Configurer Cisco IOS VPN SSL client léger (WebVPN) avec SDM

Contenu

Introduction

La technologie VPN SSL client léger peut être utilisée pour permettre un accès sécurisé aux applications qui utilisent des ports statiques. Exemples : Telnet (23), SSH (22), POP3 (110), IMAP4 (143) et SMTP (25). Le client léger peut être piloté par l'utilisateur, piloté par des politiques, ou les deux. L'accès peut être configuré utilisateur par utilisateur, ou des stratégies de groupe qui incluent un ou plusieurs utilisateurs peuvent être créées. La technologie VPN SSL peut être configurée en trois modes principaux : VPN SSL sans client (WebVPN), VPN SSL client léger (transfert de port) et client VPN SSL (mode tunnel SVC-Full).

1. VPN SSL sans client (WebVPN) :

Un client distant a seulement besoin d'un navigateur Web compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur le LAN de l'entreprise. L'accès est également disponible pour parcourir des fichiers Windows avec le système de fichiers Common Internet File System (CIFS). Un bon exemple d'accès HTTP est le client Outlook Web Access (OWA).

Référez-vous à Exemple de configuration de VPN SSL sans client (WebVPN) sur Cisco IOS utilisant SDM afin d'en savoir plus sur le VPN SSL sans client.

2. VPN SSL client léger (transfert de port)

Un client distant doit télécharger un petit applet Javas pour l'accès sécurisé des applications TCP qui utilisent des numéros de port statiques. UDP n'est pas pris en charge. Les exemples incluent l'accès à POP3, SMTP, IMAP, SSH et Telnet. L'utilisateur doit disposer de privilèges d'administration locaux parce que des modifications sont apportées à des fichiers sur l'ordinateur local. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, par exemple, plusieurs applications FTP.

3. Client VPN SSL (mode de tunnel SVC-Full) :

Le client VPN SSL télécharge un petit client sur le poste de travail distant et permet un accès total et sécurisé aux ressources sur le réseau d'entreprise interne. Le SVC peut être téléchargé de manière permanente sur le poste de travail distant, ou il peut être supprimé après la fin de la session sécurisée.

Référez-vous à Exemple de configuration du client VPN SSL (SVC) sur IOS à l'aide de SDM afin d'en savoir plus sur le client VPN SSL.

Ce document présente une configuration simple pour le VPN SSL client léger sur un routeur Cisco IOS®. Le VPN SSL client léger s'exécute sur les routeurs Cisco IOS suivants :

- Routeurs de la gamme Cisco 870, 1811, 1841, 2801, 2811, 2821 et 2851
- Routeurs de la gamme Cisco 3725, 3745, 3825, 3845, 7200 et 7301

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Configuration requise pour le routeur Cisco IOS

- Tous les routeurs répertoriés chargés avec SDM et une image avancée d'IOS version 12.4(6)T ou ultérieure
- Station de gestion chargée avec SDMCisco fournit de nouveaux routeurs avec une copie préinstallée de SDM. Si SDM n'est pas installé sur votre routeur, vous pouvez obtenir le logiciel sur Software Download-Cisco Security Device Manager. Vous devez posséder un compte CCO avec un contrat de service. Référez-vous à Configurer votre routeur avec Security Device Manager pour des instructions détaillées.

Configuration requise pour les ordinateurs clients

- Les clients distants doivent disposer de privilèges d'administration locaux ; il n'est pas nécessaire, mais il est fortement suggéré.
- Les clients distants doivent disposer de Java Runtime Environment (JRE) version 1.4 ou ultérieure.
- Navigateurs clients distants : Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 ou Firefox 1.0
- Cookies activés et fenêtres publicitaires intempestives autorisées sur les clients distants

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Image logicielle Cisco Advanced Enterprise 12.4(9)T
- Routeur à services intégrés Cisco 3825
- Cisco Router and Security Device Manager (SDM) version 2.3.1

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont commencé par une configuration effacée (par défaut). If your network is live, make sure that you understand the potential impact of any command. Les adresses IP utilisées pour cette configuration proviennent de l'espace d'adressage RFC 1918. Ils ne sont pas légaux sur Internet.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

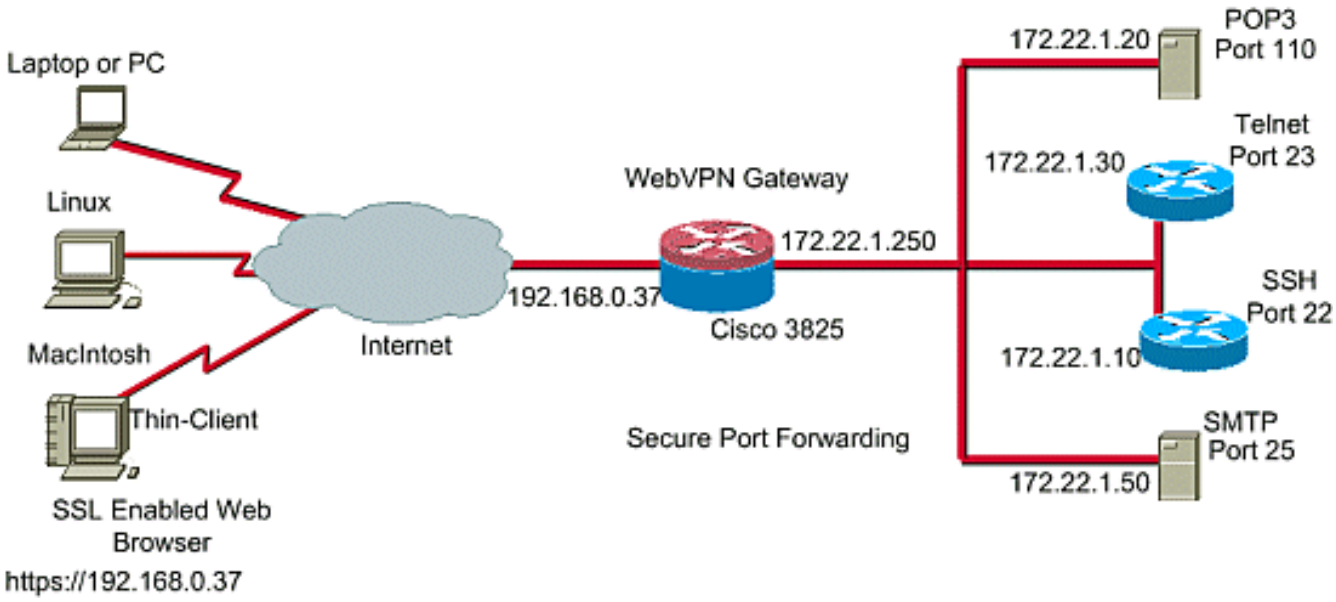
Configuration

Tâche

Cette section contient les informations requises pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

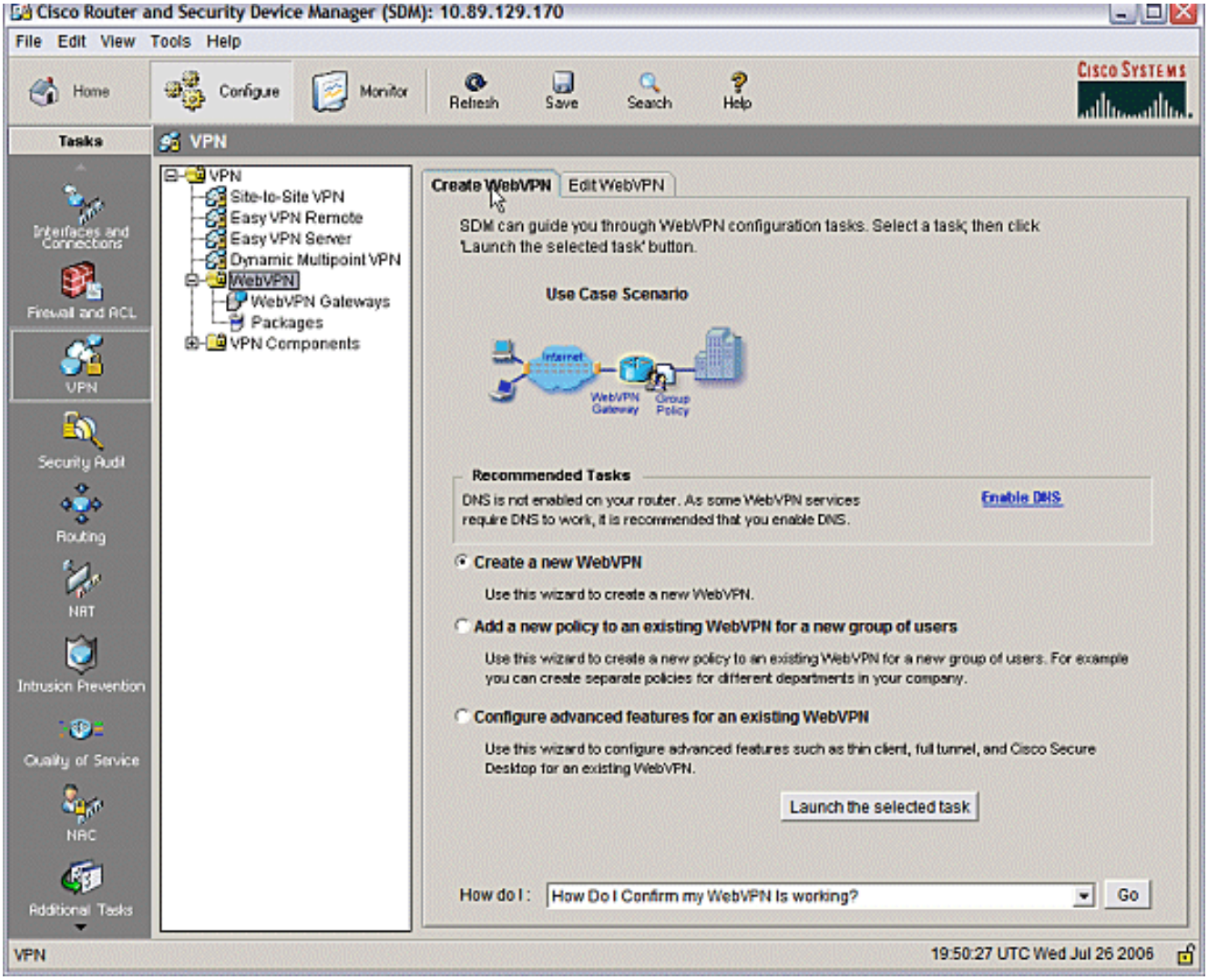
Ce document utilise la configuration réseau suivante :



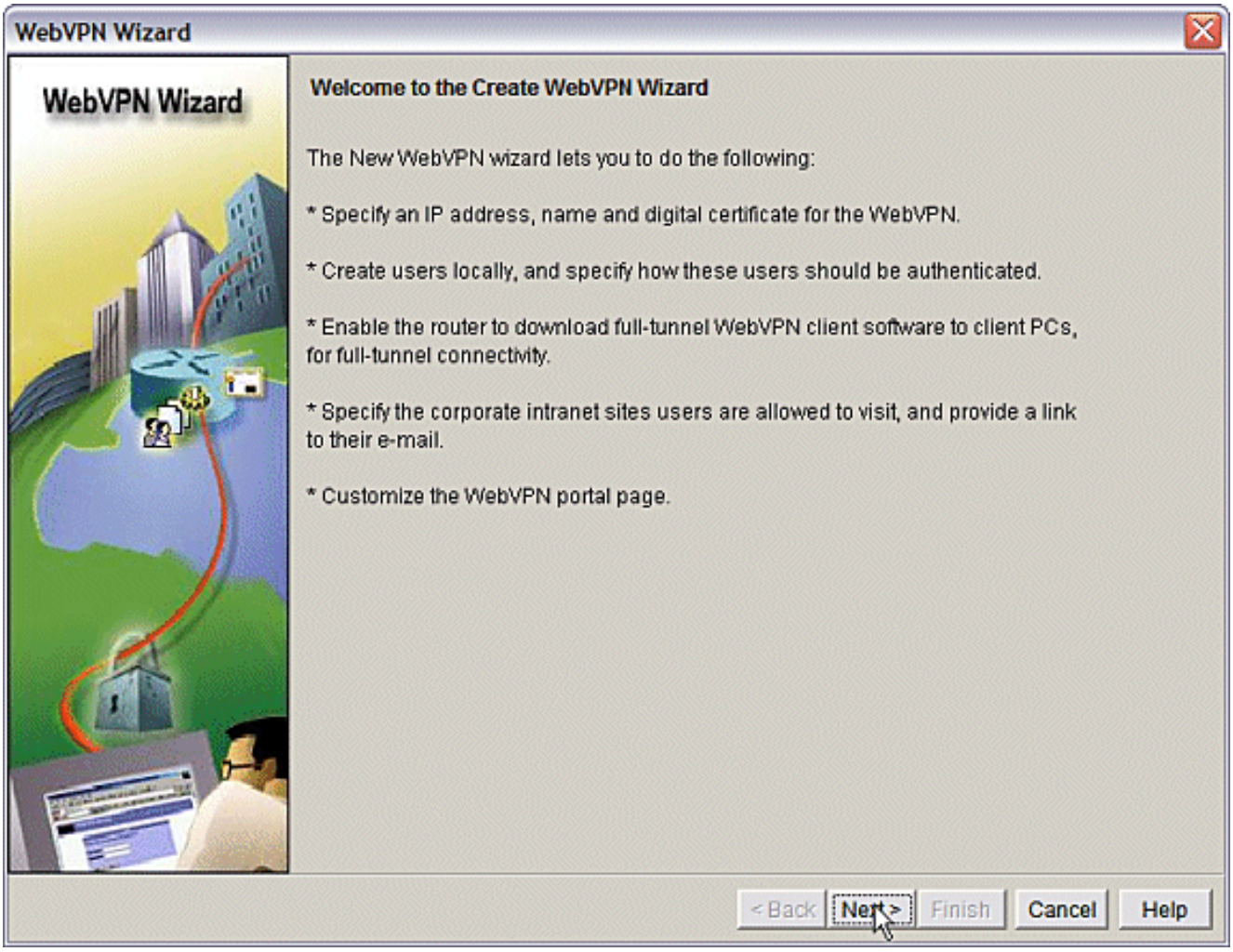
Configuration du VPN SSL client léger

Utilisez l'Assistant fourni dans l'interface SDM (Security Device Manager) pour configurer le VPN SSL client léger sur Cisco IOS, ou configurez-le soit à l'interface de ligne de commande (CLI), soit manuellement dans l'application SDM. Cet exemple utilise l'Assistant.

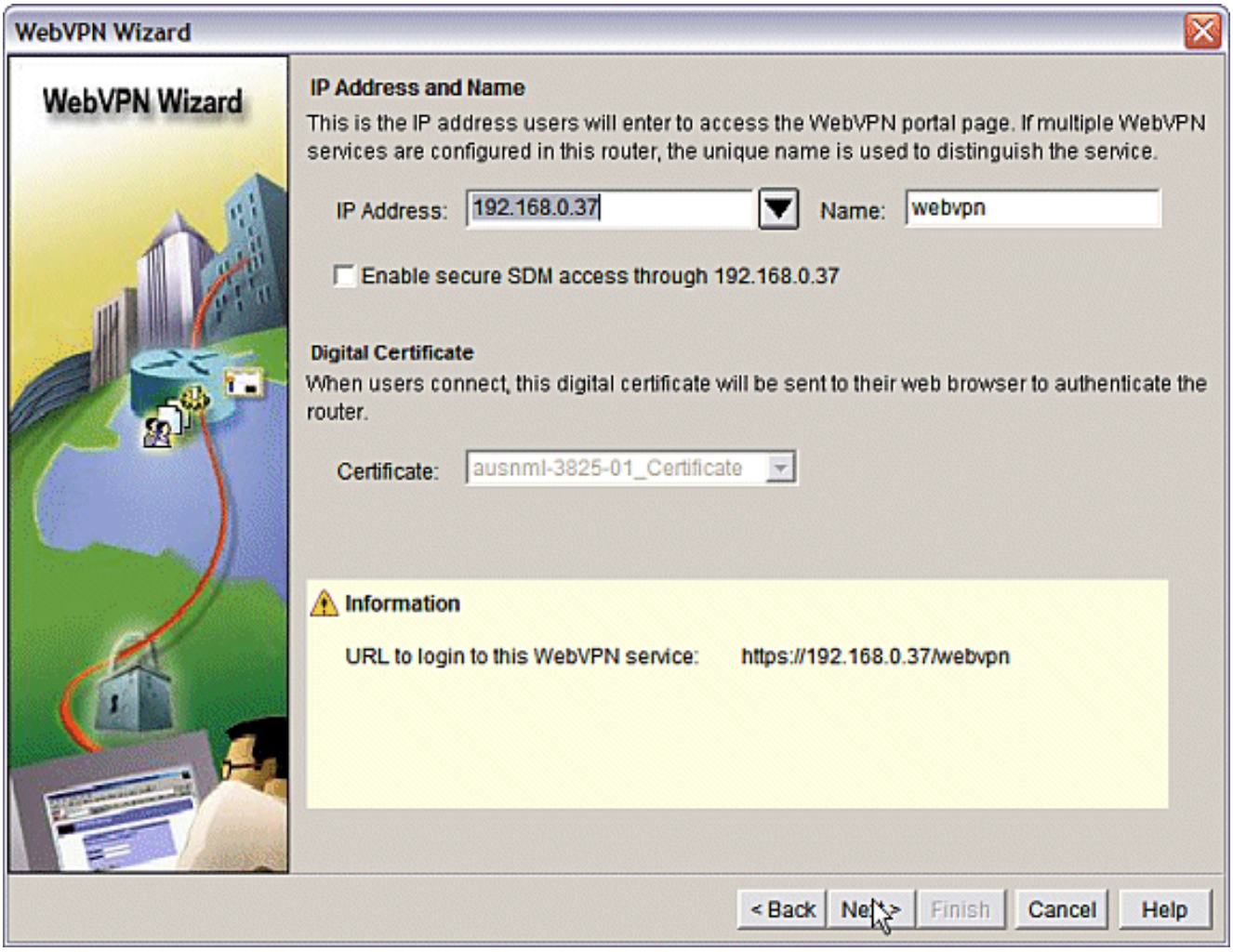
1. Sélectionnez l'onglet **Configurer**.Dans le volet de navigation, sélectionnez **VPN > WebVPN**.Cliquez sur l'onglet **Create WebVPN**.Activez la case d'option en regard de **Create a new WebVPN**.Cliquez sur le bouton **Lancer la tâche sélectionnée**.



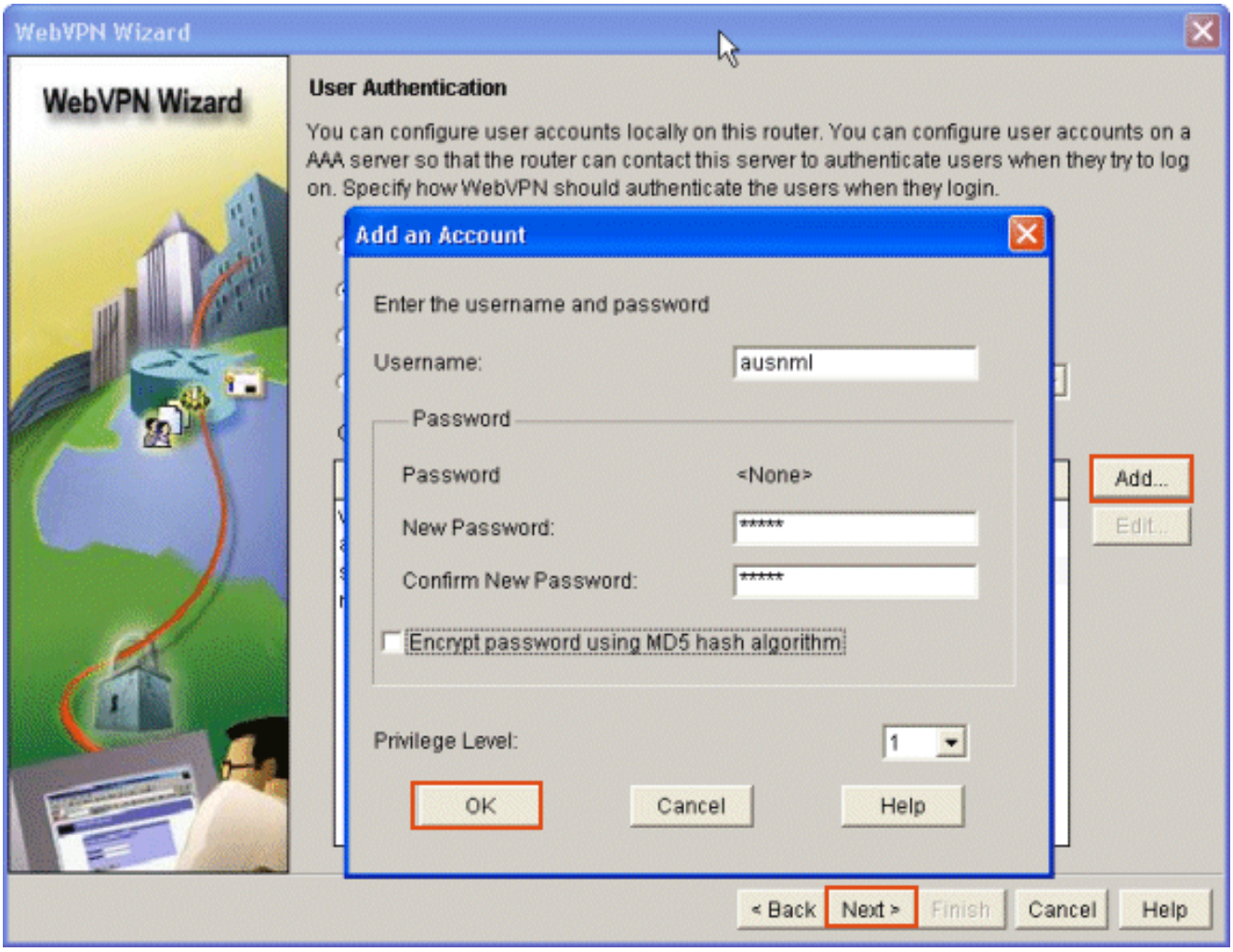
2. L'Assistant WebVPN démarre. Cliquez sur **Next** (Suivant).



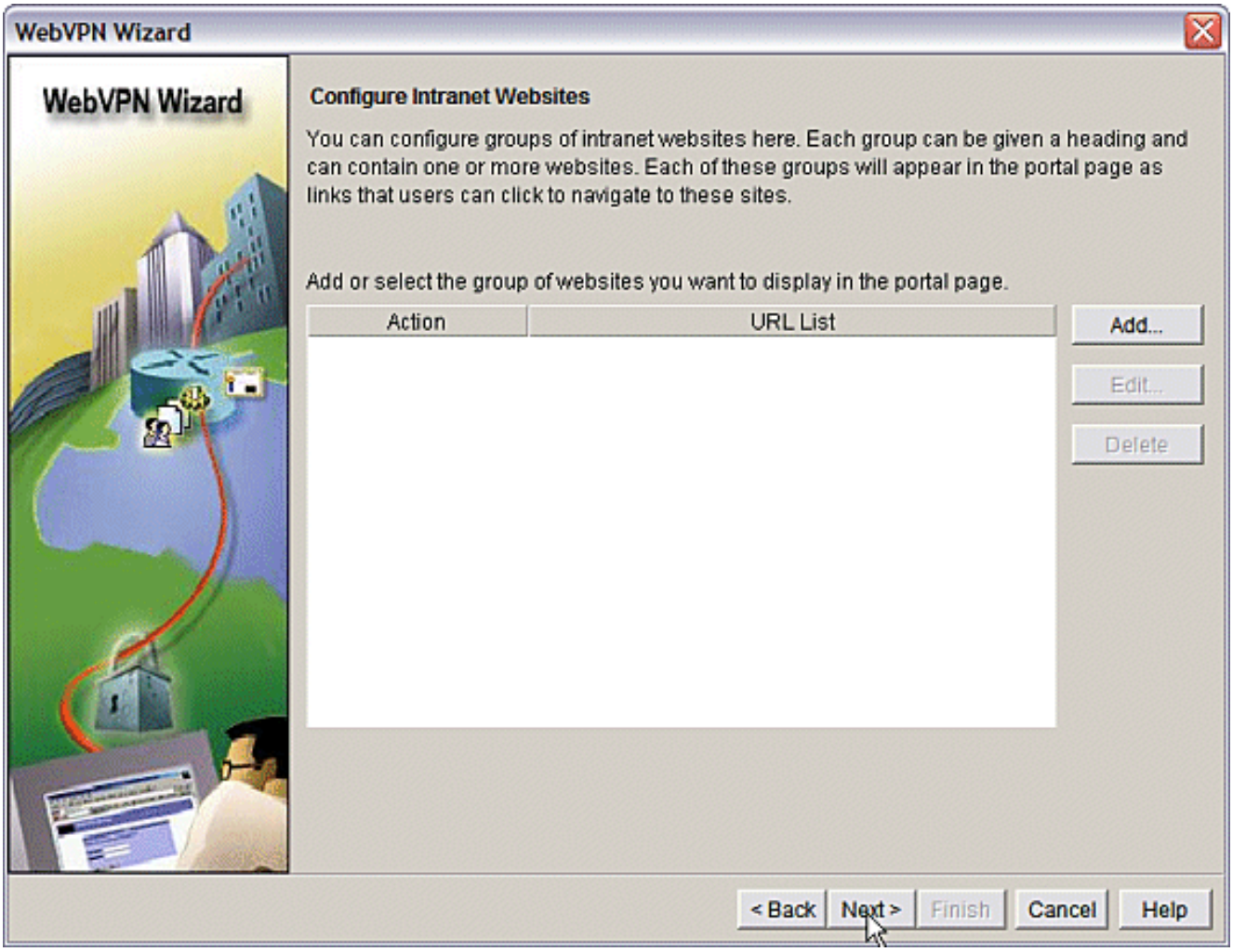
Entrez l'adresse IP et un nom unique pour cette passerelle WebVPN. Cliquez sur **Next** (Suivant).



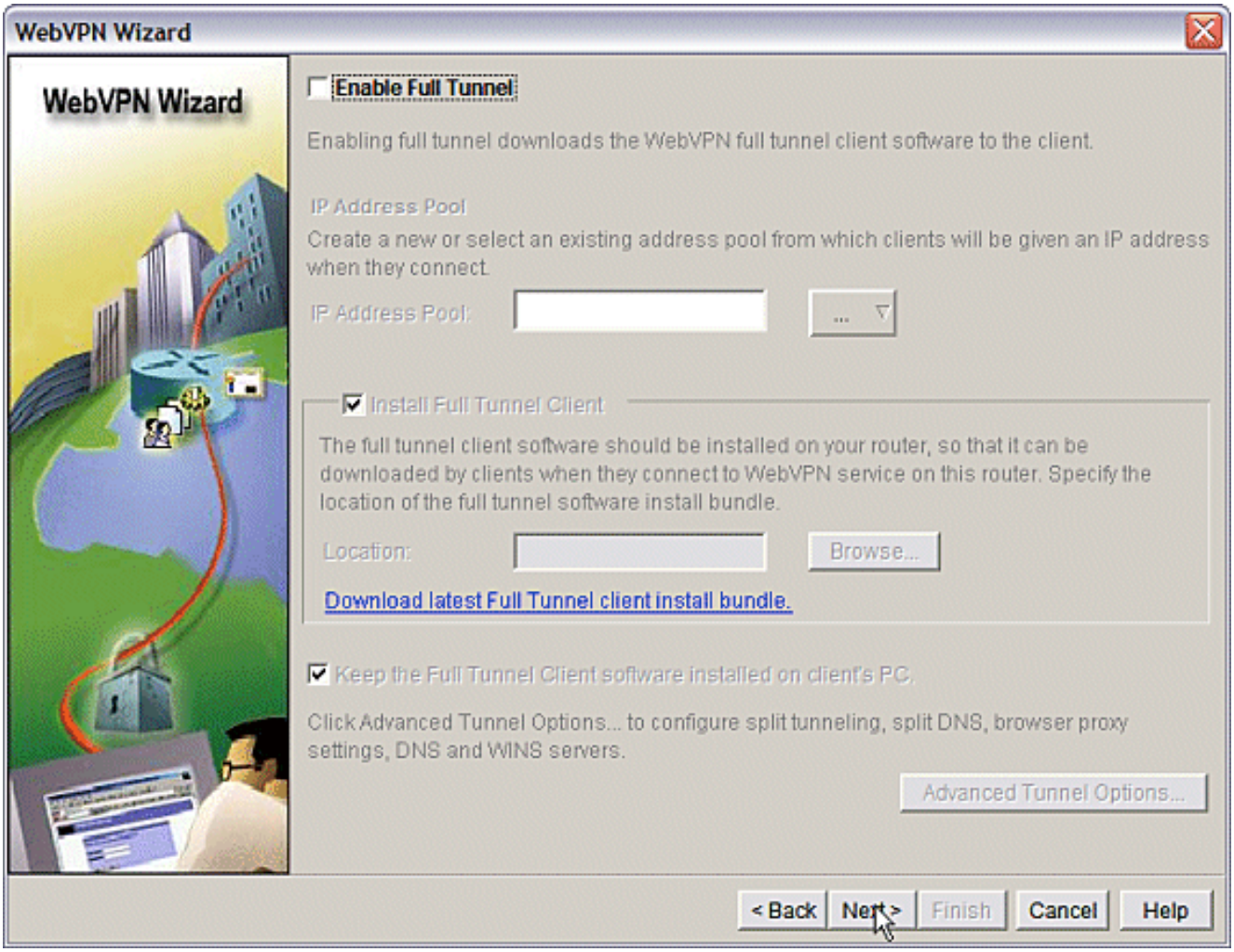
3. L'écran User Authentication (Authentification utilisateur) permet de fournir l'authentification des utilisateurs. Cette configuration utilise un compte créé localement sur le routeur. Vous pouvez également utiliser un serveur AAA (Authentication, Authorization, and Accounting).Pour ajouter un utilisateur, cliquez sur **Ajouter**.Entrez les informations utilisateur dans l'écran Ajouter un compte, puis cliquez sur **OK**.Cliquez sur **Suivant** dans l'écran Authentification
utilisateur.



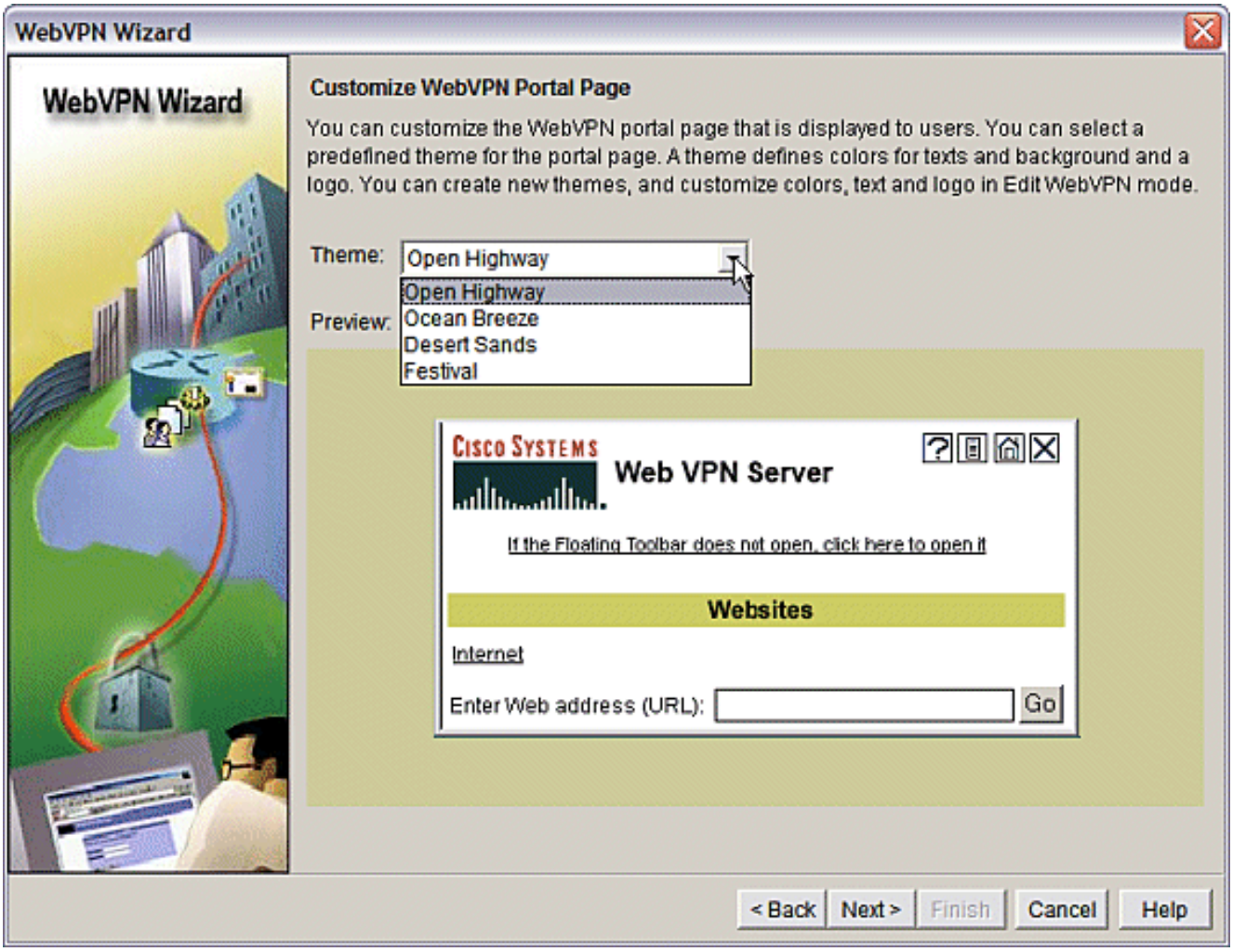
L'écran WebVPN Wizard permet de configurer des sites Web intranet, mais cette étape est omise car Port-Forwarding est utilisé pour cet accès d'application. Si vous souhaitez autoriser l'accès à des sites Web, utilisez les configurations VPN SSL sans client ou client complet, qui ne sont pas dans le champ d'application de ce document.



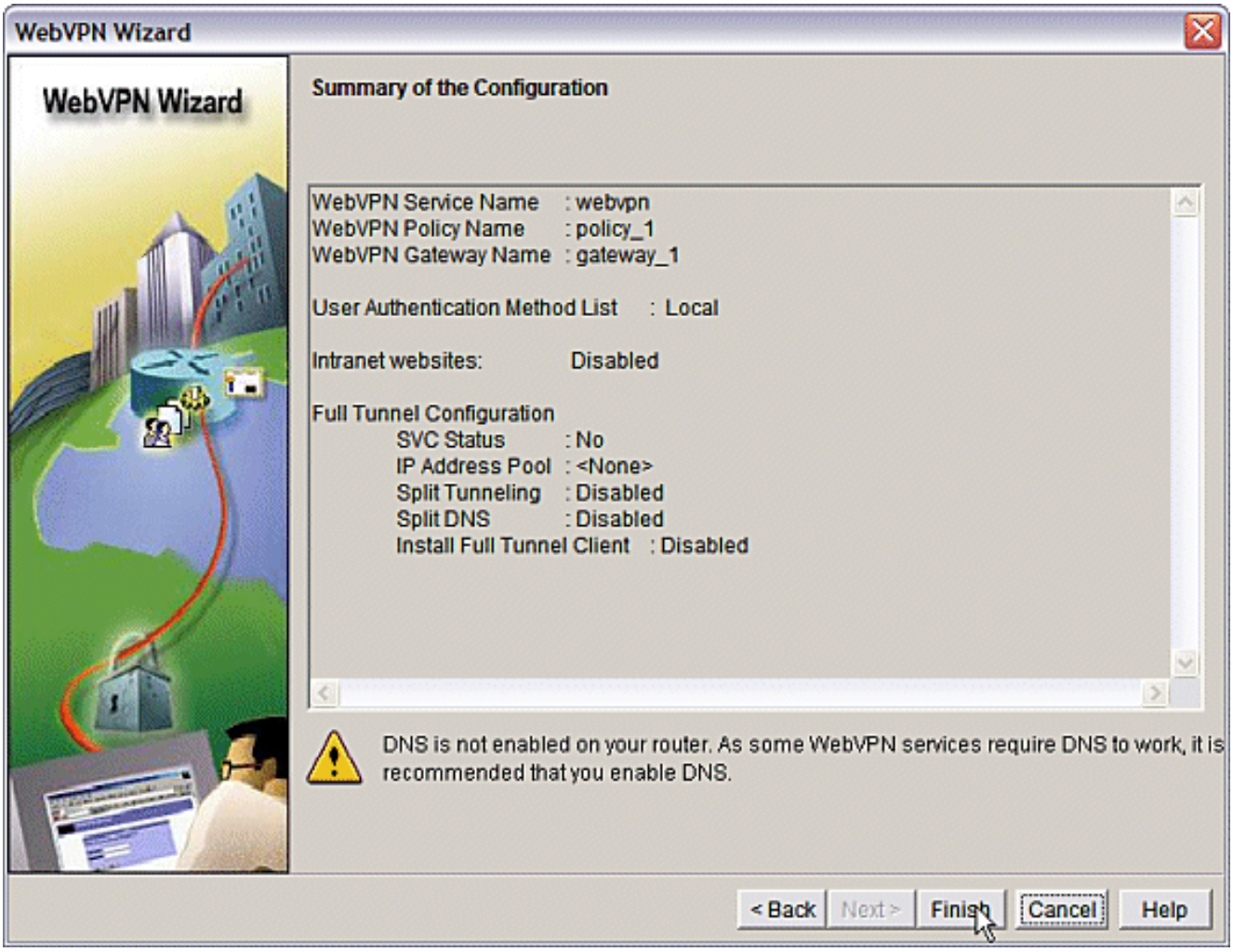
Cliquez sur **Next** (Suivant). L'Assistant affiche un écran qui permet de configurer le client Full Tunnel. Cela ne s'applique pas au VPN SSL client léger (transfert de port).Désélectionnez **Activer le tunnel complet**. Cliquez sur **Next**
(Suivant).



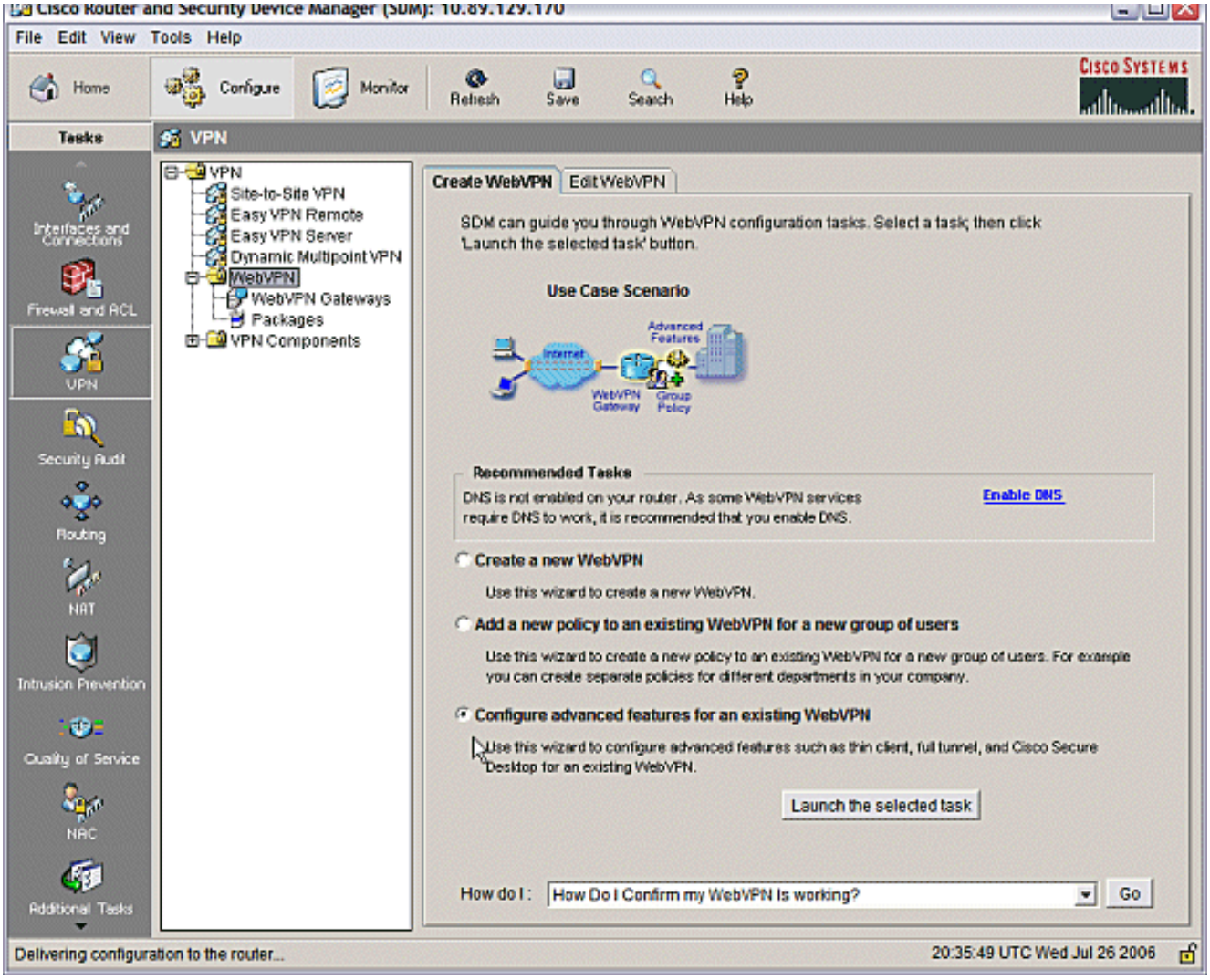
4. Personnalisez l'apparence de la page du portail WebVPN ou acceptez l'apparence par défaut.Cliquez sur **Next**
(Suivant).



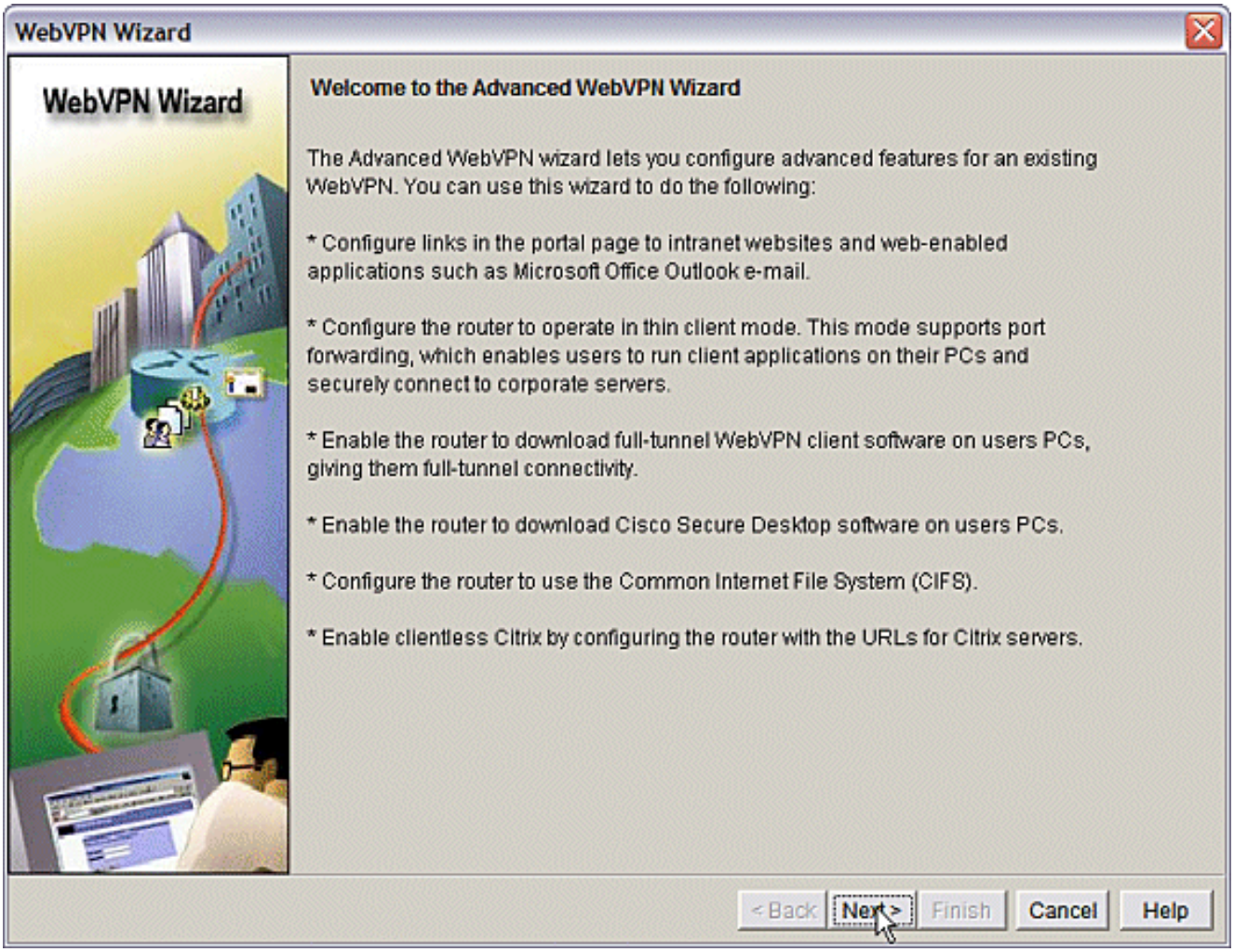
Affichez un aperçu du récapitulatif de la configuration et cliquez sur **Terminer > Enregistrer**.



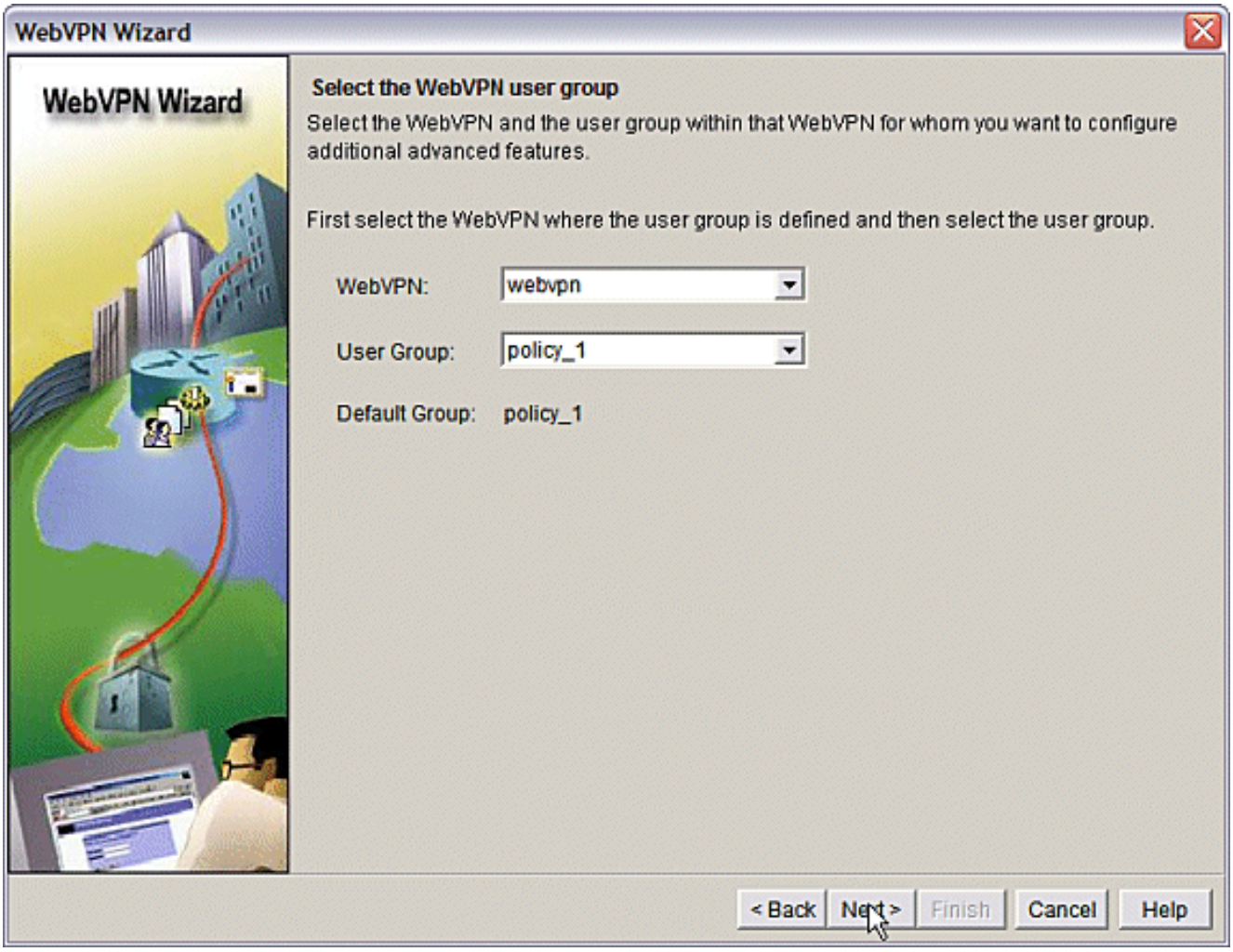
5. Vous avez créé une passerelle WebVPN et un contexte WebVPN avec une stratégie de groupe liée. Configurez les ports client léger, qui sont rendus disponibles lorsque les clients se connectent au WebVPN.Choisissez **Configurer**.Choisissez **VPN > WebVPN**.Choisissez **Create WebVPN**.Sélectionnez la case d'option **Configurer les fonctionnalités avancées pour un WebVPN existant** et cliquez sur **Lancer la tâche sélectionnée**.



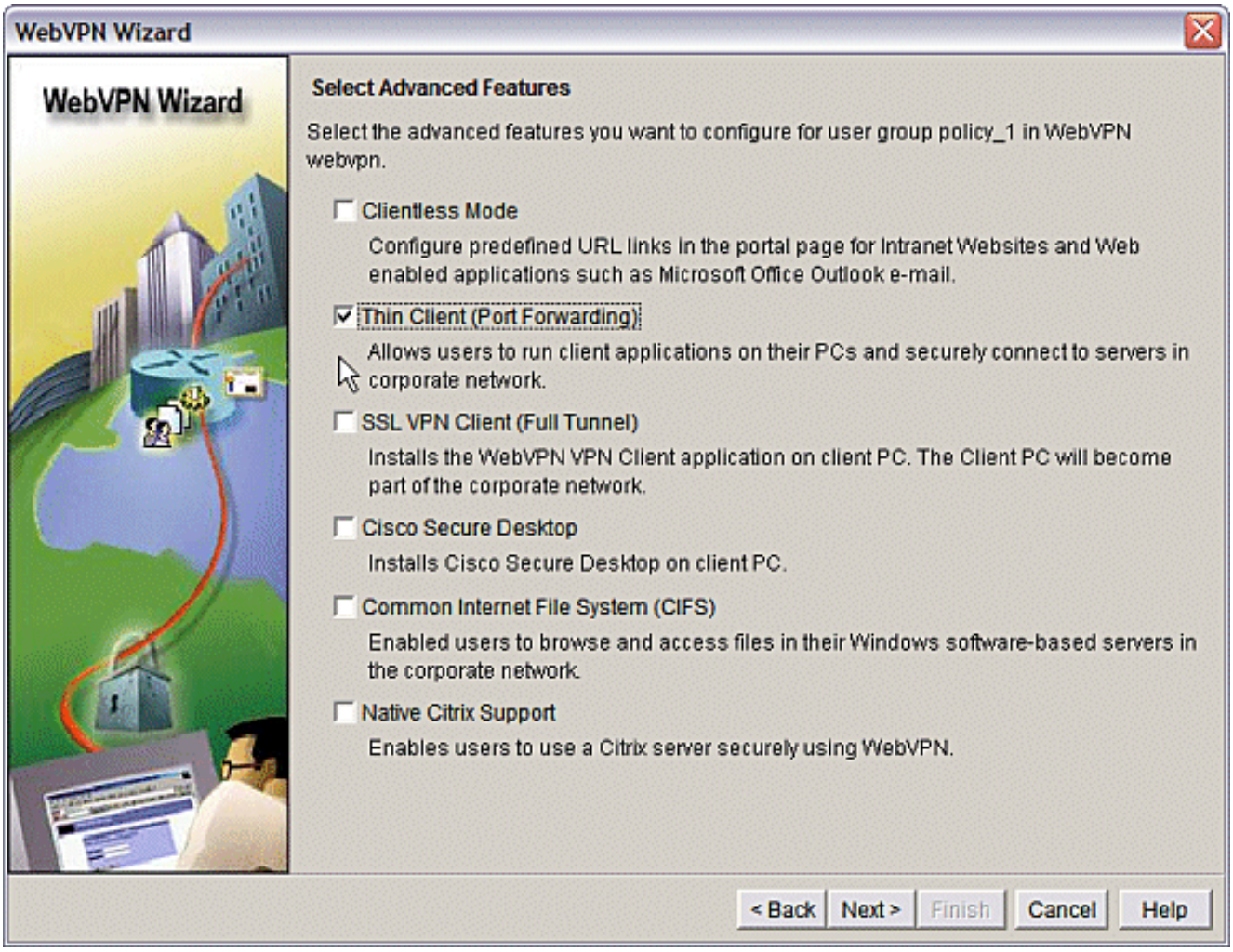
L'écran Welcome (Bienvenue) présente les fonctionnalités de l'Assistant. Cliquez sur **Next** (Suivant).



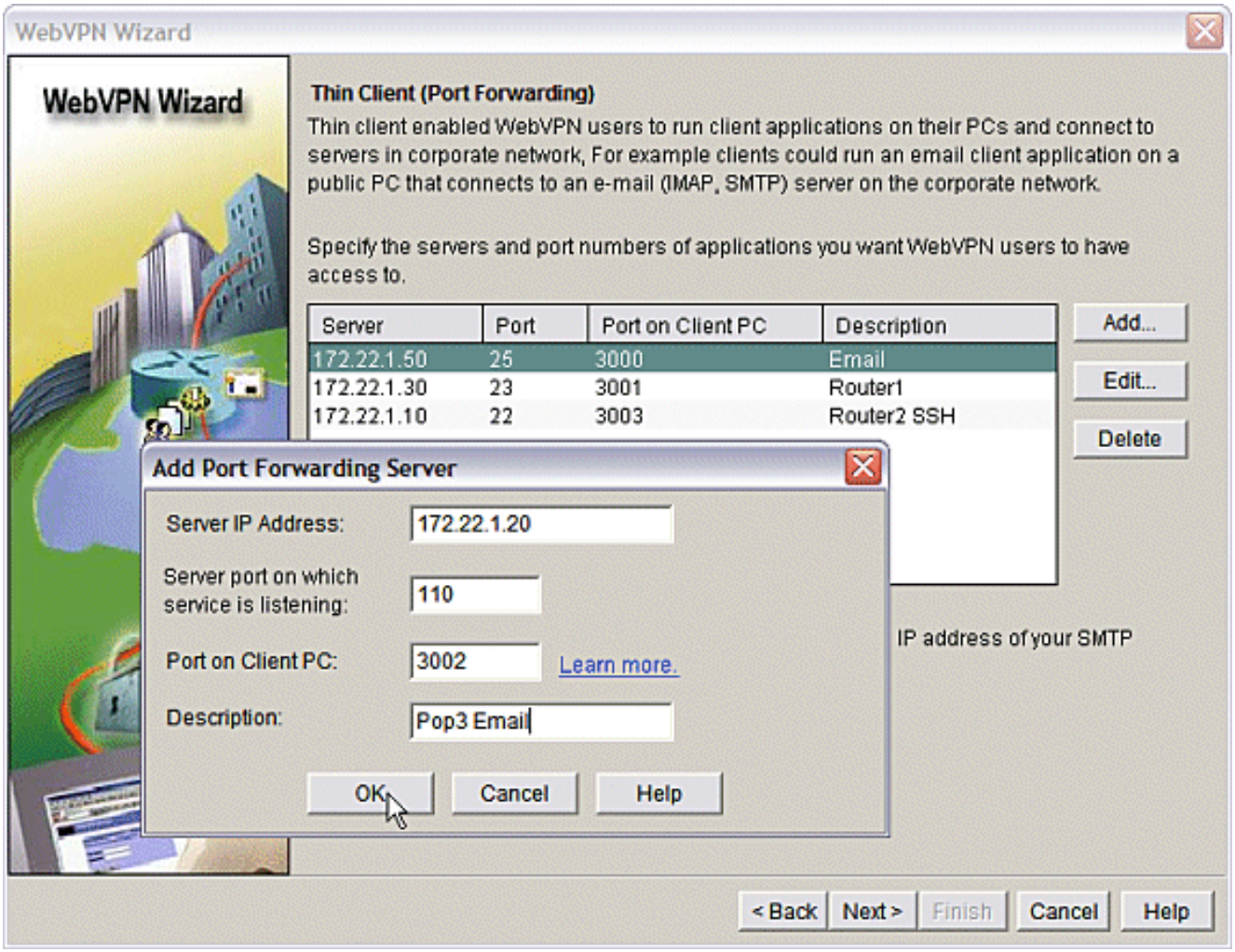
Sélectionnez le contexte WebVPN et le groupe d'utilisateurs dans les menus déroulants. Cliquez sur **Next**
(Suivant).



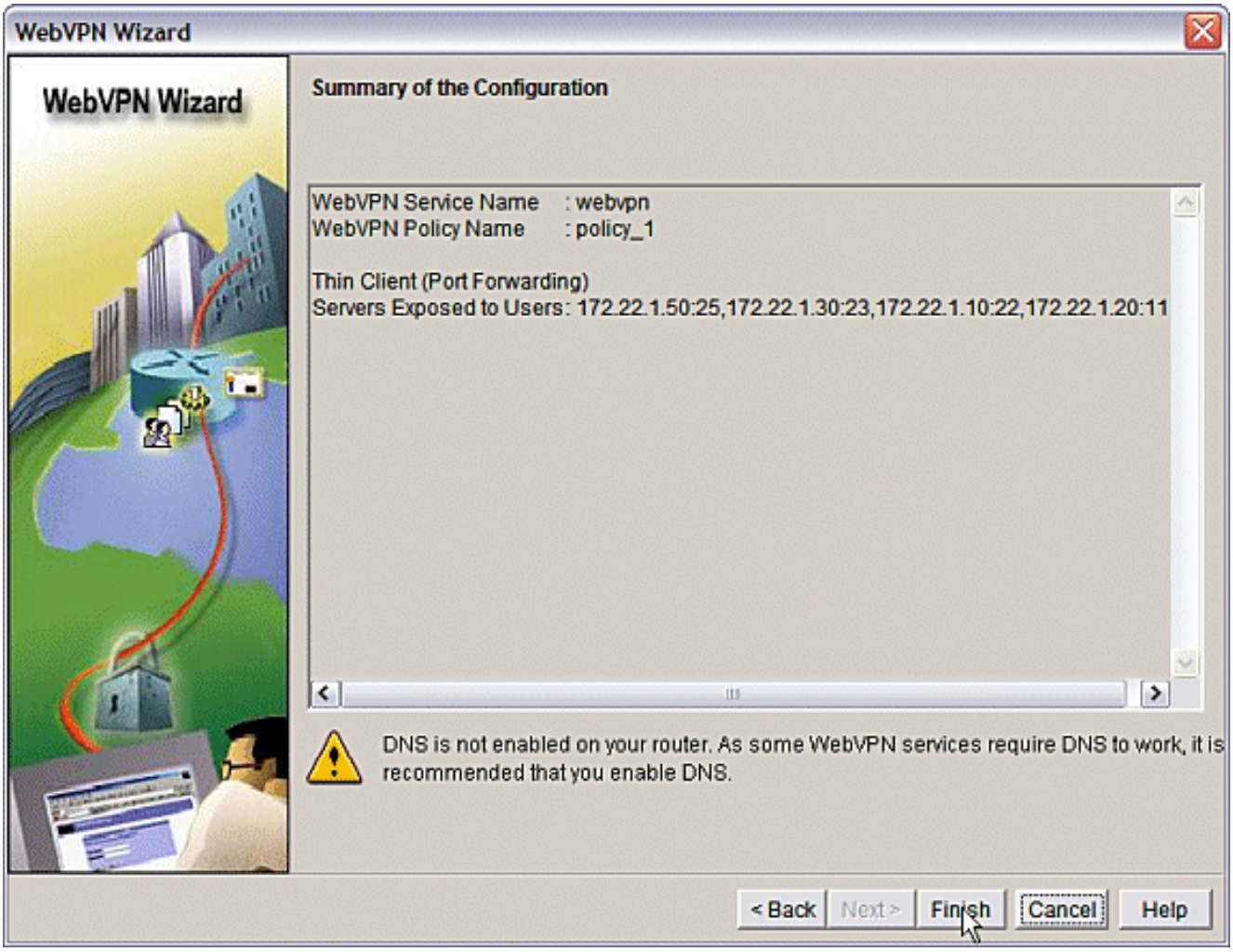
Choisissez **Client léger (Transfert de port)** et cliquez sur **Suivant**.



Saisissez les ressources que vous souhaitez rendre disponibles via Port Forwarding. Le port de service doit être un port statique, mais vous pouvez accepter le port par défaut sur le PC client attribué par l'Assistant. Cliquez sur **Next**
(Suivant).



Affichez un aperçu de votre configuration et cliquez sur **Terminer > OK > Enregistrer**.



Configuration

Résultats de la configuration 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/
```

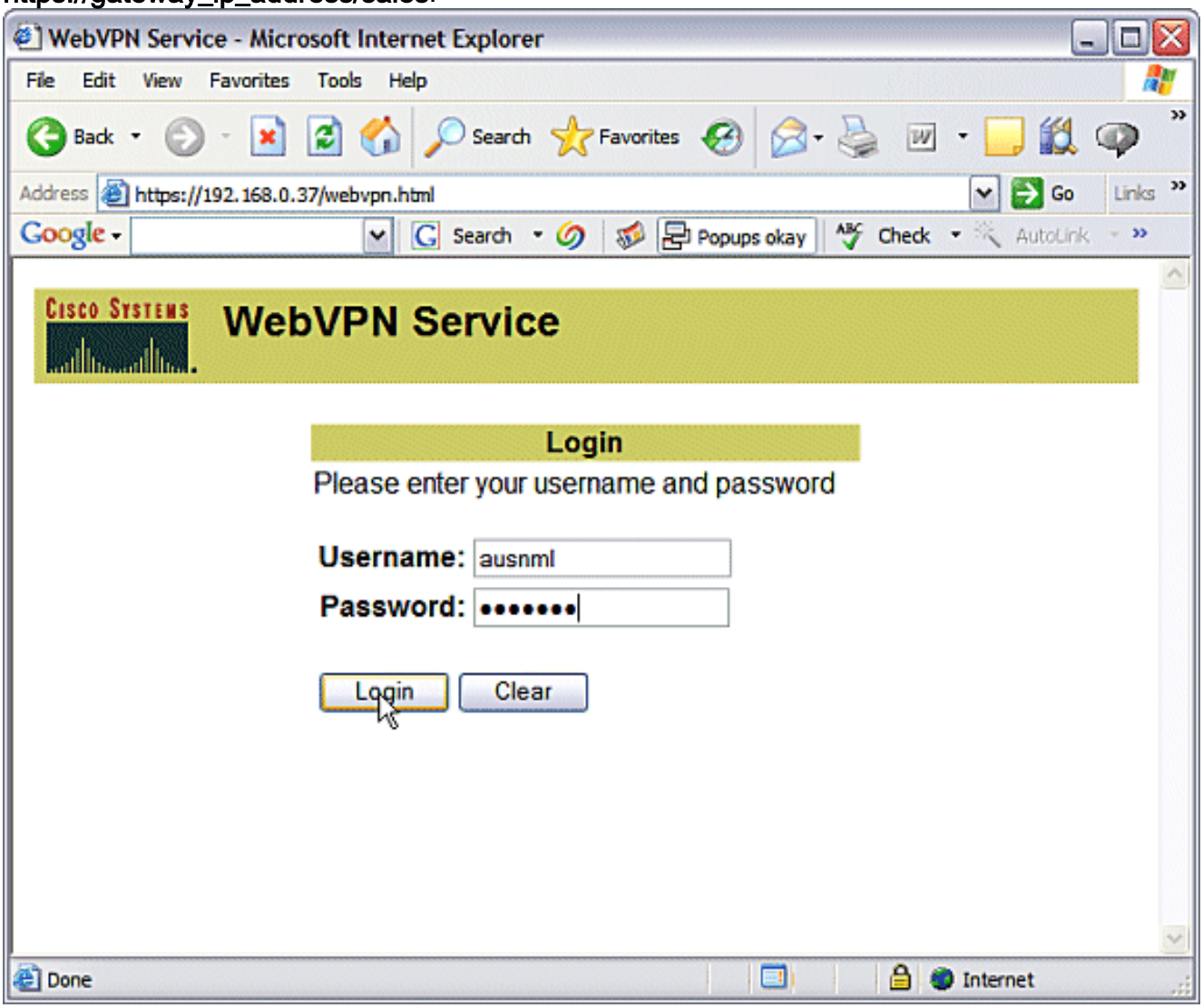
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm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

Vérification

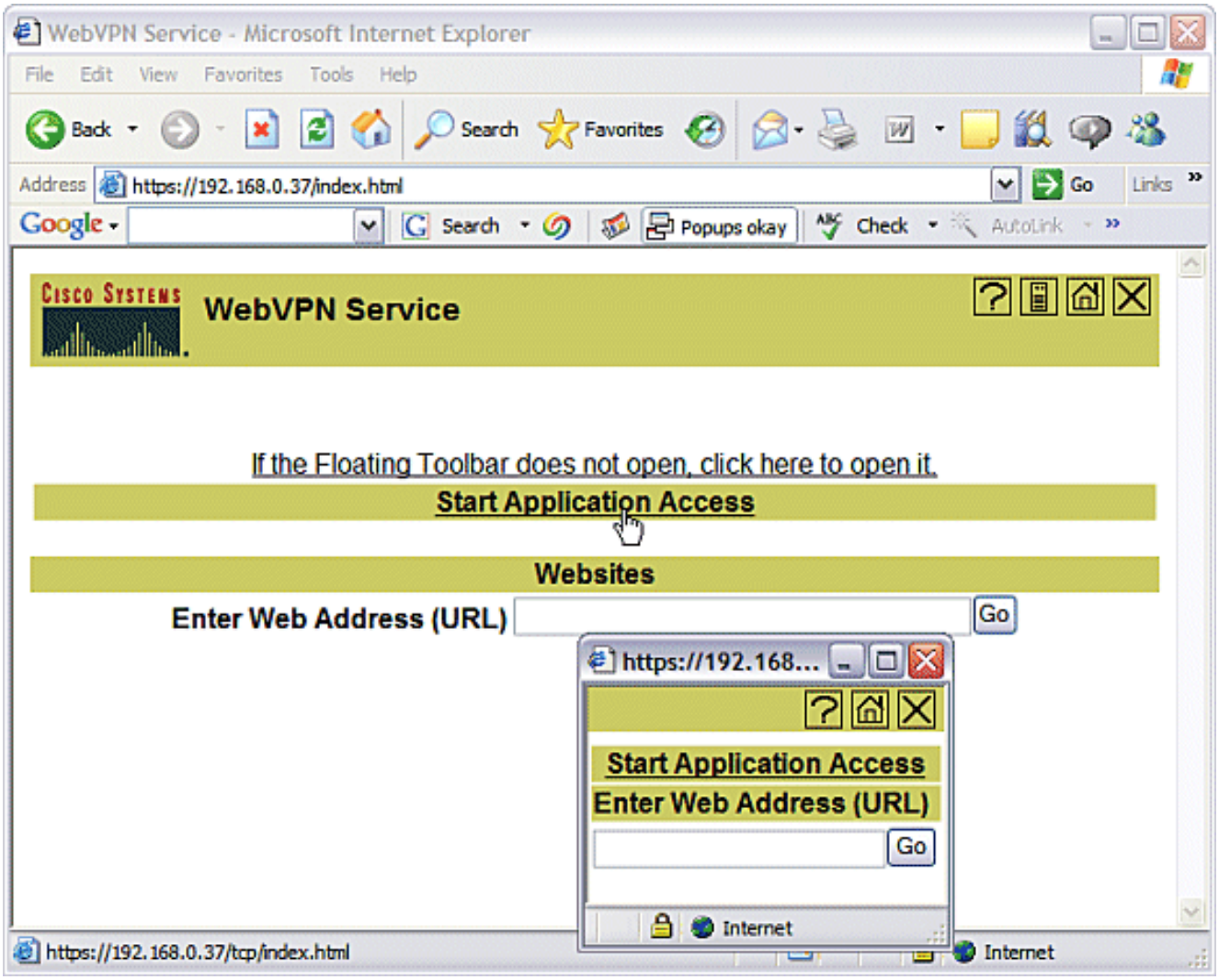
Vérifier votre configuration

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

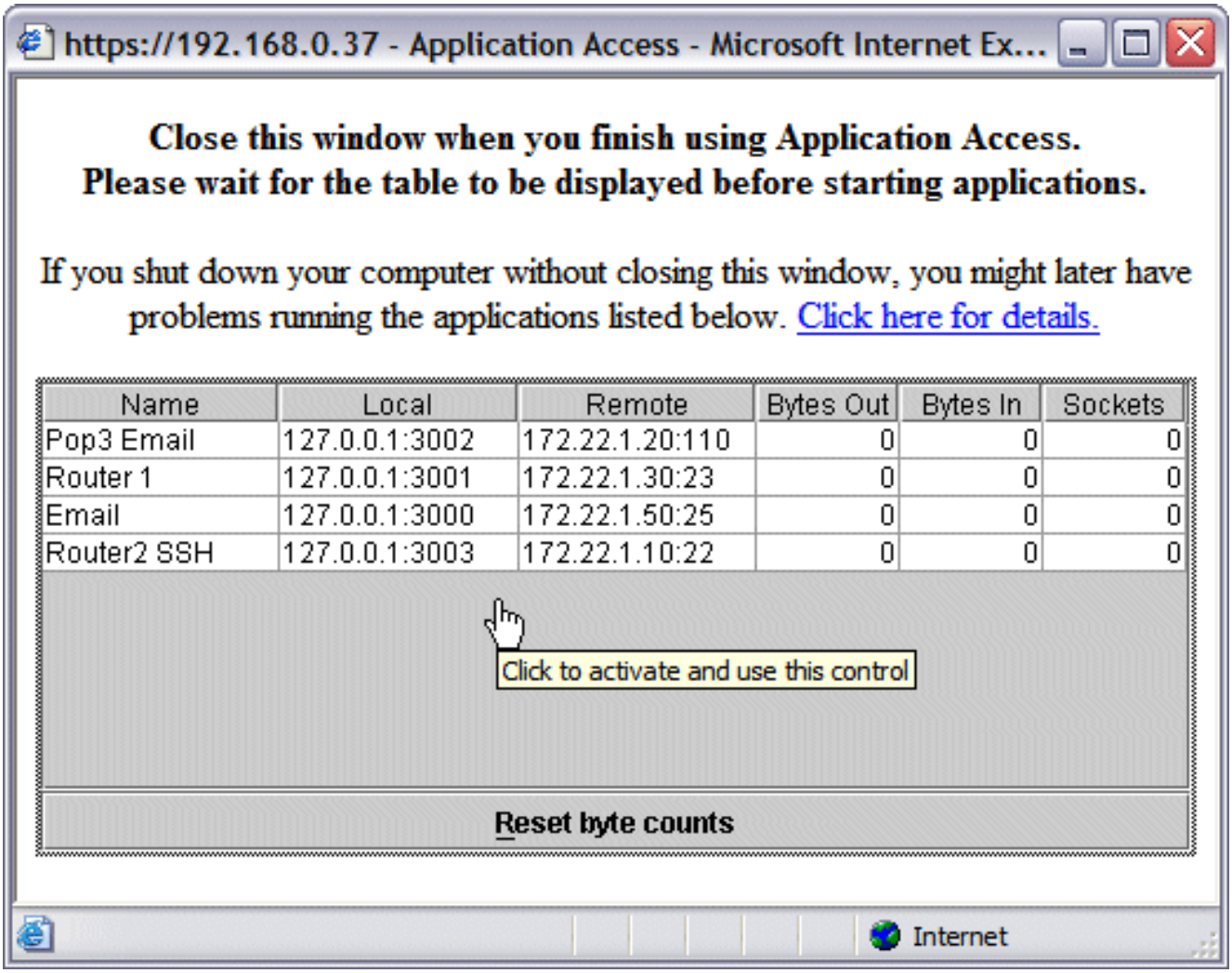
1. Utilisez un ordinateur client pour accéder à la passerelle WebVPN à l'adresse **https://gateway_ip_address.** N'oubliez pas d'inclure le nom de domaine WebVPN si vous créez des contextes WebVPN uniques. Par exemple, si vous avez créé un domaine appelé ventes, saisissez **https://gateway_ip_address/sales**.



2. Connectez-vous et acceptez le certificat offert par la passerelle WebVPN. Cliquez sur **Start Application Access**.



3. Un écran Application Access s'affiche. Vous pouvez accéder à une application avec le numéro de port local et votre adresse IP de bouclage local. Par exemple, pour établir une connexion Telnet avec le routeur 1, entrez **telnet 127.0.0.1 3001**. La petite applet Java envoie ces informations à la passerelle WebVPN, qui relie ensuite les deux extrémités de la session de manière sécurisée. Les connexions réussies peuvent entraîner l'augmentation des colonnes **Bytes Out** et **Bytes In**.



Commandes

Plusieurs **commandes show sont associées à WebVPN.** Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour voir l'utilisation des commandes **show** en détail, référez-vous à Vérification de la configuration WebVPN.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

Dépannage

Utilisez cette section pour dépanner votre configuration.

Les ordinateurs clients doivent être chargés avec SUN Java Version 1.4 ou ultérieure. Obtenir une copie de ce logiciel à partir du téléchargement de logiciels Java

Commandes utilisées pour dépanner

Remarque : reportez-vous à Informations importantes sur les commandes de débogage avant d'utiliser les commandes **de débogage**.

- **show webvpn ?**—Il existe de nombreuses commandes **show** associées à WebVPN. Elles

peuvent être effectuées à l'interface de ligne de commande pour afficher des statistiques et d'autres informations. Afin de voir l'utilisation des commandes **show** en détail, référez-vous à Vérification de la configuration WebVPN.

- **debug webvpn ?**—L'utilisation des commandes **debug** peut avoir un impact négatif sur le routeur. Afin de voir l'utilisation des commandes de **débogage** plus en détail, référez-vous à Utilisation des commandes de débogage WebVPN.

Informations connexes

- Cisco IOS SSLVPN
- VPN SSL - WebVPN
- Questions et réponses sur Cisco IOS WebVPN
- Support et documentation techniques - Cisco Systems