Configuración de Thin-Client SSL VPN (WebVPN) Cisco IOS con SDM

Contenido

Introducción

La tecnología Thin-Client SSL VPN se puede utilizar para permitir el acceso seguro a las aplicaciones que utilizan puertos estáticos. Los ejemplos son Telnet (23), SSH (22), POP3 (110), IMAP4 (143) y SMTP (25). Thin-Client puede estar dirigido por el usuario, por políticas o por ambos. El acceso se puede configurar usuario por usuario o se pueden crear políticas de grupo que incluyan uno o más usuarios. La tecnología SSL VPN se puede configurar en tres modos principales: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port Forwarding) y SSL VPN Client (SVC-Full Tunnel Mode).

1. VPN SSL sin cliente (WebVPN):

Un cliente remoto necesita solamente un buscador Web habilitado por SSL para acceder a los servidores Web http o https en la LAN corporativa. El acceso está también disponible para buscar archivos de Windows con el sistema Común de Archivos de Internet (CIFS). Un buen ejemplo del acceso http es el cliente de Outlook Web Access (OWA).

Consulte Ejemplo de Configuración de SSL VPN sin cliente (WebVPN) en Cisco IOS mediante SDM para obtener más información sobre la VPN SSL sin cliente.

2. Thin-Client SSL VPN (reenvío de puertos)

Un cliente remoto debe descargar un pequeño subprograma Java para el acceso seguro de las aplicaciones TCP que utilizan los números del puerto estático. El UDP no se soporta. Los ejemplos incluyen el acceso a POP3, S TP, IMAP, SSH, y a Telnet. El usuario necesita privilegios administrativos locales porque los cambios se realizan a los archivos en el equipo local. Este método de SSL VPN no funciona con las aplicaciones que utilizan las asignaciones de puerto dinámico, por ejemplo, varias aplicaciones FTP.

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

El SSL VPN Client descarga a un pequeño cliente a la estación de trabajo remota y permite por completo, acceso seguro a los recursos en la red corporativa interna. El SVC se puede descargar permanentemente a la estación remota, o puede ser quitado una vez que finaliza la sesión segura.

Consulte Ejemplo de Configuración de SSL VPN Client (SVC) en IOS mediante SDM para obtener más información sobre SSL VPN Client.

Este documento muestra una configuración simple para Thin-Client SSL VPN en un Cisco IOS® router. La VPN SSL de Thin-Client se ejecuta en estos routers Cisco IOS:

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

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

Requisitos para el router Cisco IOS

- Cualquiera de los routers enumerados cargado con SDM y una imagen avanzada de IOS versión 12.4(6)T o posterior
- Estación de administración cargada con SDMCisco envía nuevos routers con una copia preinstalada de SDM. Si su router no tiene SDM instalado, puede obtener el software en Descarga de Software - Cisco Security Device Manager. Debe poseer una cuenta CCO con un contrato de servicio. Consulte Configuración del Router con el Administrador de Dispositivos de Seguridad para obtener instrucciones detalladas.

Requisitos para ordenadores cliente

- Los clientes remotos deben tener privilegios administrativos locales; no es obligatorio, pero se sugiere con sumo cuidado.
- Los clientes remotos deben tener Java Runtime Environment (JRE) versión 1.4 o superior.
- Exploradores de clientes remotos: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 o Firefox 1.0
- Cookies activadas y Popups permitidas en clientes remotos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Imagen de software empresarial avanzado de Cisco 12.4(9)T
- Router de servicios integrados Cisco 3825
- Router de Cisco y Security Device Manager (SDM) versión 2.3.1

The information in this document was created from the devices in a specific lab environment. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (predeterminada). If your network is live, make sure that you understand the potential impact of any command. Las direcciones IP utilizadas para esta configuración provienen del espacio de direcciones RFC 1918. No son legales en Internet.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

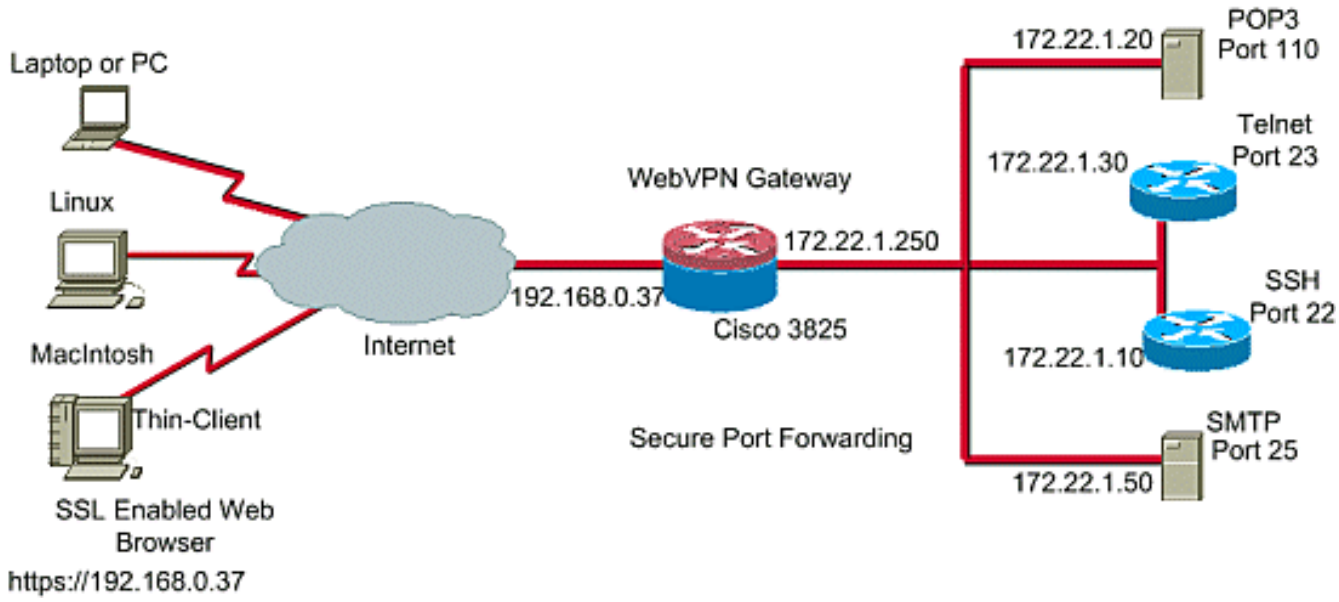
Configurar

Tarea

Esta sección contiene la información necesaria para configurar las características descritas dentro de este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

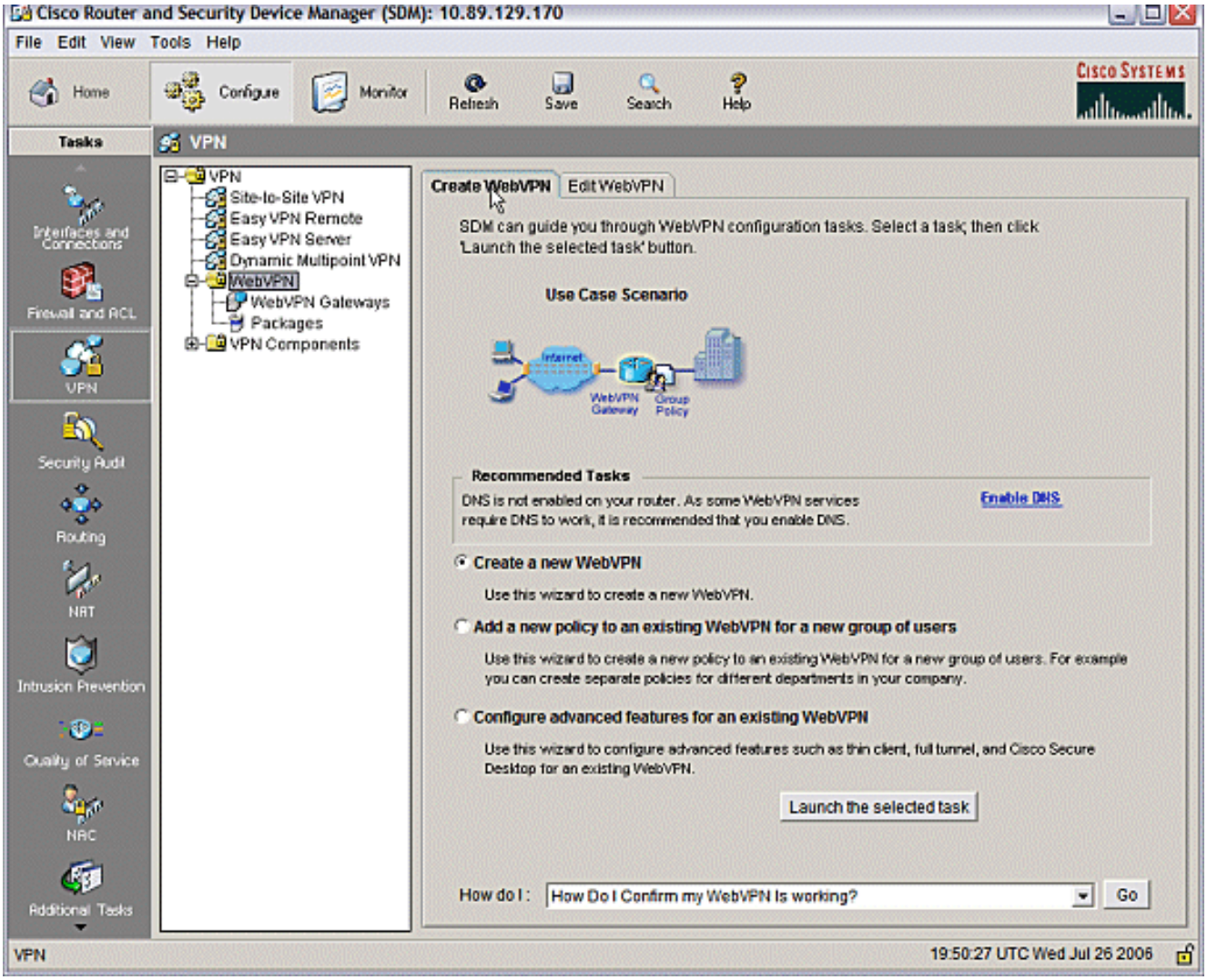


Configuración de Thin-Client SSL VPN

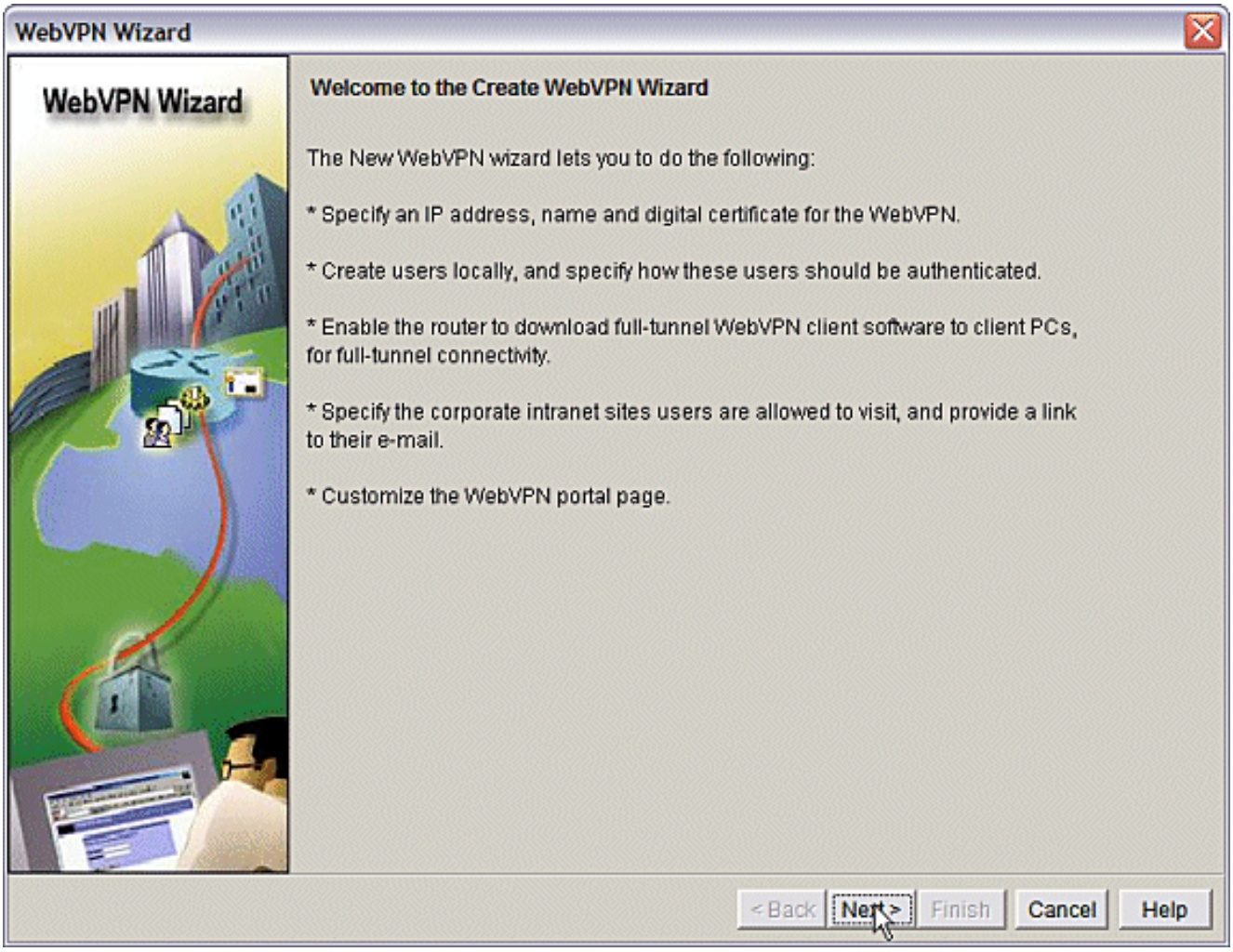
Utilice el asistente proporcionado en la interfaz del administrador de dispositivos de seguridad (SDM) para configurar Thin-Client SSL VPN en Cisco IOS o bien configúrelo en la interfaz de línea de comandos (CLI) o manualmente en la aplicación SDM. En este ejemplo se utiliza el

asistente.

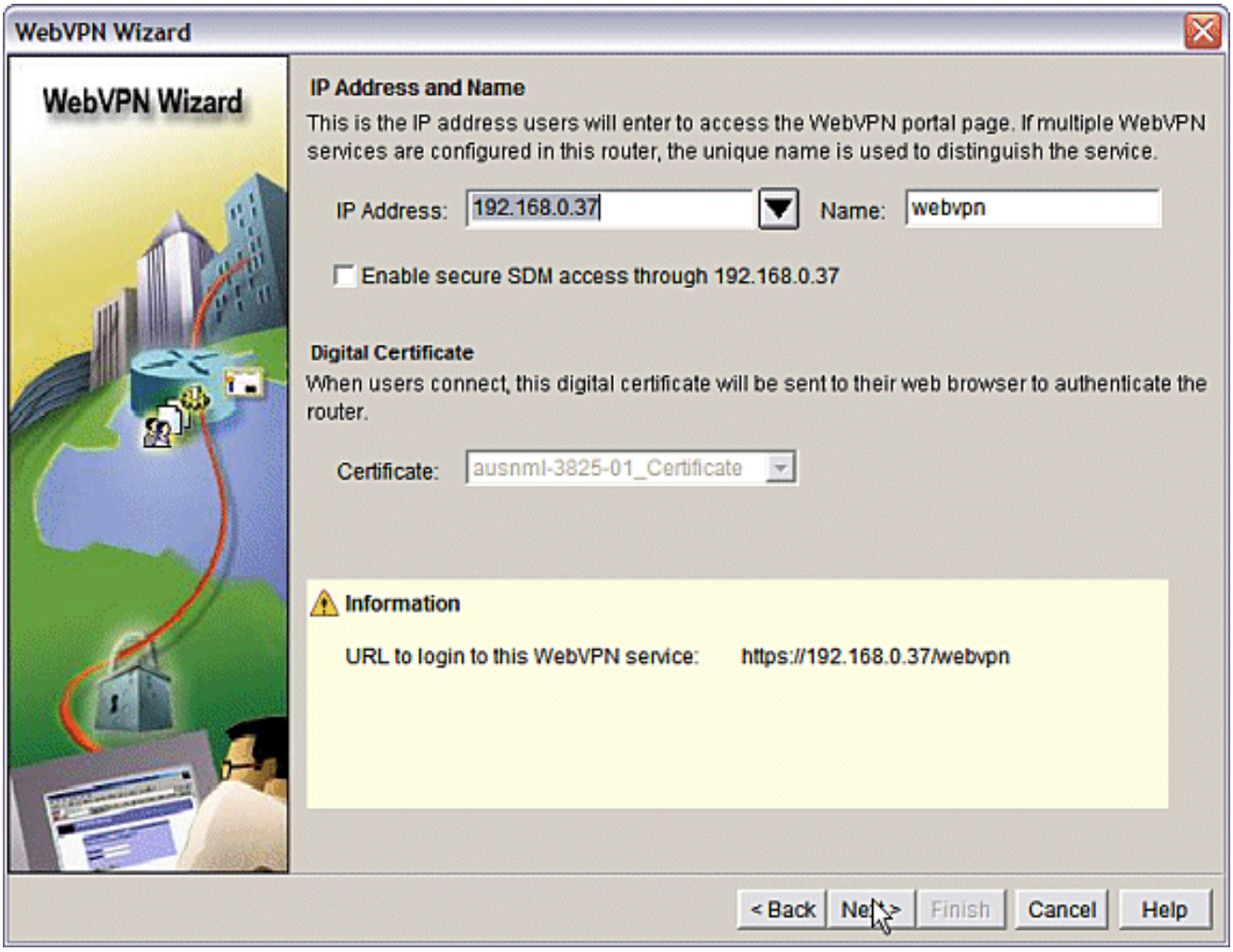
1. Elija la pestaña **Configurar**.En el panel de navegación, elija **VPN > WebVPN**.Haga clic en la pestaña **Create WebVPN**.Haga clic en el botón de opción situado junto a **Create a new WebVPN**.Haga clic en el botón **Iniciar la tarea seleccionada**.



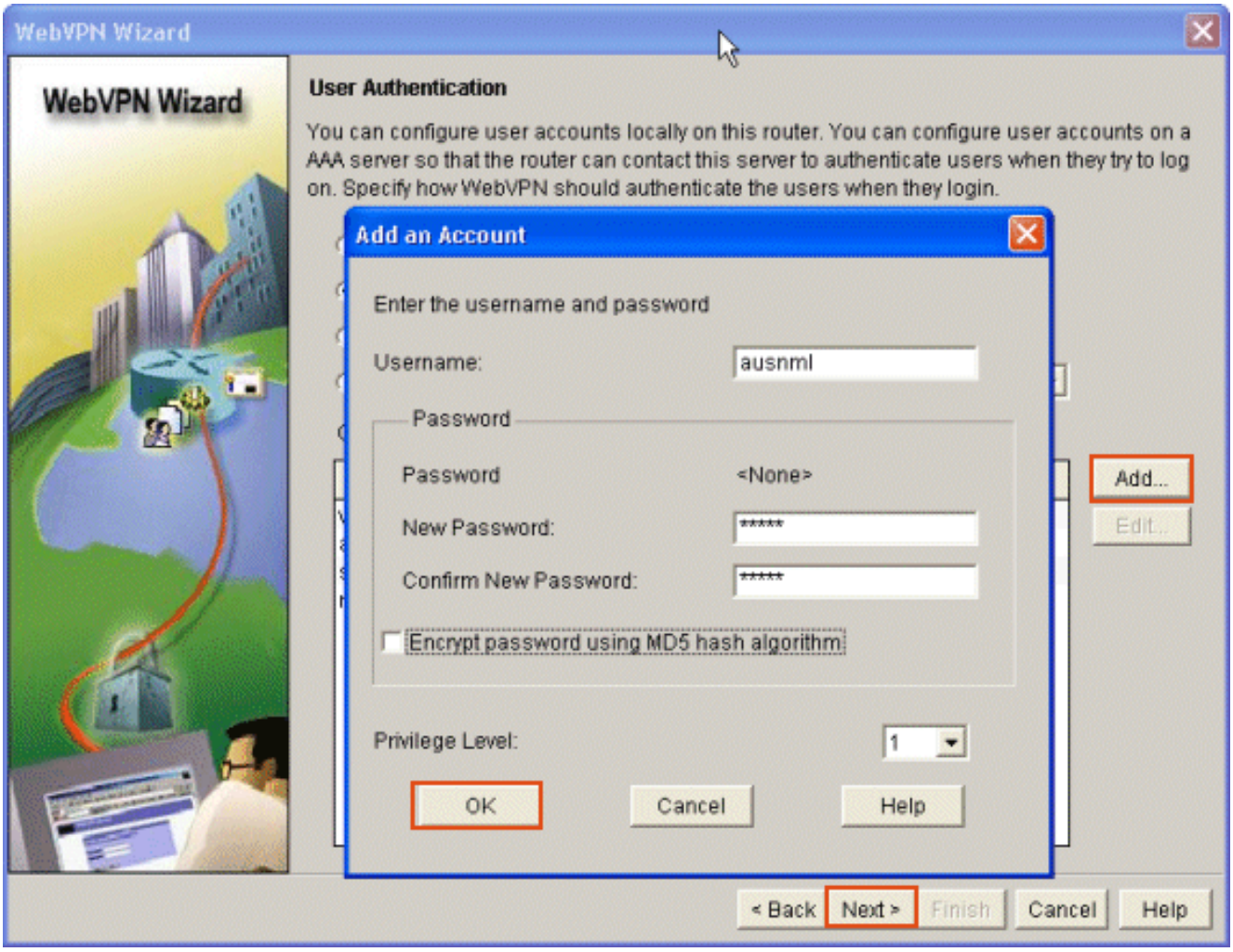
2. Se inicia el asistente de WebVPN. Haga clic en Next (Siguiente).



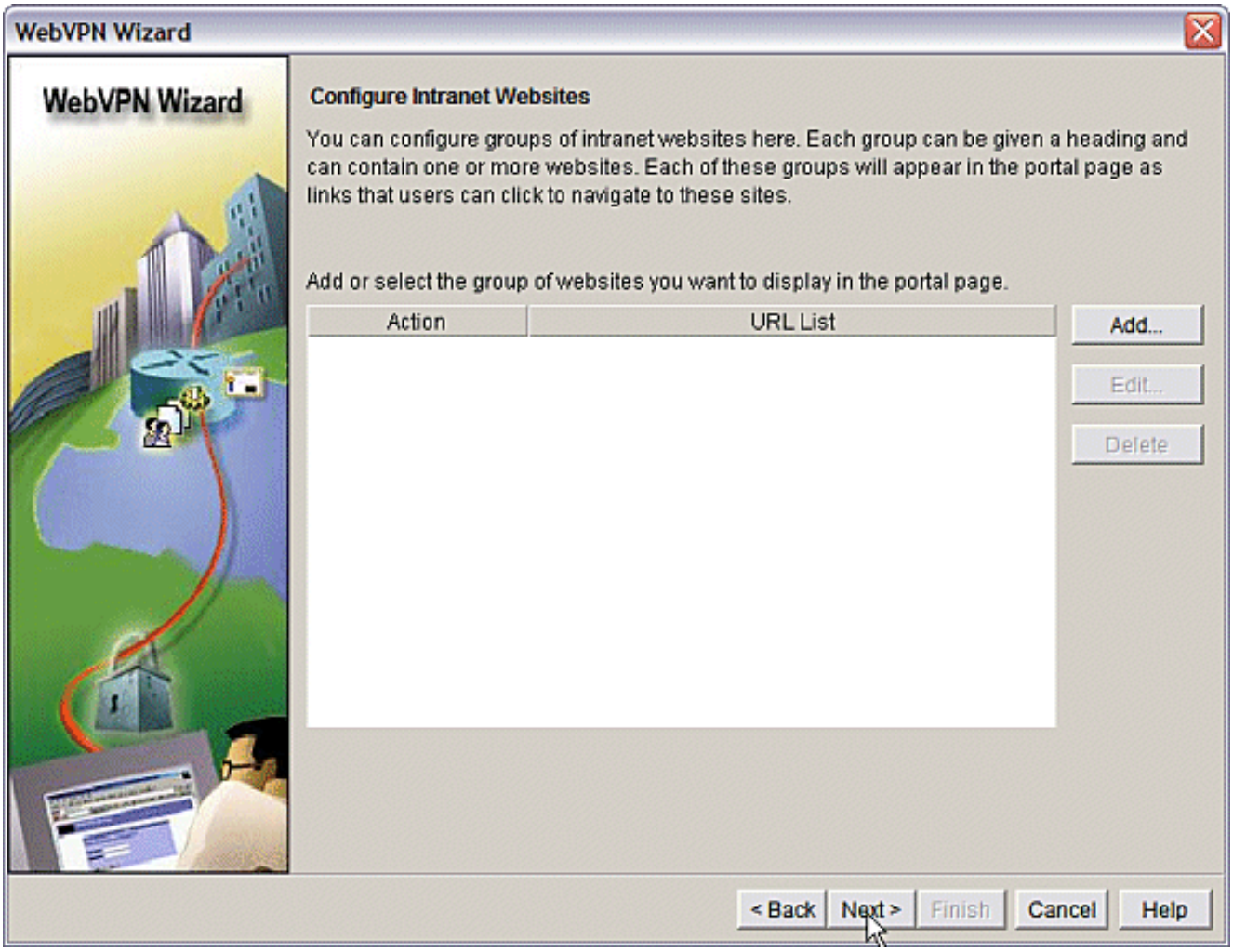
Introduzca la dirección IP y un nombre único para este gateway de WebVPN. Haga clic en Next
(Siguiente).



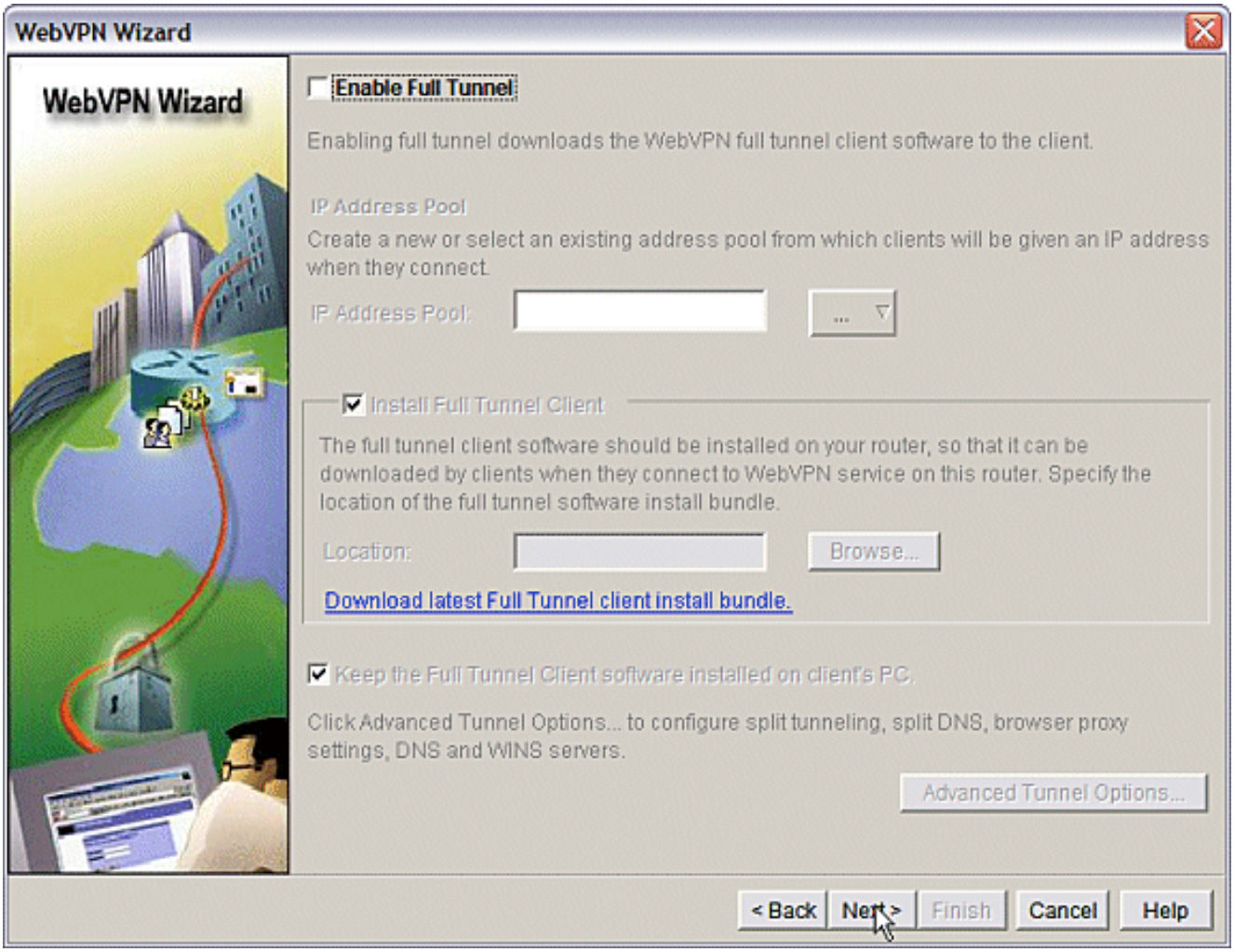
3. La pantalla User Authentication (Autenticación de usuario) permite proporcionar la autenticación de los usuarios. Esta configuración utiliza una cuenta creada localmente en el router. También puede utilizar un servidor de autenticación, autorización y contabilidad (AAA).Para agregar un usuario, haga clic en **Agregar**.Introduzca la información del usuario en la pantalla Add an Account (Agregar una cuenta) y haga clic en **OK (Aceptar)**.Haga clic en **Next** en la pantalla User Authentication (Autenticación de usuario).



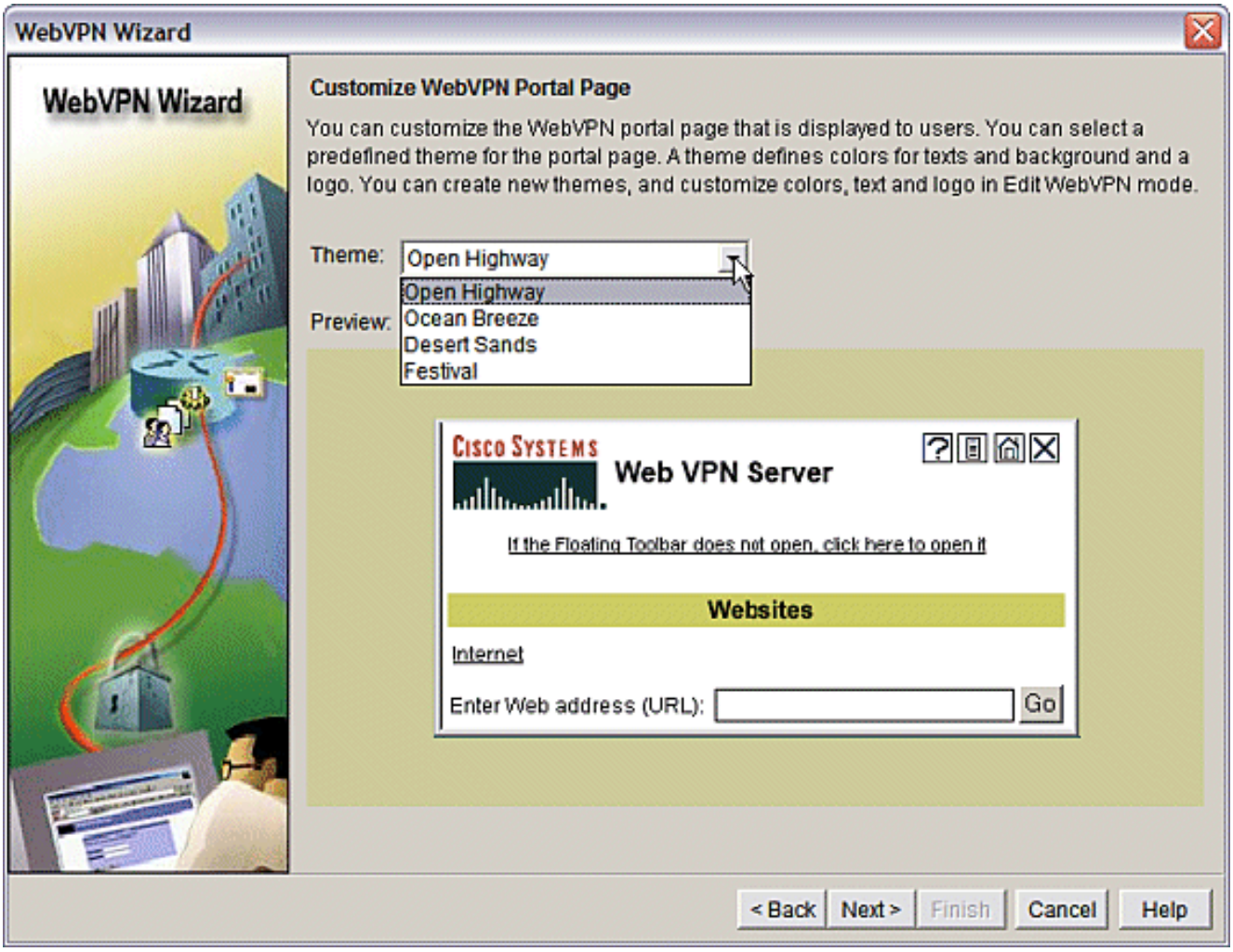
La pantalla WebVPN Wizard (Asistente WebVPN) permite la configuración de sitios Web de Intranet, pero este paso se omite porque se utiliza Port-Forwarding para este acceso a la aplicación. Si desea permitir el acceso a sitios web, utilice las configuraciones SSL VPN sin cliente o Cliente completo, que no están dentro del alcance de este documento.



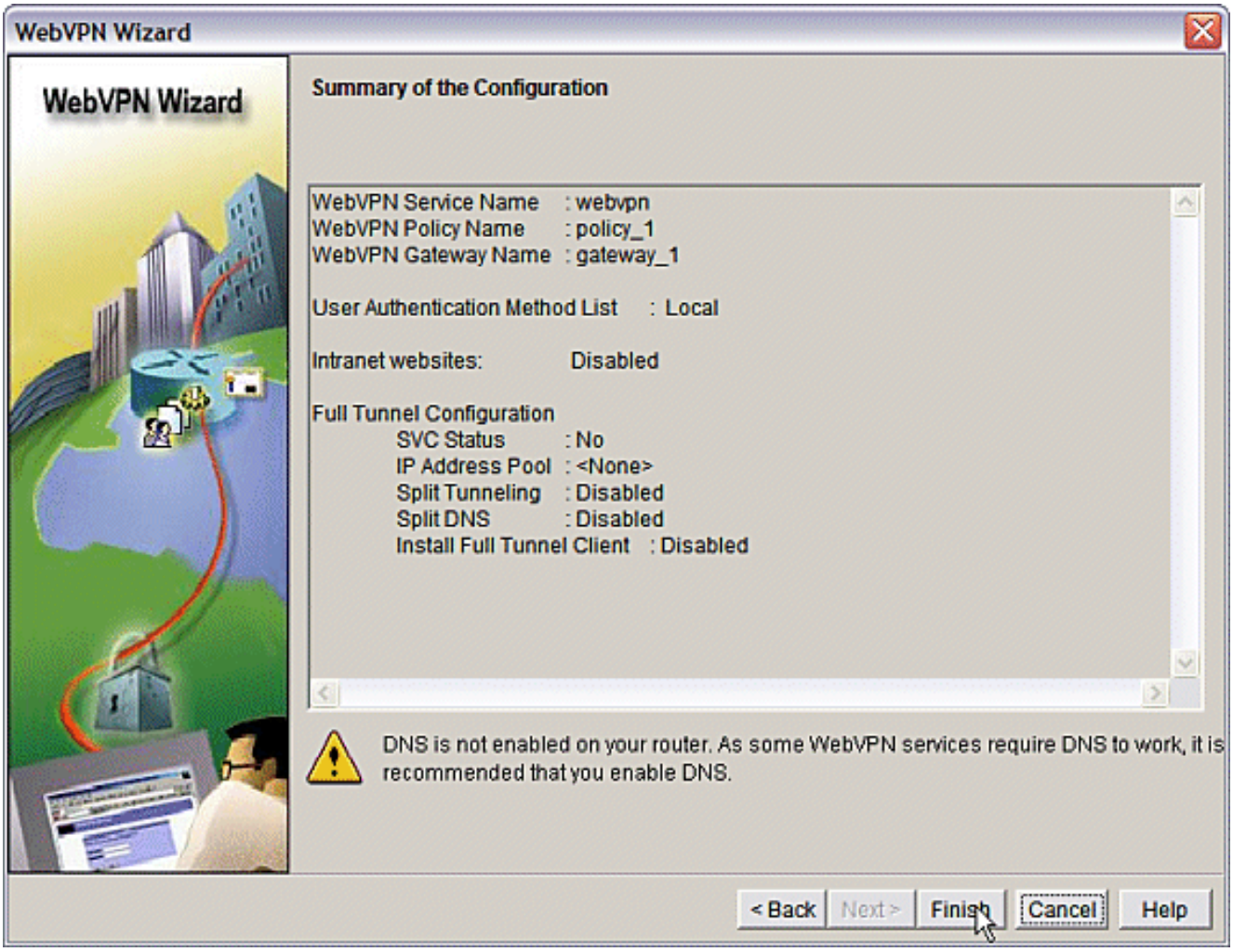
Haga clic en Next (Siguiente). El asistente muestra una pantalla que permite configurar el cliente de túnel completo. Esto no se aplica a Thin-Client SSL VPN (Port Forwarding).Desmarque **Enable Full Tunnel**. Haga clic en Next (Siguiente).



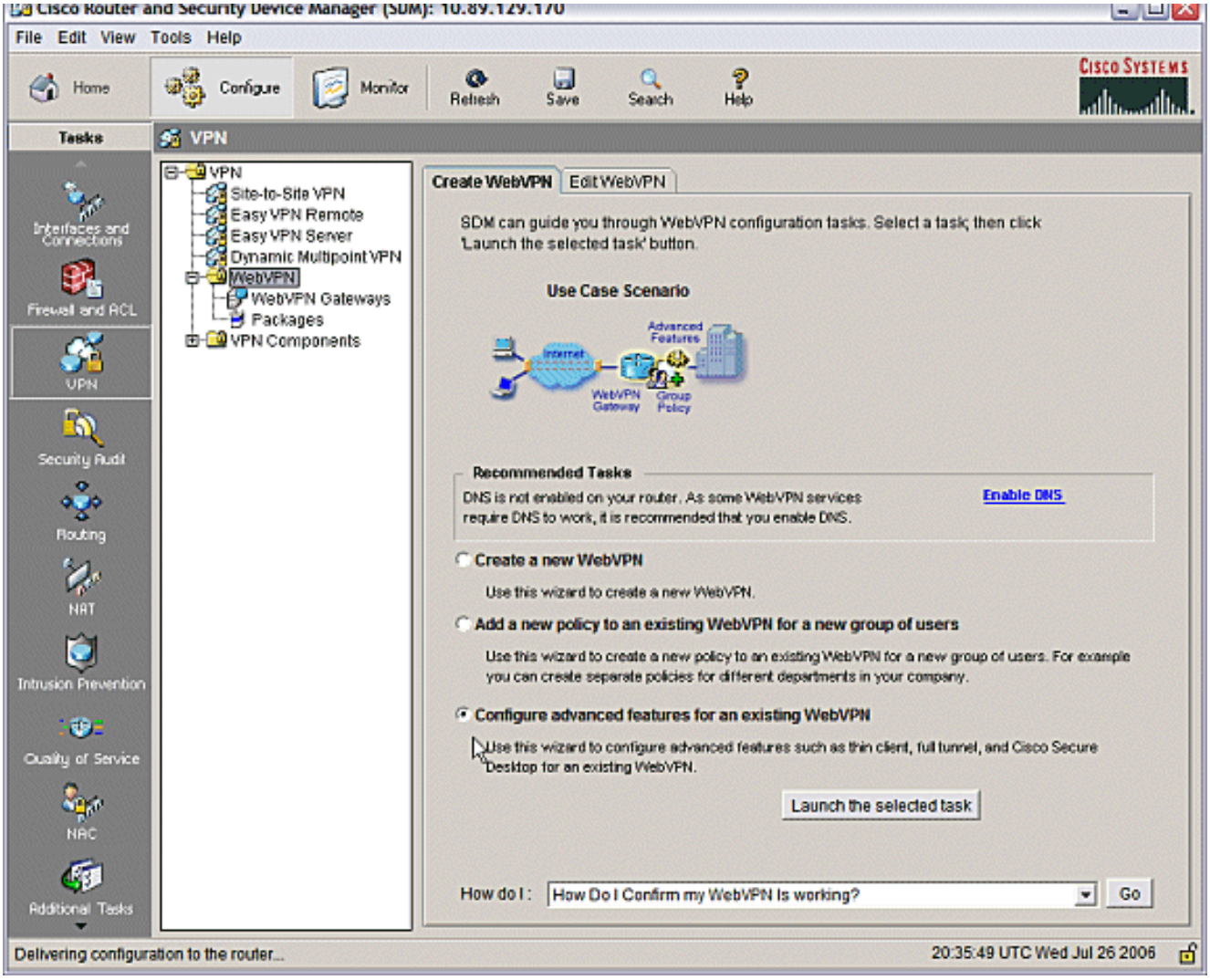
4. Personalice la apariencia de la página del portal WebVPN o acepte la apariencia predeterminada.Haga clic en Next
(Siguiente).



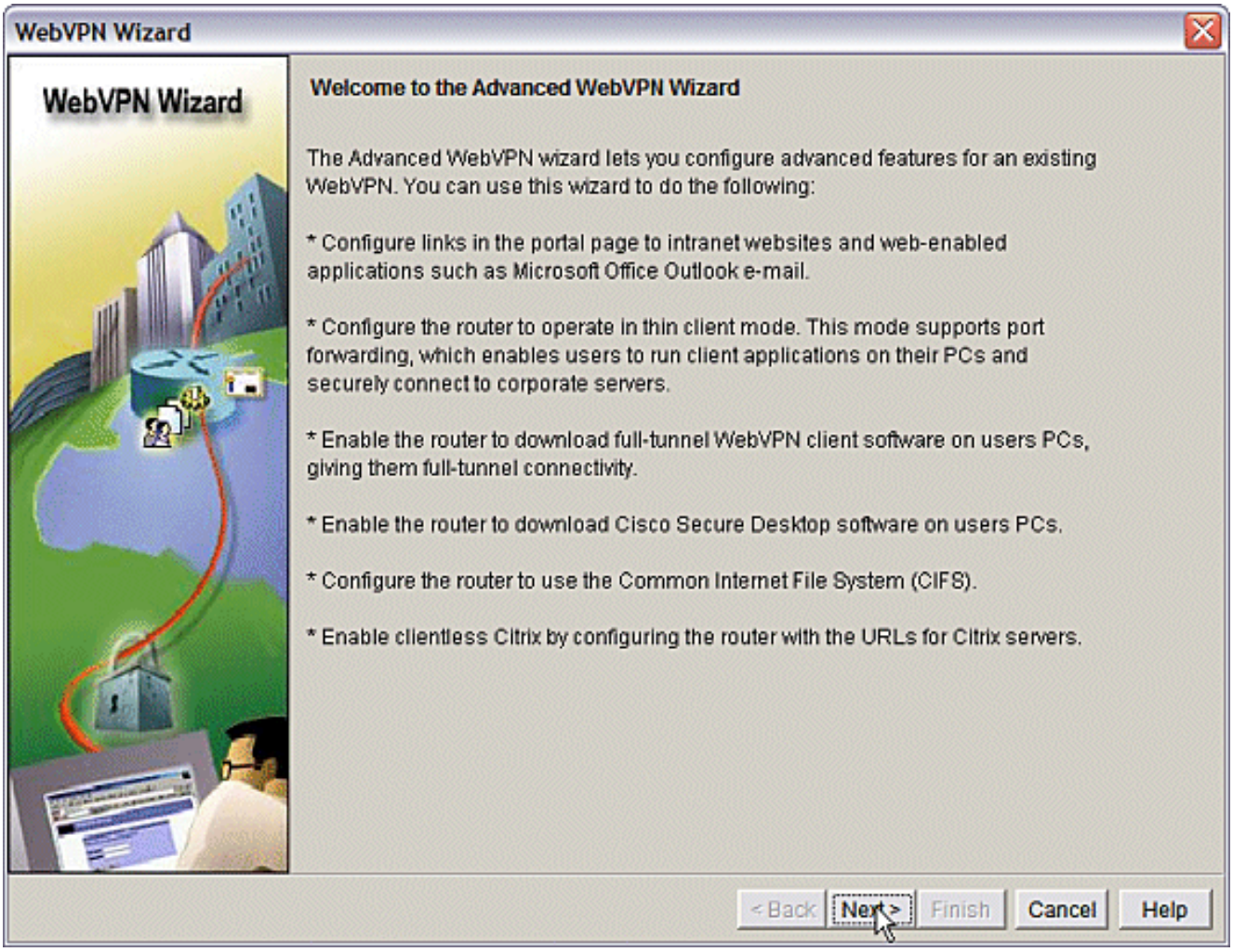
Vista previa del resumen de la configuración y haga clic en **Finalizar > Guardar**.



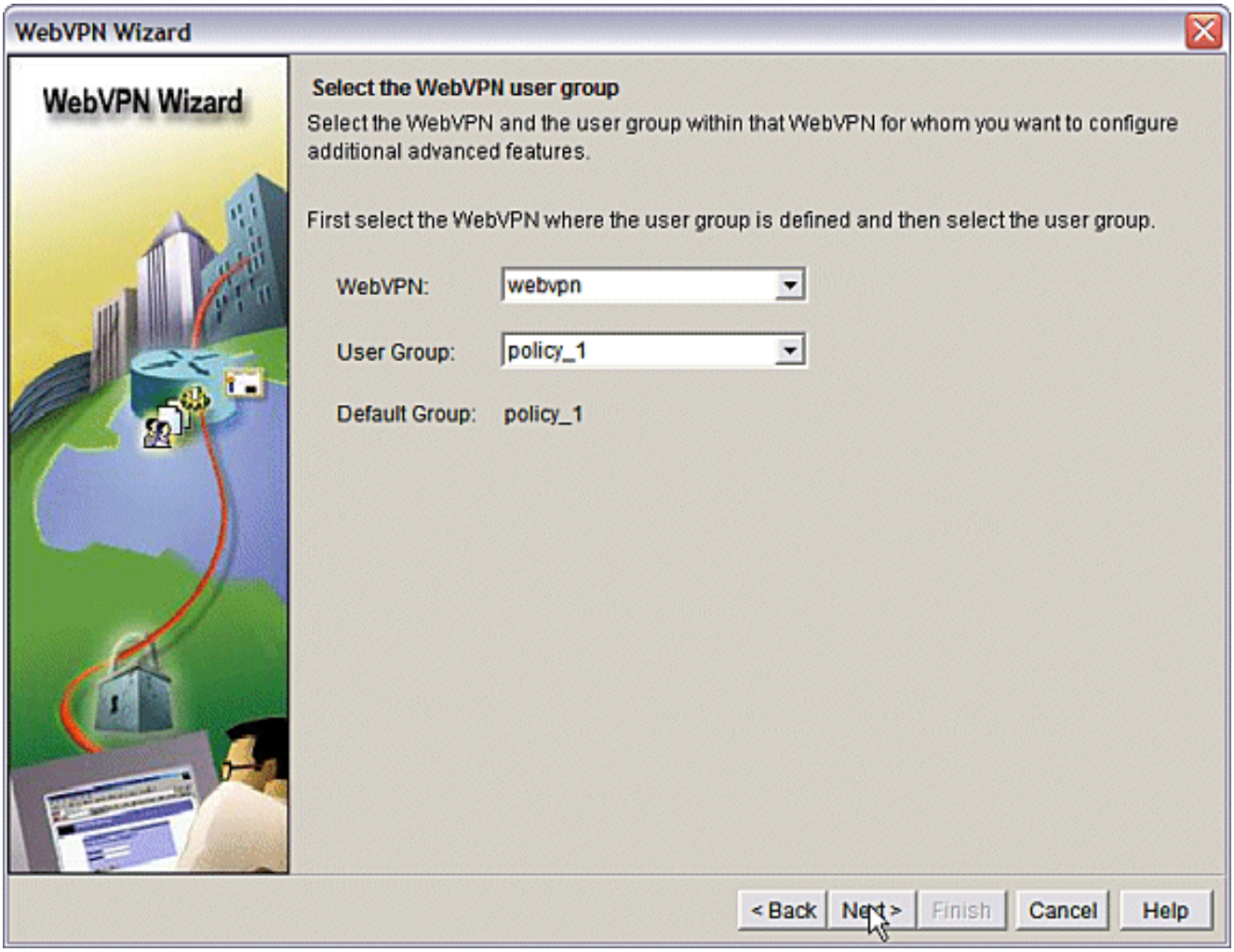
5. Ha creado un gateway WebVPN y un contexto WebVPN con una política de grupo vinculada. Configure los puertos Thin-Client, que están disponibles cuando los clientes se conectan al WebVPN.Elija **Configure**.Elija **VPN > WebVPN**.Elija **Create WebVPN**.Elija el botón de opción **Configurar funciones avanzadas para una WebVPN existente** y haga clic en **Iniciar la tarea seleccionada**.



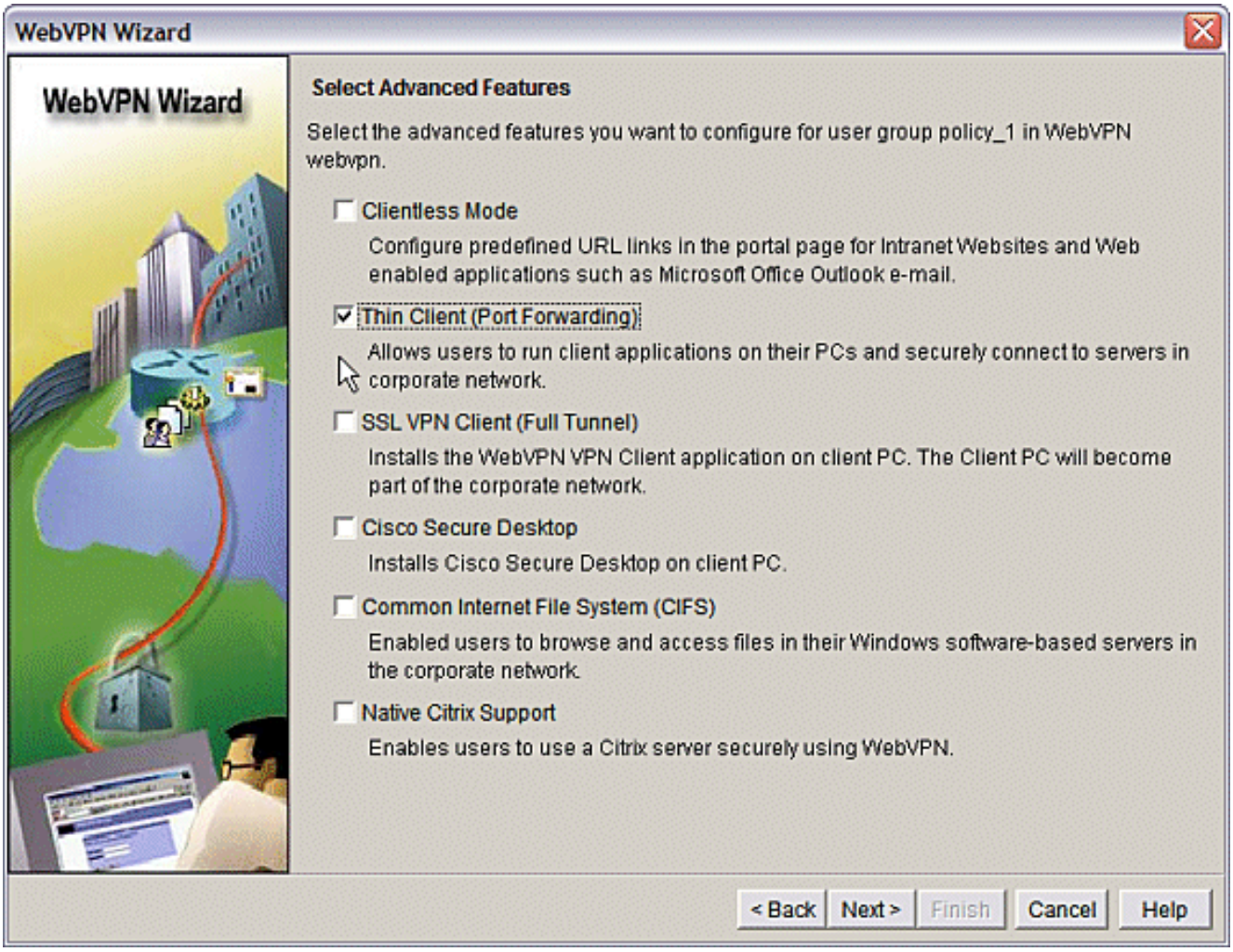
La pantalla Welcome (Bienvenido) ofrece información destacada sobre las funciones del asistente. Haga clic en Next
(Siguiente).



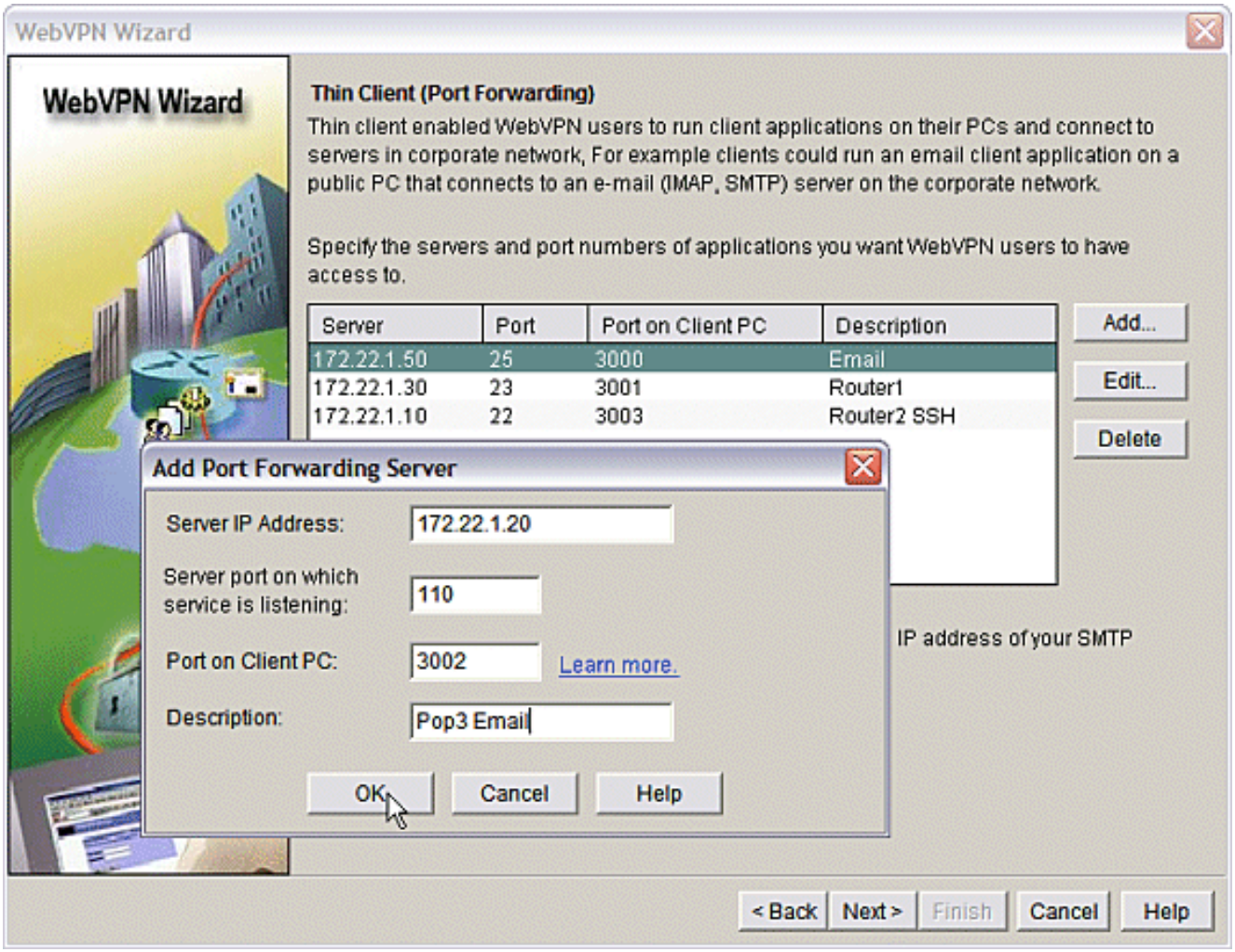
Elija el contexto WebVPN y el grupo de usuarios en los menús desplegables. Haga clic en Next
(Siguiente).



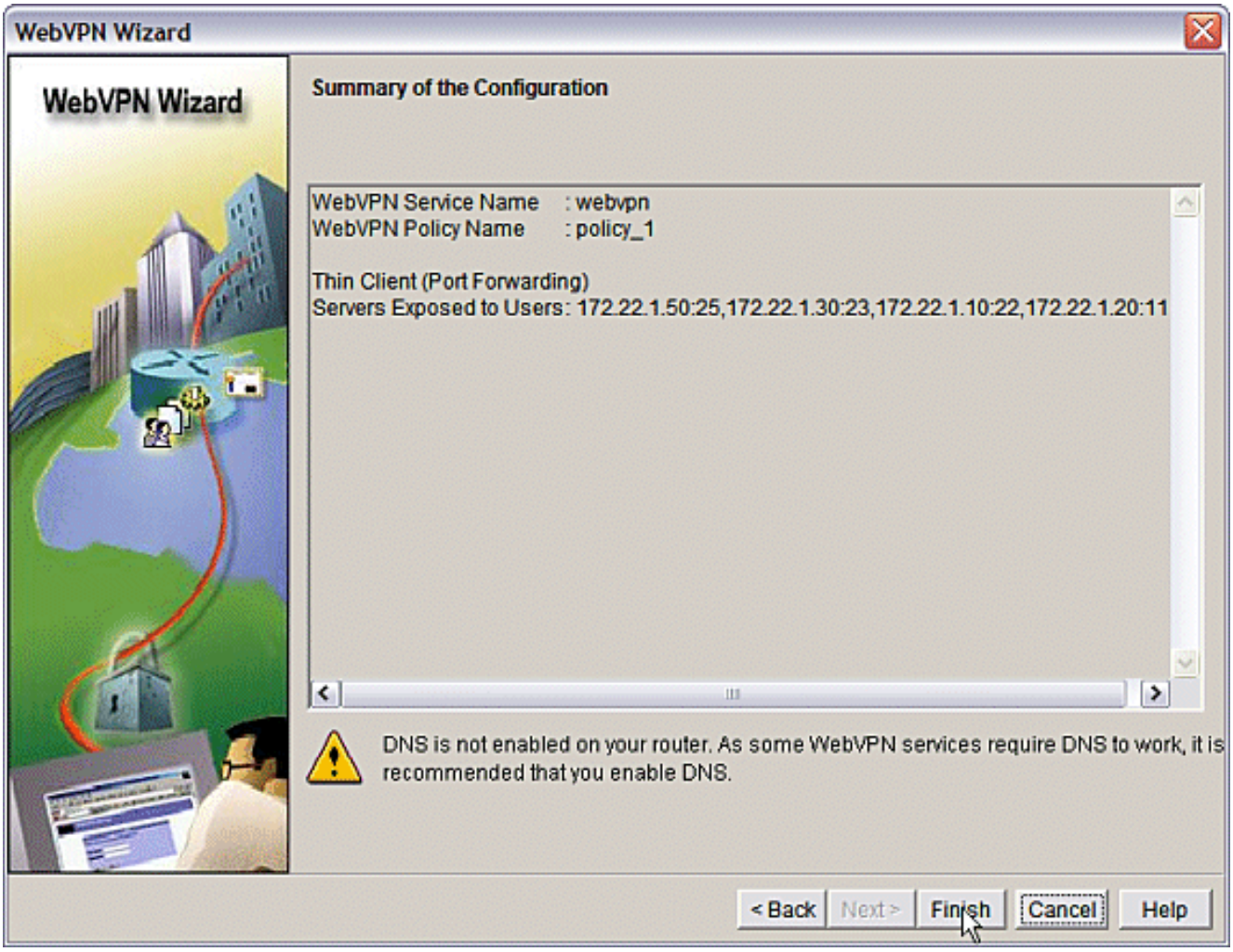
Elija **Thin Client (Port Forwarding)** y haga clic en **Next**.



Introduzca los recursos que desea poner a disposición a través de Port Forwarding (Reenvío de puertos). El puerto de servicio debe ser un puerto estático, pero puede aceptar el puerto predeterminado en el equipo cliente asignado por el asistente. Haga clic en Next (Siguiente).



Vista previa del resumen de configuración y haga clic en **Finalizar > Aceptar > Guardar**.



Configuración

Resultados de la configuración de 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/
```

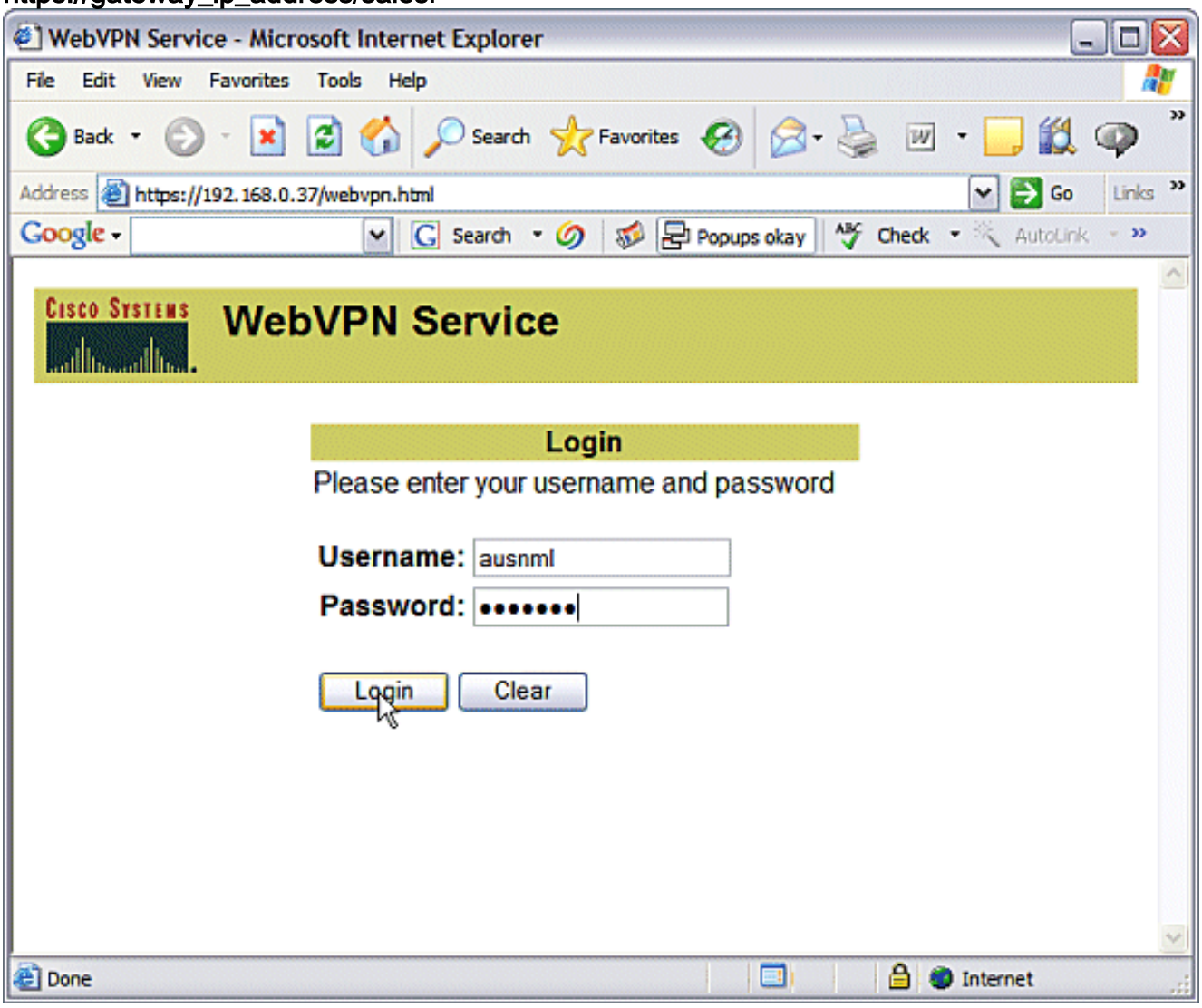
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm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

Verificación

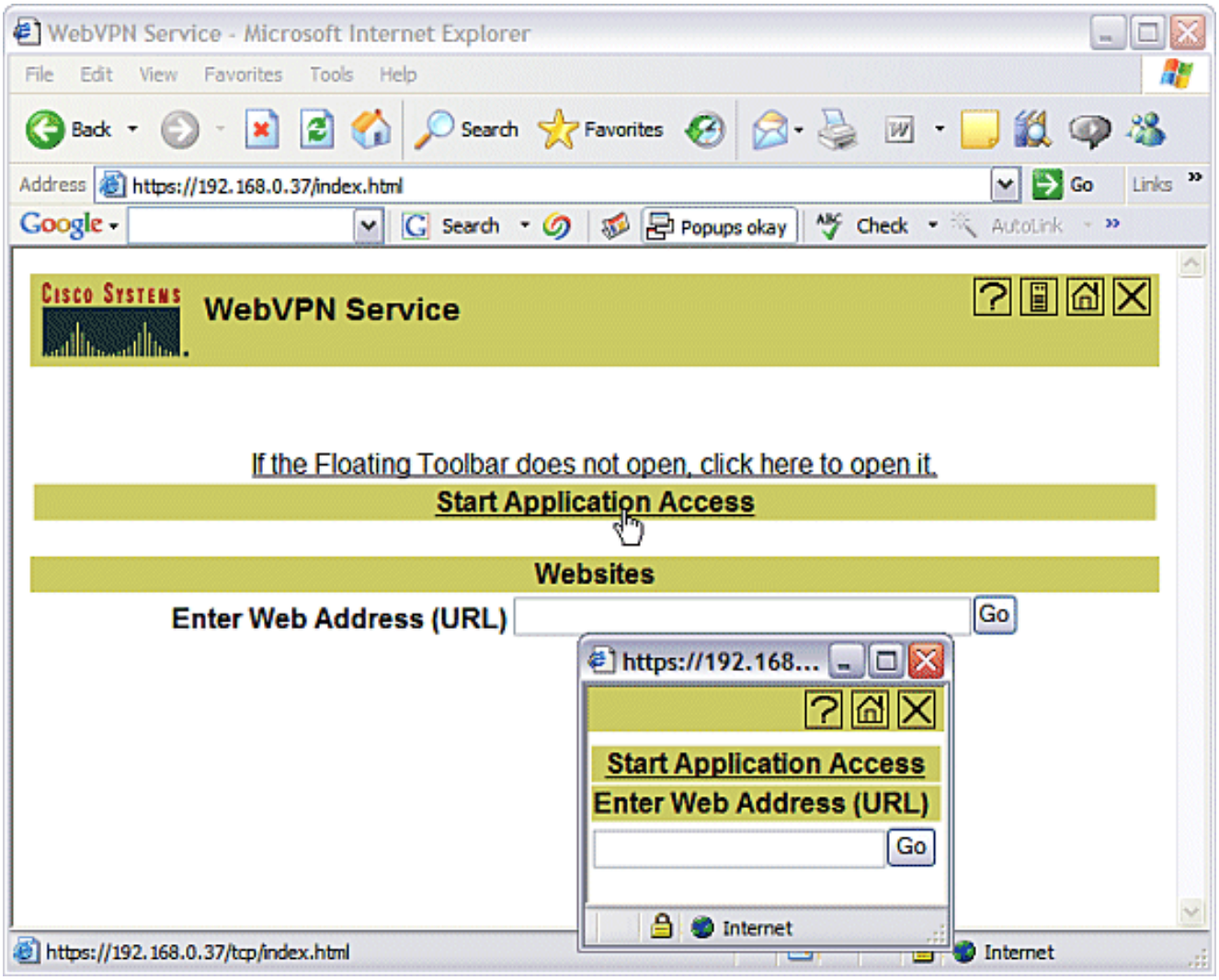
Verifique su configuración

Use esta sección para confirmar que su configuración funciona correctamente.

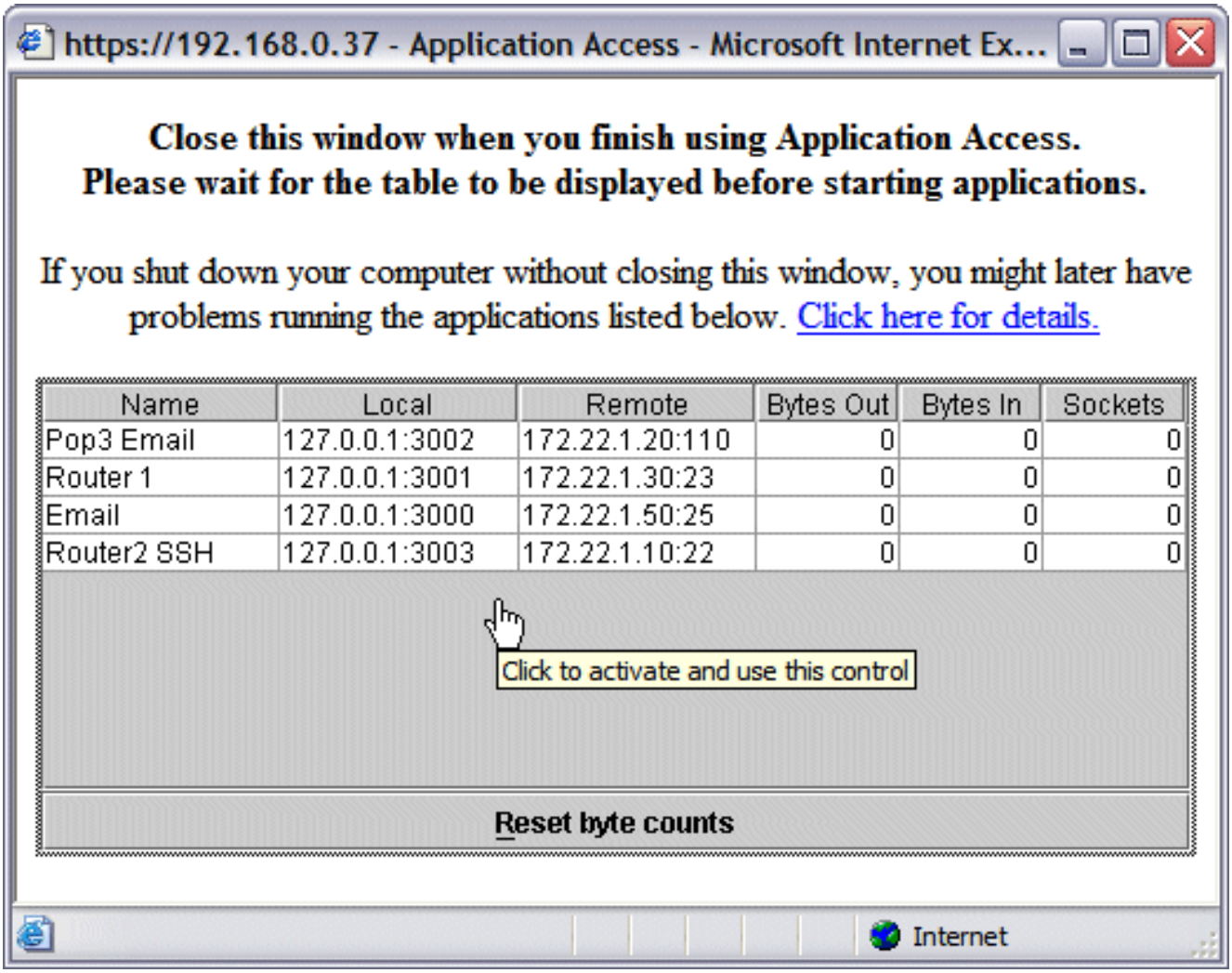
1. Utilice un equipo cliente para acceder al gateway WebVPN en **https://gateway_ip_address.** Recuerde incluir el nombre de dominio WebVPN si crea contextos WebVPN únicos. Por ejemplo, si ha creado un dominio llamado ventas, ingrese **https://gateway_ip_address/sales**.



2. Inicie sesión y acepte el certificado ofrecido por el gateway de WebVPN. Haga clic en **Iniciar acceso a la aplicación**.



3. Se muestra una pantalla Application Access (Acceso a la aplicación). Puede acceder a una aplicación con el número de puerto local y la dirección IP de loopback local. Por ejemplo, para Telnet al Router 1, ingrese **telnet 127.0.0.1 3001**. El pequeño applet Java envía esta información al gateway de WebVPN, que luego une los dos extremos de la sesión de forma segura. Las conexiones exitosas pueden hacer que las columnas **Bytes Out** y **Bytes In** aumenten.



Comandos

Varios **comandos show se asocian a WebVPN.** Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Para ver el uso de los comandos **show** en detalle, consulte Verificación de la Configuración de WebVPN.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Troubleshoot

Use esta sección para resolver problemas de configuración.

Los equipos cliente deben cargarse con la versión 1.4 o posterior de SUN Java. Obtenga una copia de este software de la descarga de software Java

Comandos Usados para Troubleshooting

Nota: Consulte Información Importante sobre Comandos Debug antes del uso de **comandos debug**.

- **show webvpn ?**—Hay muchos **comandos show** asociados con WebVPN. Se pueden realizar en la CLI para mostrar estadísticas y otra información. Para ver el uso de los comandos **show**

en detalle, consulte Verificación de la Configuración de WebVPN.

- **debug webvpn ?**—El uso de los comandos **debug** puede afectar negativamente al router. Para ver el uso de los comandos **debug** con más detalle, consulte Uso de los Comandos Debug WebVPN.

Información Relacionada

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Preguntas y respuestas sobre Cisco IOS WebVPN
- Soporte Técnico y Documentación - Cisco Systems