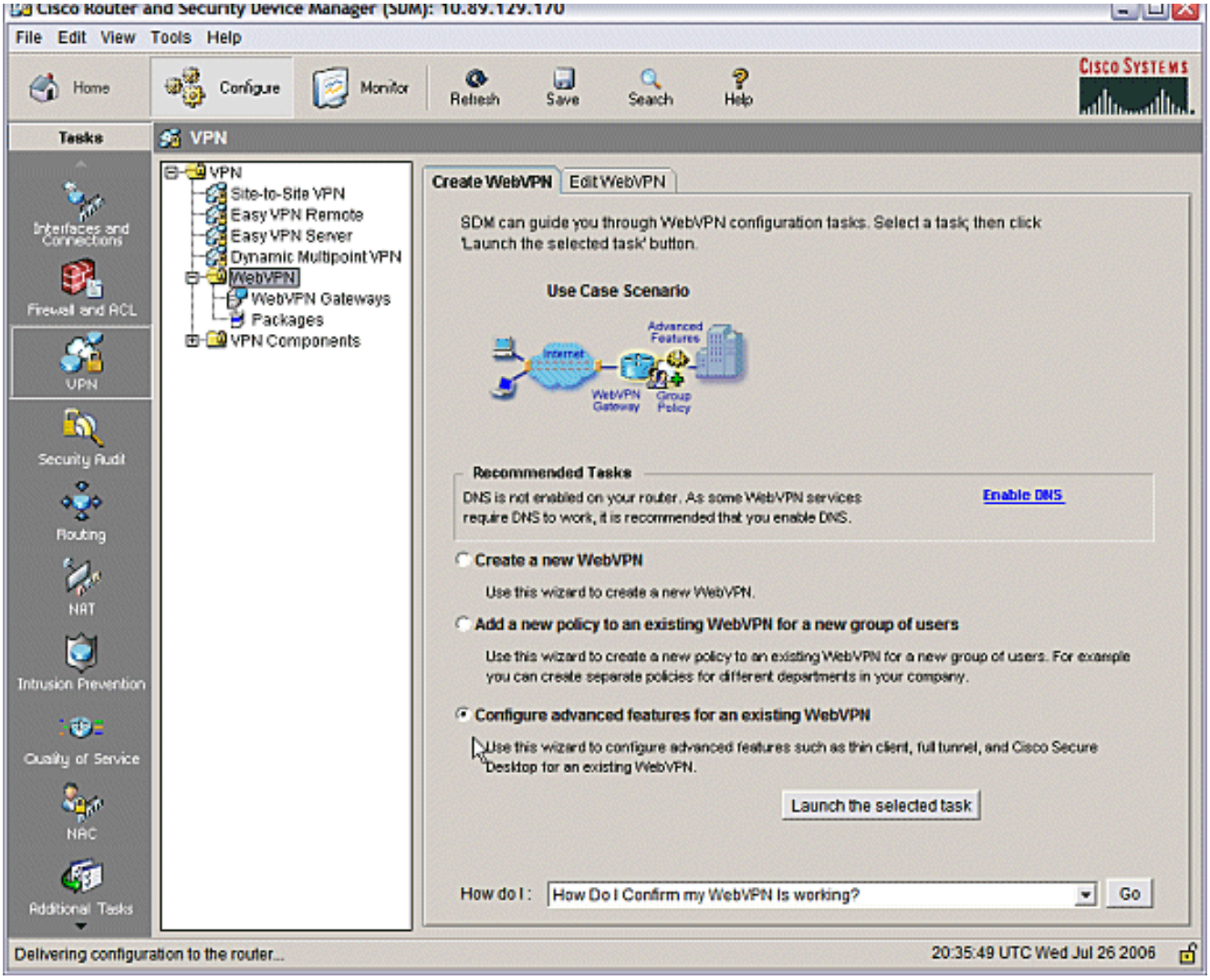
4. Personalize a aparência da página do portal WebVPN ou aceite a aparência padrão.Clique em
   Next.



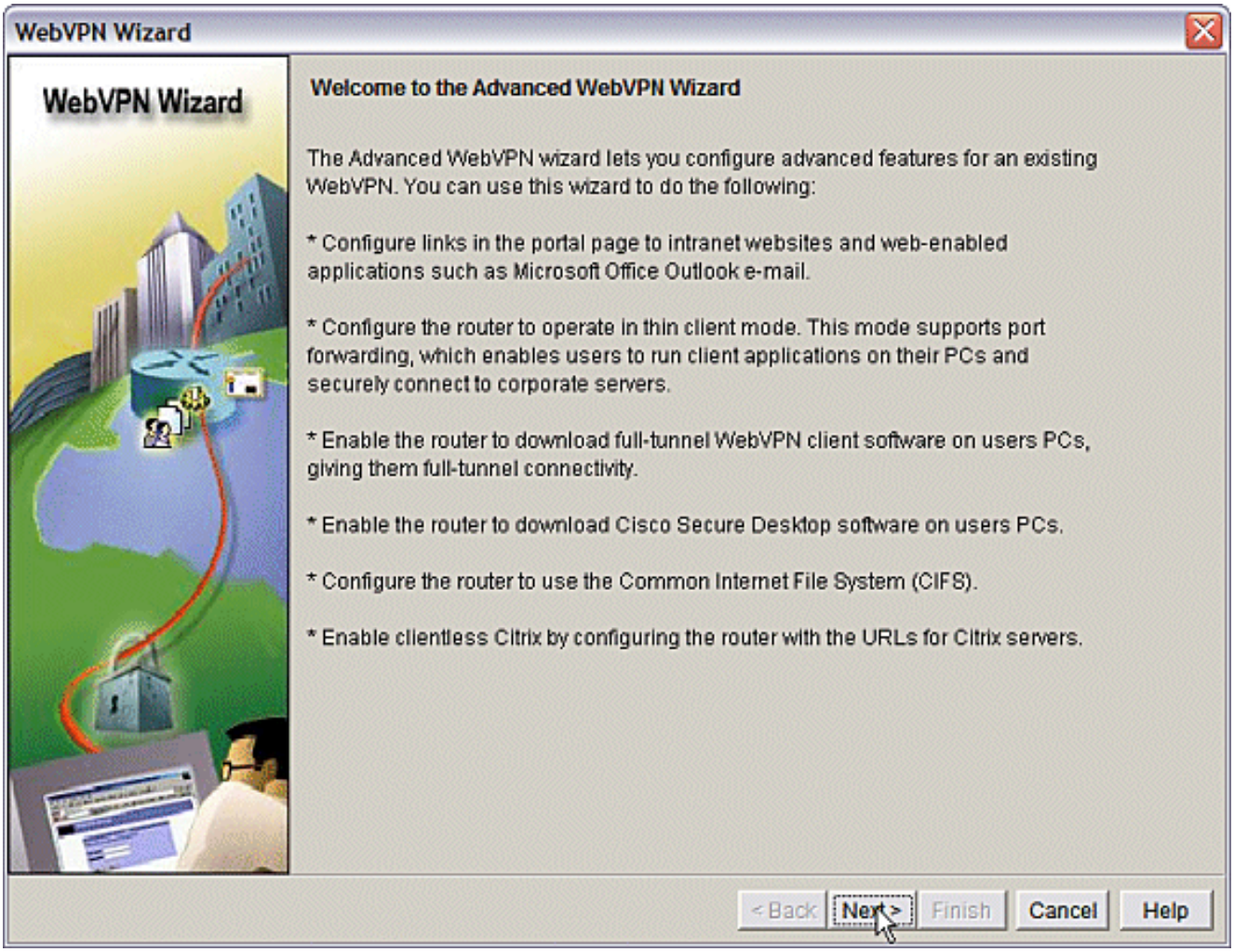
Visualize o resumo da configuração e clique em **Concluir > Salvar**.



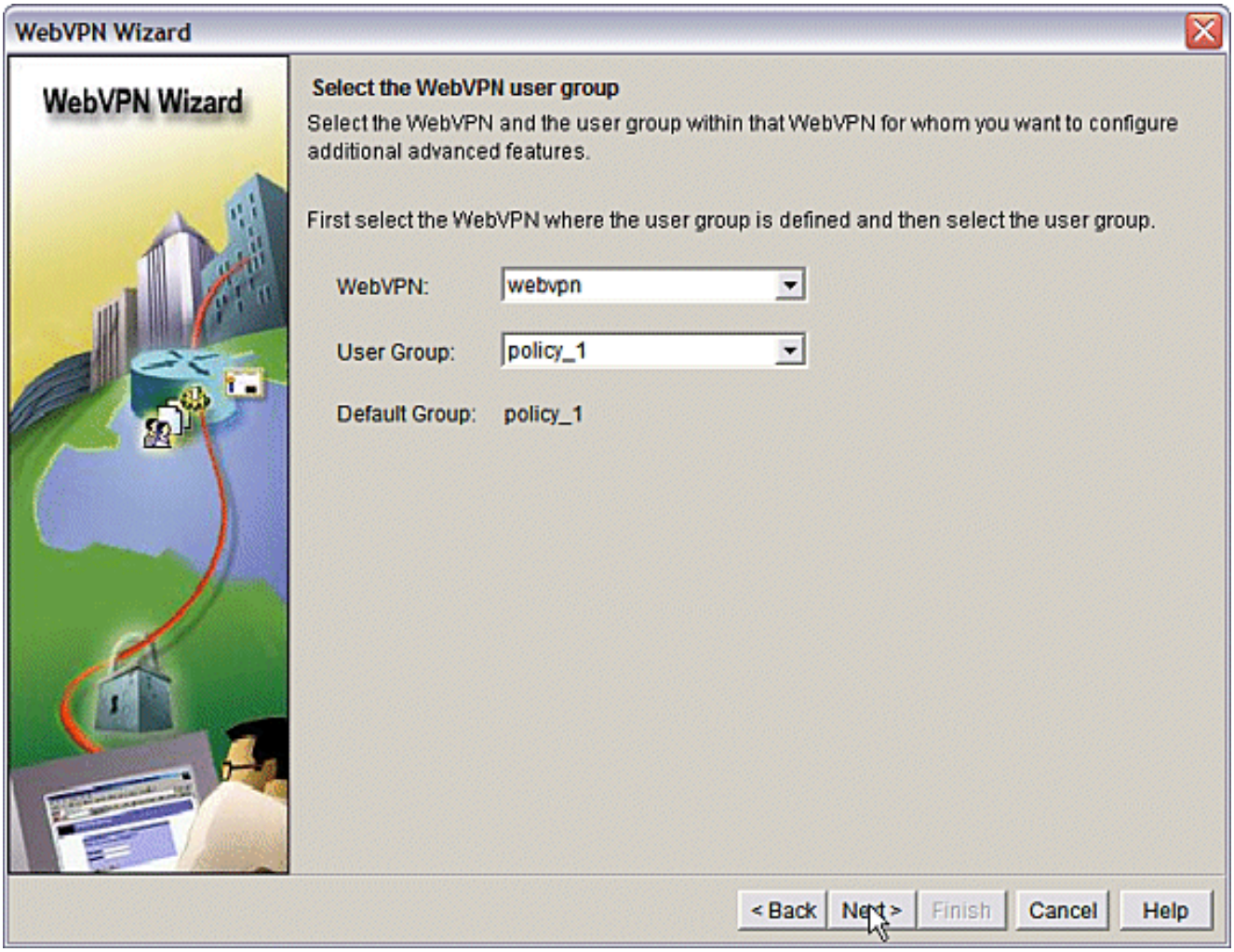
5. Você criou um Gateway WebVPN e um Contexto WebVPN com uma Política de Grupo vinculada. Configure as portas Thin-Client, que são disponibilizadas quando os clientes se conectam ao WebVPN.Escolha **Configurar**.Escolha **VPN > WebVPN**.Escolha **Create WebVPN**.Escolha o botão de opção **Configurar recursos avançados para uma WebVPN existente** e clique em **Iniciar a tarefa selecionada**.



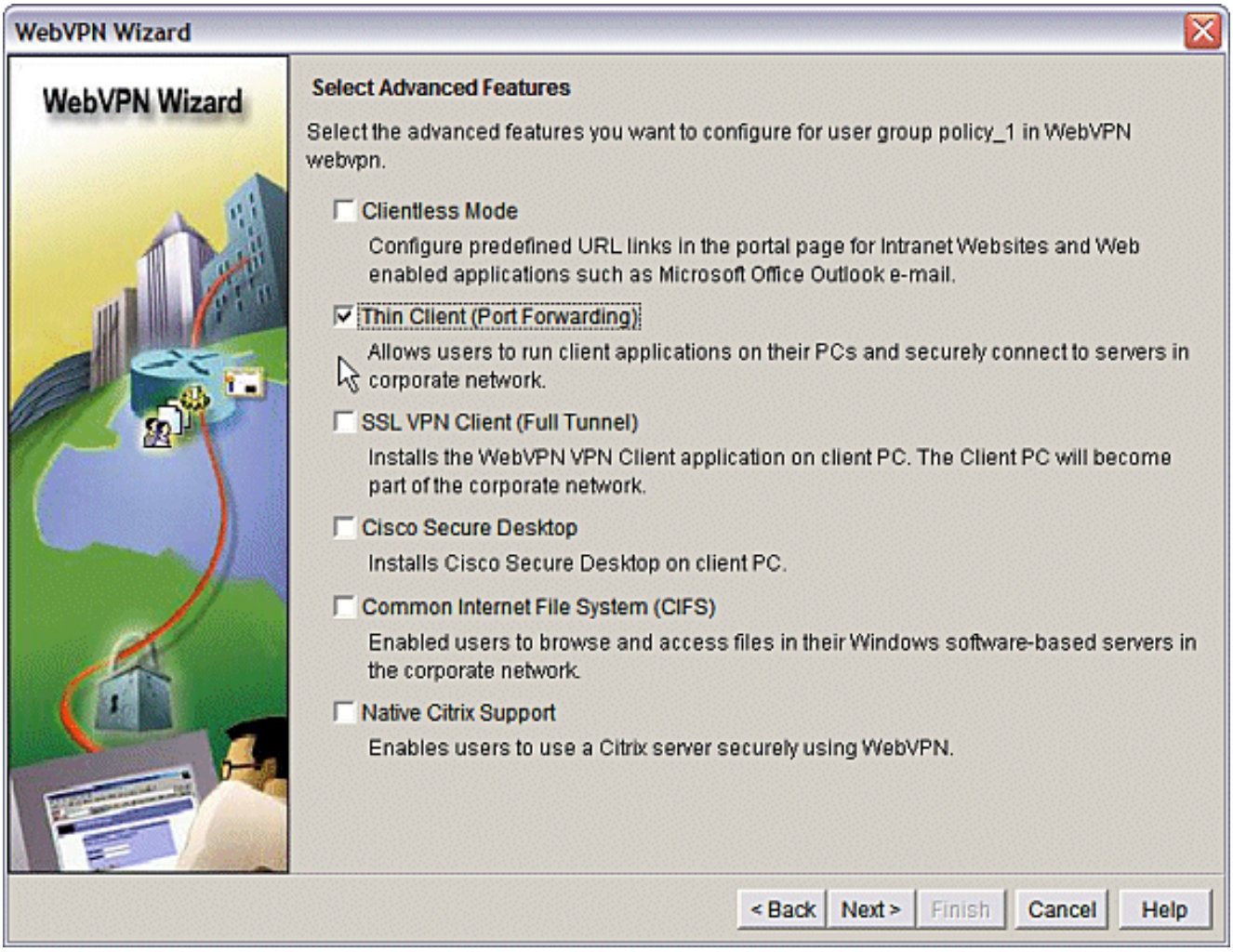
A tela Welcome (Bem-vindo) oferece os destaques dos recursos do Assistente. Clique em Next.



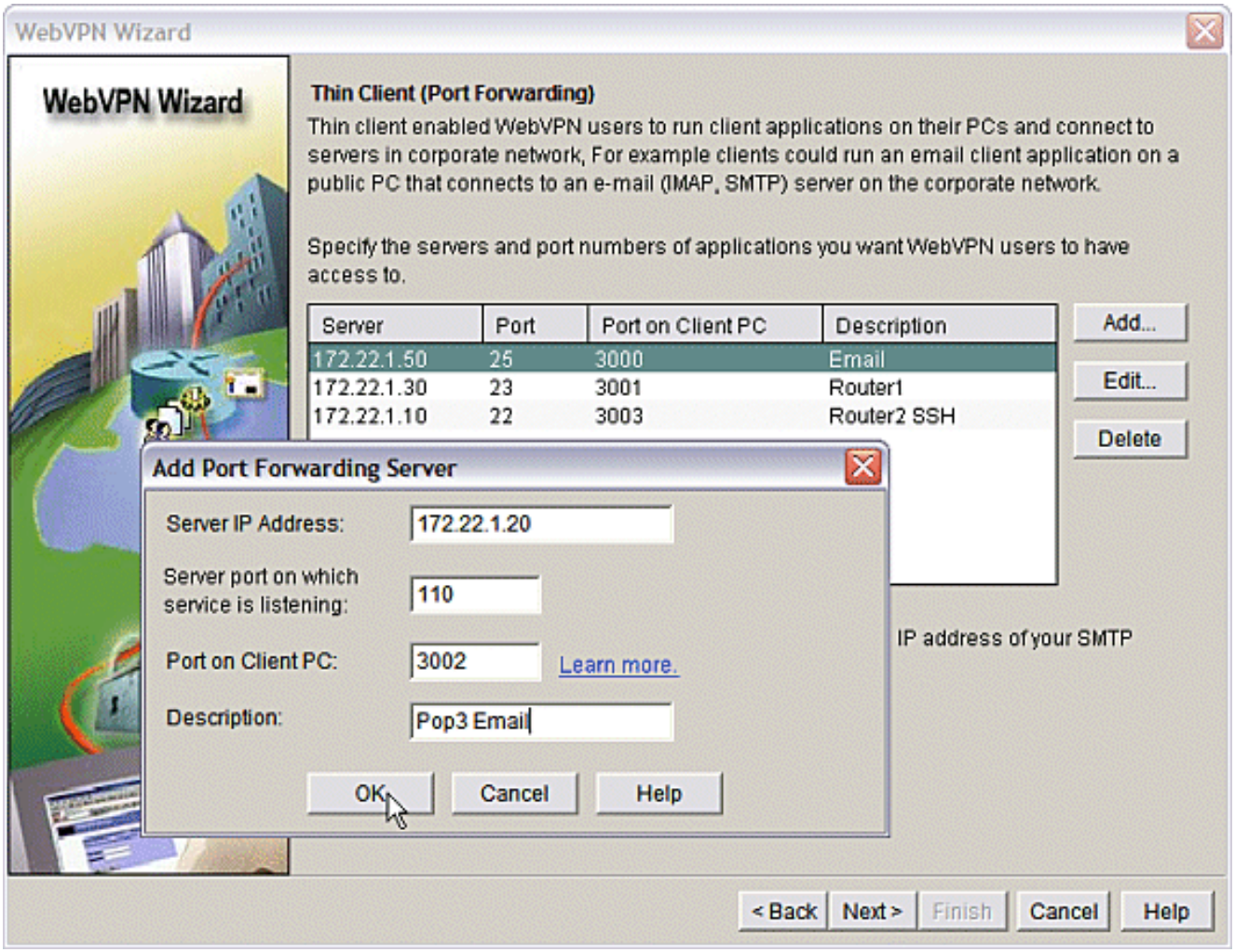
Escolha o contexto e o grupo de usuários do WebVPN nos menus suspensos. Clique em Next.



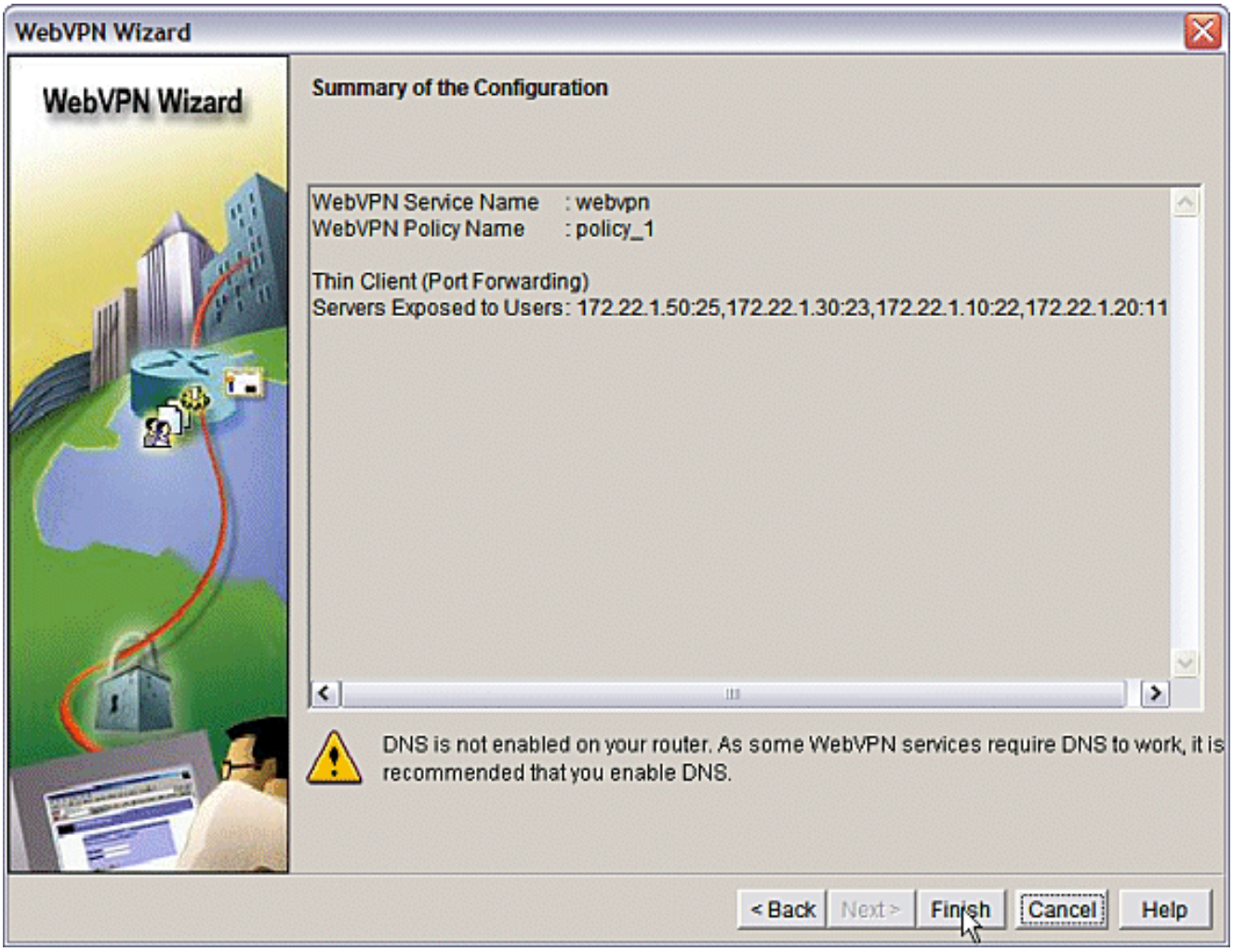
Escolha **Thin Client (Port Forwarding)** e clique em **Next**.



Insira os recursos que deseja disponibilizar por meio do Port Forwarding. A porta de serviço deve ser uma porta estática, mas você pode aceitar a porta padrão no PC cliente atribuída pelo Assistente. Clique em
Next.



Visualize o resumo da configuração e clique em **Concluir > OK > Salvar**.



Configuração

Resultados da configuração do SDM.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
```

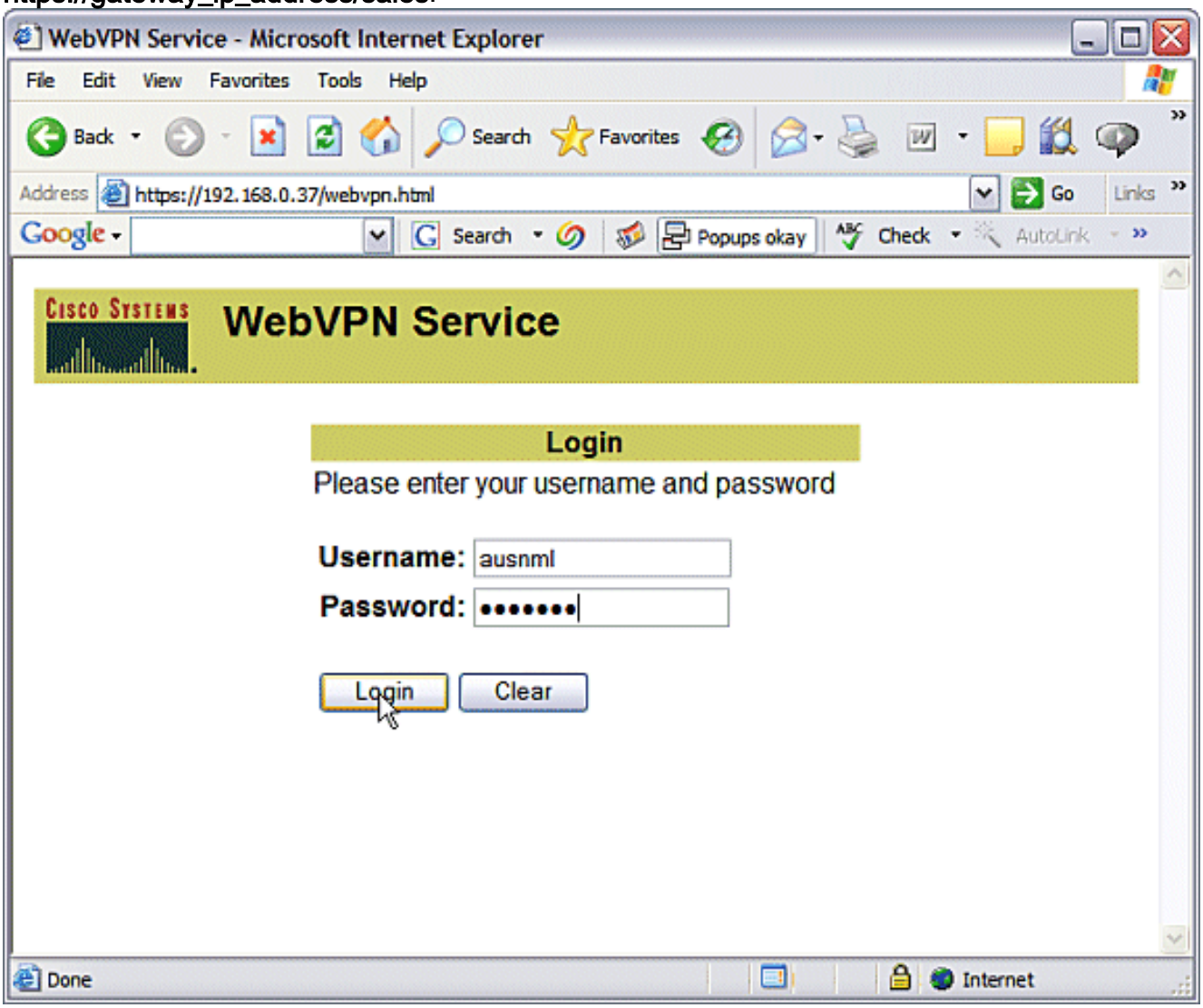
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http secure-server ip http
timeout-policy idle 600 life 86400 requests 100 !
control-plane ! line con 0 stopbits 1 line aux 0
stopbits 1 line vty 0 4 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

Verificar

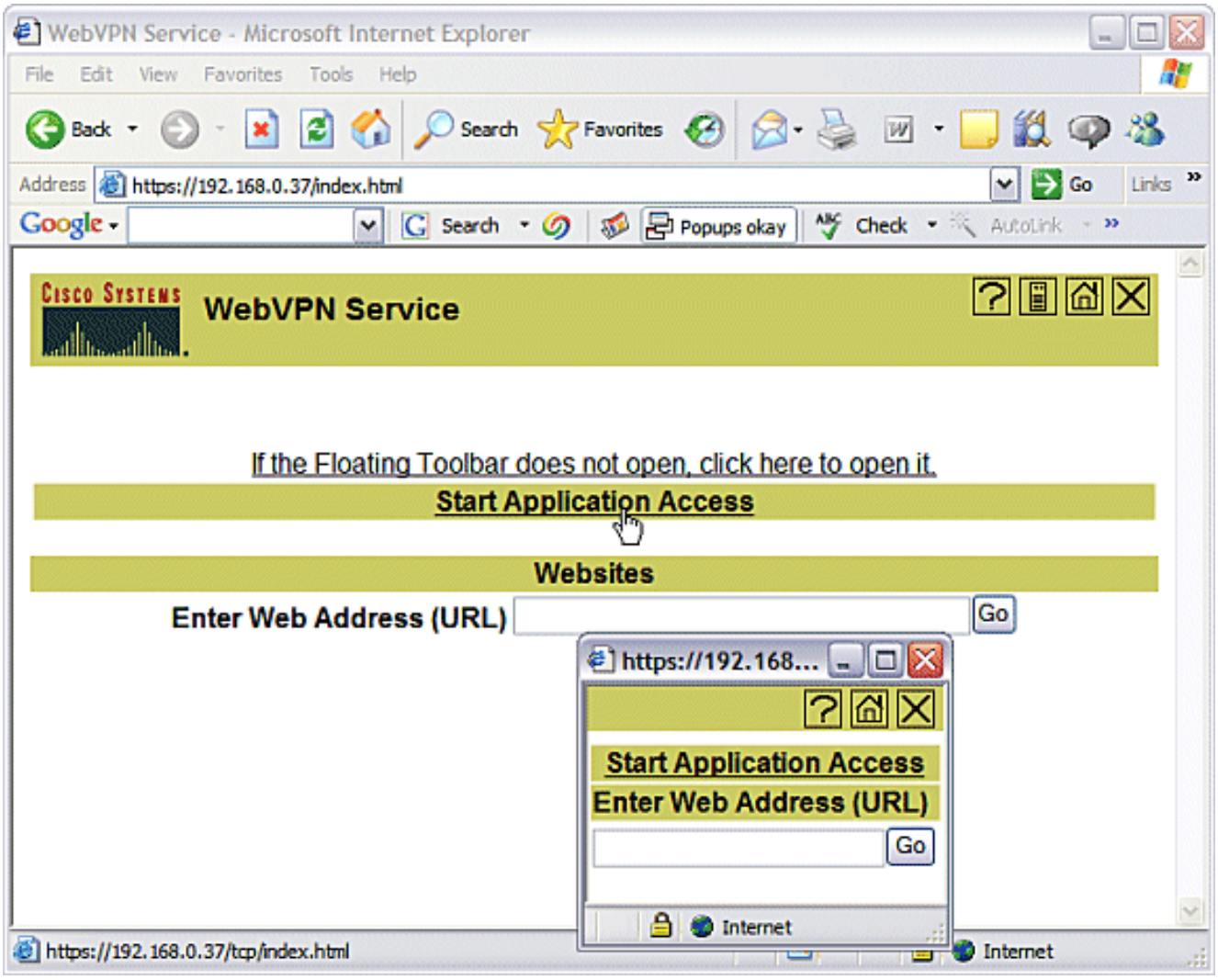
Verifique sua configuração

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

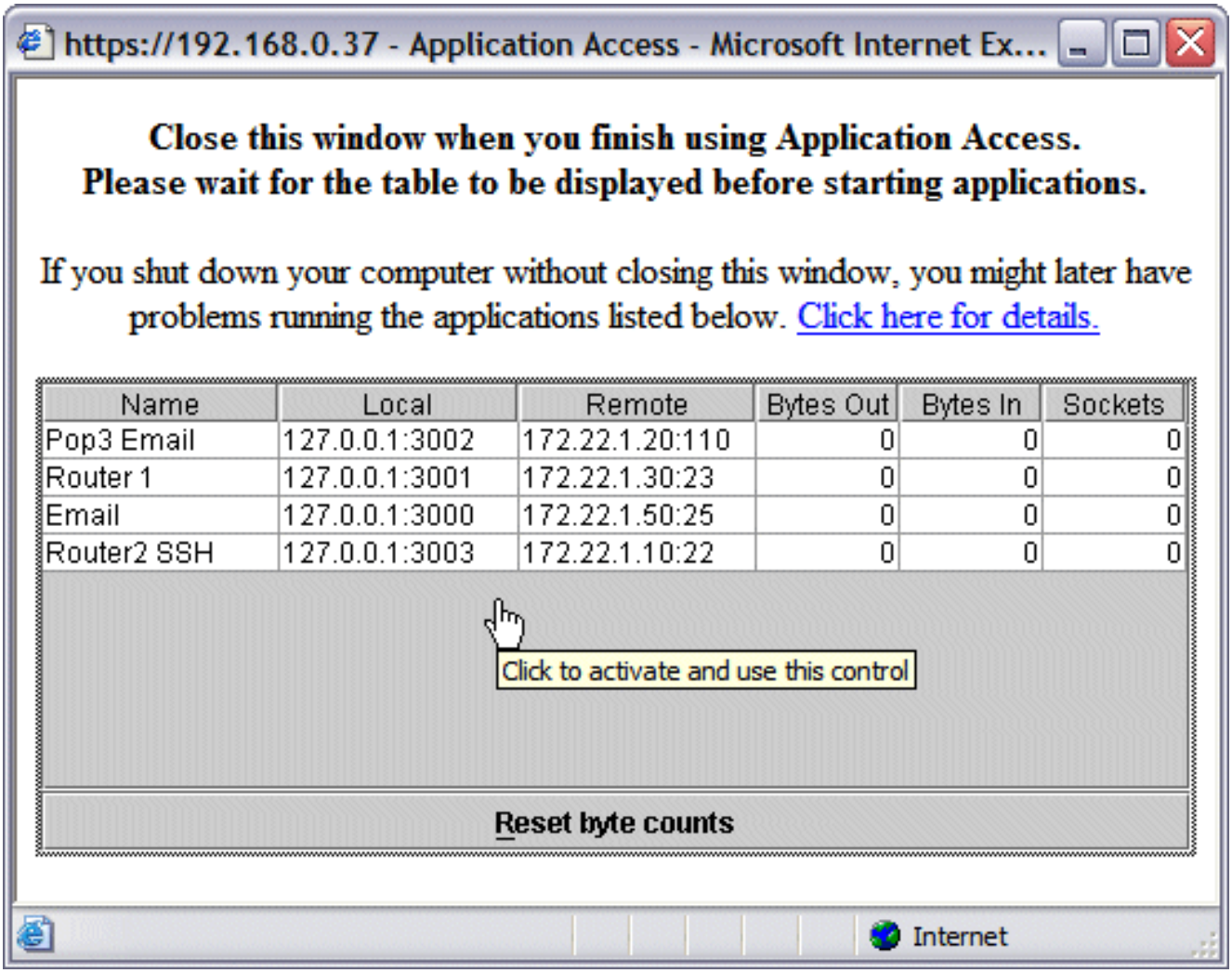
1. Use um computador cliente para acessar o gateway WebVPN em **https://gateway_ip_address.** Lembre-se de incluir o nome de domínio WebVPN se você criar contextos WebVPN exclusivos. Por exemplo, se você criou um domínio chamado vendas, digite **https://gateway_ip_address/sales**.



2. Faça login e aceite o certificado oferecido pelo gateway WebVPN. Clique em **Iniciar acesso ao aplicativo**.



3. Uma tela de acesso a aplicativos é exibida. Você pode acessar um aplicativo com o número de porta local e o endereço IP de loopback local. Por exemplo, para executar telnet para o Roteador 1, insira **telnet 127.0.0.1 3001**. O miniaplicativo Java envia essas informações para o gateway WebVPN, que depois une as duas extremidades da sessão de forma segura. As conexões bem-sucedidas podem fazer com que as colunas **Bytes Out** e **Bytes In** aumentem.



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 ver o uso dos comandos **show** em detalhes, consulte Verificando a configuração do WebVPN.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshoot

Use esta seção para resolver problemas de configuração.

Os computadores clientes devem ser carregados com SUN Java versão 1.4 ou posterior. Obter uma cópia deste software a partir do download do software Java

Comandos usados para solucionar problemas

Observação: consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos **debug**.

- **show webvpn ?**—Há muitos comandos **show** associados ao WebVPN. Eles podem ser executados na CLI para mostrar estatísticas e outras informações. Para ver o uso de

comandos **show** em detalhes, consulte Verificando a configuração do WebVPN.
- **debug webvpn ?**—O uso de comandos **debug** pode afetar adversamente o roteador. Para ver o uso dos comandos **debug** mais detalhadamente, consulte Usando Comandos de Depuração WebVPN.

Informações Relacionadas

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Perguntas e respostas sobre a WebVPN do Cisco IOS
- Suporte Técnico e Documentação - Cisco Systems