Exemple de configuration d'un client VPN SSL (SVC) sur IOS avec SDM

Table des matières

Introduction

Le Client VPN SSL (SVC) fournit un tunnel complet pour les communications sécurisées au réseau d'entreprise interne. Vous pouvez configurer l'accès utilisateur par utilisateur, ou vous pouvez créer différents contextes WebVPN dans lesquels vous placez un ou plusieurs utilisateurs.

Le technologie VPN SSL ou WebVPN est prise en charge sur les plate-formes de routeur IOS suivantes :

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

Vous pouvez configurer la technologie VPN SSL dans les modes suivants :

- VPN SSL sans client (WebVPN) - Fournit un client distant nécessitant un navigateur Web

compatible SSL pour accéder à des serveurs Web HTTP ou HTTPS sur un réseau local d'entreprise (LAN). En outre, le VPN SSL sans client permet l'exploration de fichiers Windows via le protocole Common Internet File System (CIFS). Outlook Web Access (OWA) est un exemple d'accès HTTP.

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

- VPN SSL client léger (redirection de port) - Fournit un client distant qui télécharge un petit applet basé sur Java et permet l'accès sécurisé aux applications de Protocole de contrôle de transmissions (TCP) qui utilisent des numéros de port statiques. Les protocoles POP3 (Point of Presence), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), ssh (Secure Shell) et Telnet sont des exemples d'accès sécurisé. Puisque les fichiers sur l'ordinateur local changent, les utilisateurs doivent avoir des privilèges d'administrateur locaux pour utiliser cette méthode. Cette méthode de VPN SSL ne fonctionne pas avec les applications qui utilisent des affectations de ports dynamiques, telles que certaines applications de protocole de transfert de fichiers (FTP).

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

  Remarque : le protocole UDP (User Datagram Protocol) n'est pas pris en charge.

- SSL VPN Client (SVC Full Tunnel Mode) : télécharge un petit client sur la station de travail distante et permet un accès entièrement sécurisé aux ressources sur un réseau d'entreprise interne. Vous pouvez télécharger le circuit virtuel commuté sur une station de travail distante de façon permanente ou supprimer le client une fois la session sécurisée fermée.

Ce document présente la configuration d'un routeur Cisco IOS pour une utilisation par un client VPN SSL.

Conditions préalables

Exigences

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

- Microsoft Windows 2000 ou XP ;
- Navigateur Web avec SUN JRE 1.4 (ou version ultérieure) ou navigateur contrôlé par ActiveX ;
- Privilèges administratifs locaux sur le client ;
- Un des routeurs répertoriés dans l'Introduction avec une image de sécurité avancée (12.4(6)T ou ultérieure)
- Cisco Security Device Manager (SDM) version 2.3

Si Cisco SDM n'est pas déjà chargé sur votre routeur, vous pouvez obtenir une copie gratuite du logiciel à partir du site Téléchargement de logiciel (clients enregistrés seulement). Vous devez avoir un compte CCO avec un contrat de service. Pour obtenir des informations détaillées sur l'installation et la configuration de SDM, référez-vous à Cisco Router and Security Device Manager.

- Un certificat numérique sur le routeur

  Vous pouvez utiliser un certificat auto-signé permanent ou une autorité de certification (CA) externe pour répondre à cette exigence. Pour plus d'informations sur les certificats auto-signés persistants, consultez Certificats auto-signés persistants.

Composants utilisés

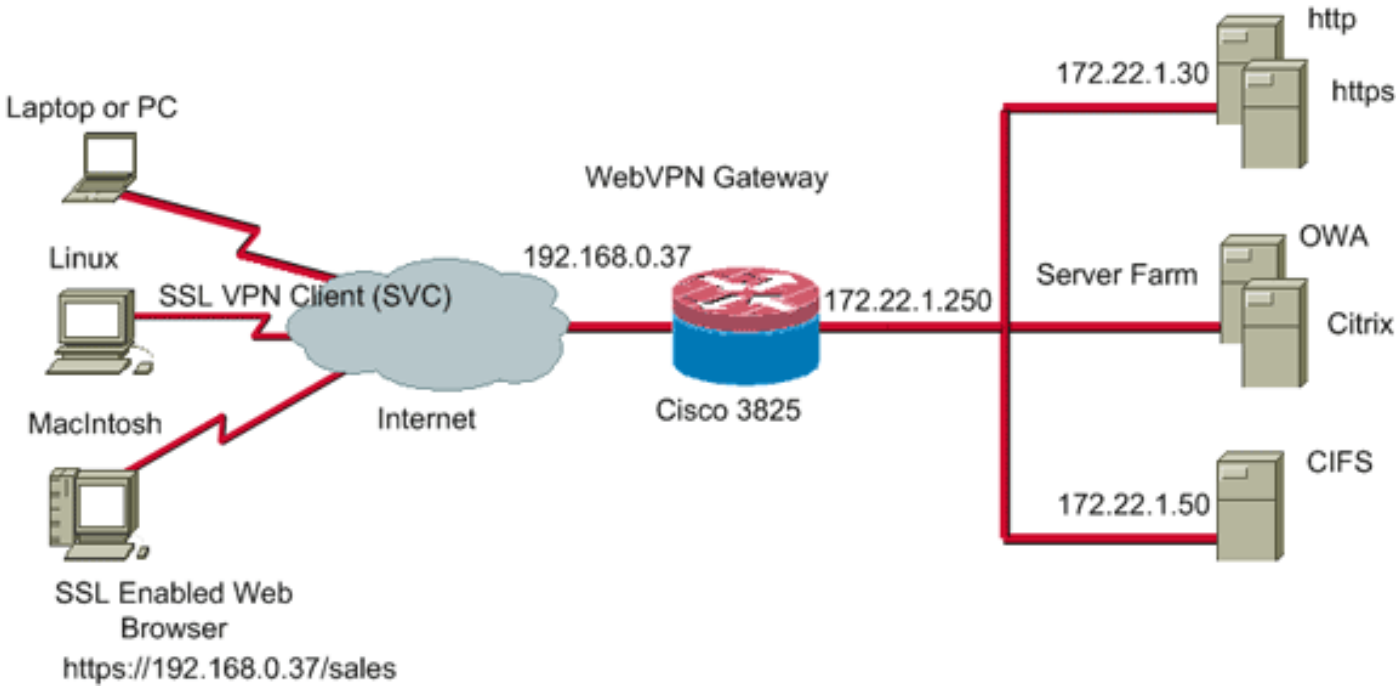
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco IOS série 3825 avec 12.4(9)T
- Security Device Manager (SDM) version 2.3.1

Remarque : les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Tâches de préconfiguration

1. Configurer le routeur pour SDM (facultatif)

   L'application SDM est déjà chargée en mémoire flash sur les routeurs disposant de la licence d'ensemble de sécurité appropriée. Référez-vous à Téléchargement et installation de Cisco Router and Security Device Manager (SDM) pour obtenir et configurer le logiciel.

2. Téléchargez une copie du circuit virtuel commuté sur votre ordinateur de gestion.

   Vous pouvez obtenir une copie du fichier de package SVC à partir de Téléchargement de logiciel : Client VPN SSL Cisco (clients enregistrés uniquement) . Vous devez disposer d'un compte CCO valide associé à un contrat de service.

3. Définissez la date, l'heure et le fuseau horaire corrects, puis configurez un certificat numérique sur le routeur.

Conventions

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

Informations générales

Le SVC est initialement chargé sur le routeur de passerelle WebVPN. Chaque fois que le client se connecte, une copie du circuit virtuel commuté est téléchargée dynamiquement sur le PC. Afin de modifier ce comportement, configurez le routeur pour permettre au logiciel de rester en permanence sur l'ordinateur client.

Configuration de SVC sur IOS

Cette section vous indique les étapes nécessaires pour configurer les fonctionnalités décrites dans ce document. Cet exemple de configuration utilise l'Assistant SDM pour activer le fonctionnement du circuit virtuel commuté sur le routeur IOS.

Complétez ces étapes afin de configurer SVC sur le routeur IOS :

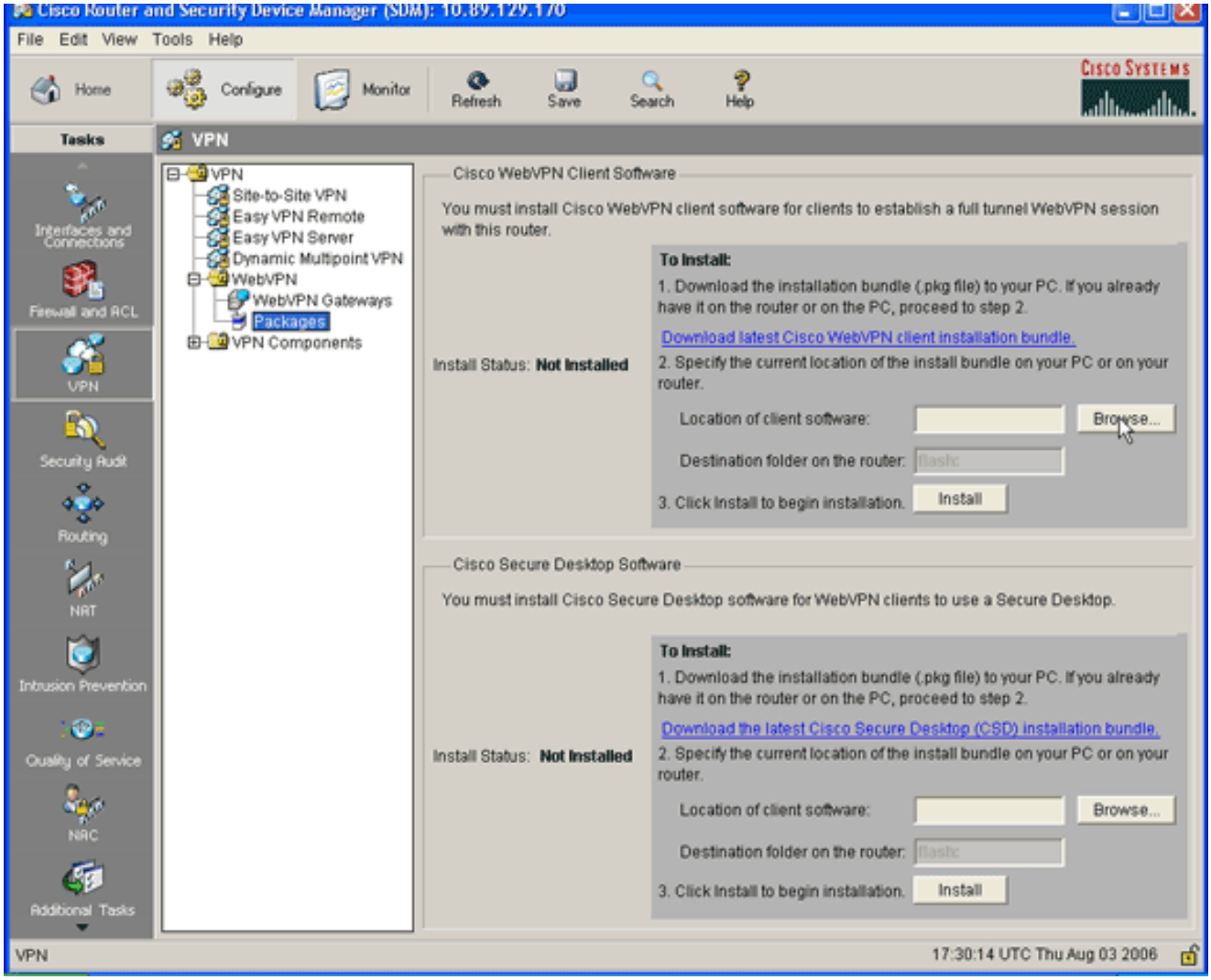
1. Installation et activation du logiciel SVC sur le routeur IOS
2. Configuration d'un contexte WebVPN et d'une passerelle WebVPN avec l'Assistant SDM
3. Configuration de la base de données utilisateur pour les utilisateurs SVC
4. Configurer les ressources à présenter aux utilisateurs

Étape 1. Installation et activation du logiciel SVC sur le routeur IOS

Complétez ces étapes afin d'installer et d'activer le logiciel SVC sur le routeur IOS :

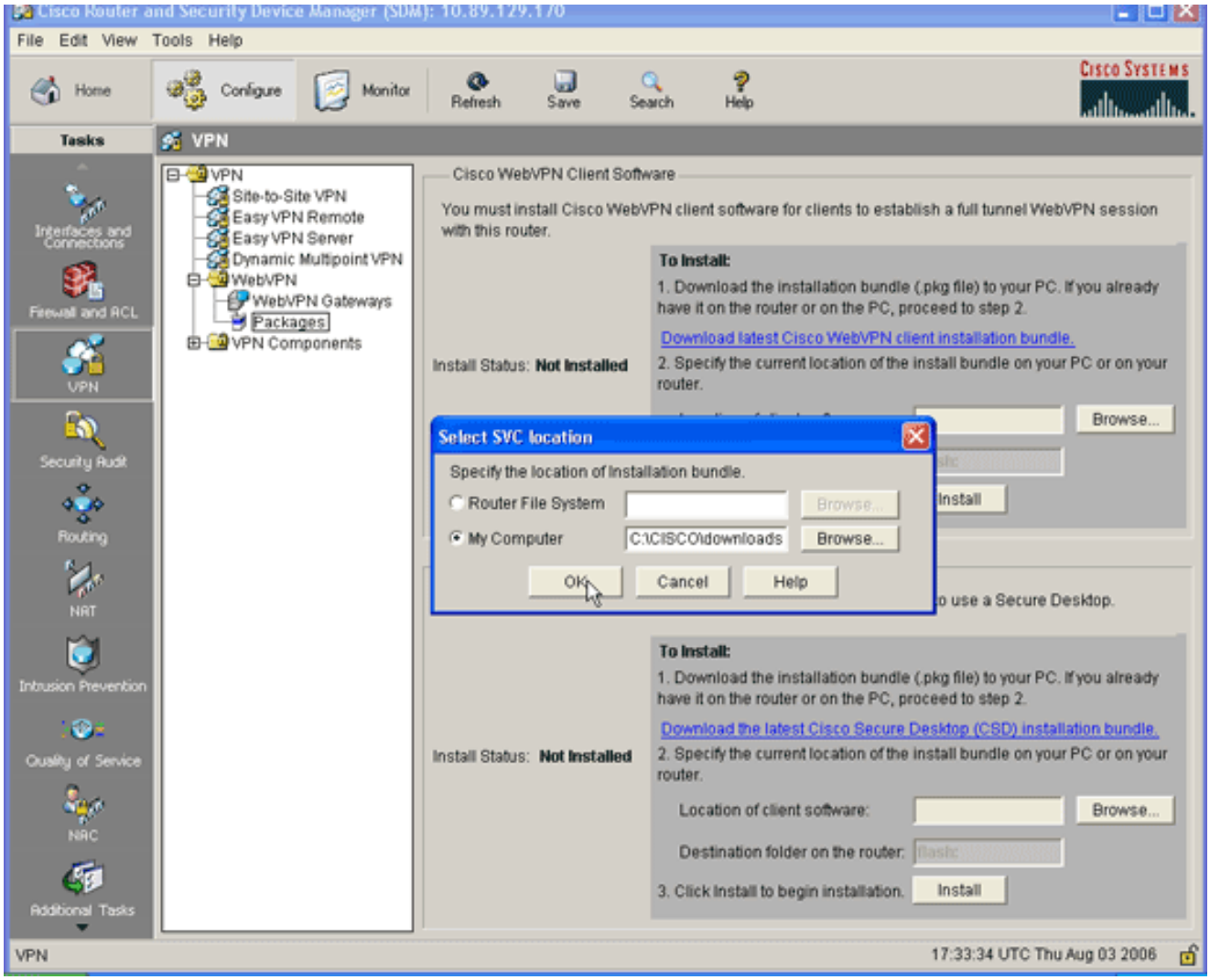
1. Ouvrez l'application SDM, cliquez sur Configure, puis cliquez sur VPN.

2. Développez WebVPN et choisissez Packages.



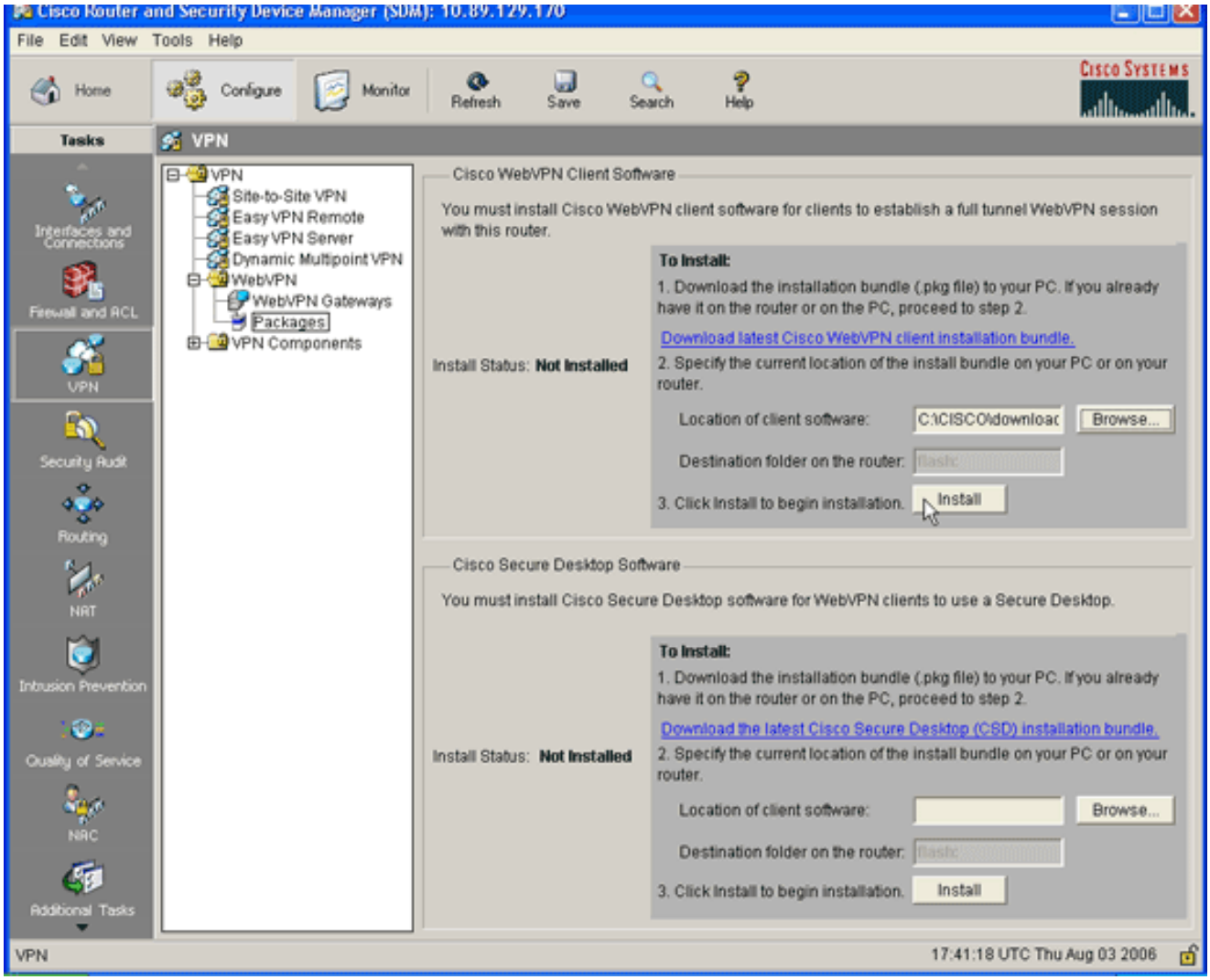
3. Dans la zone Cisco WebVPN Client Software, cliquez sur le bouton Browse.

   La boîte de dialogue Sélectionner l'emplacement SVC s'affiche.



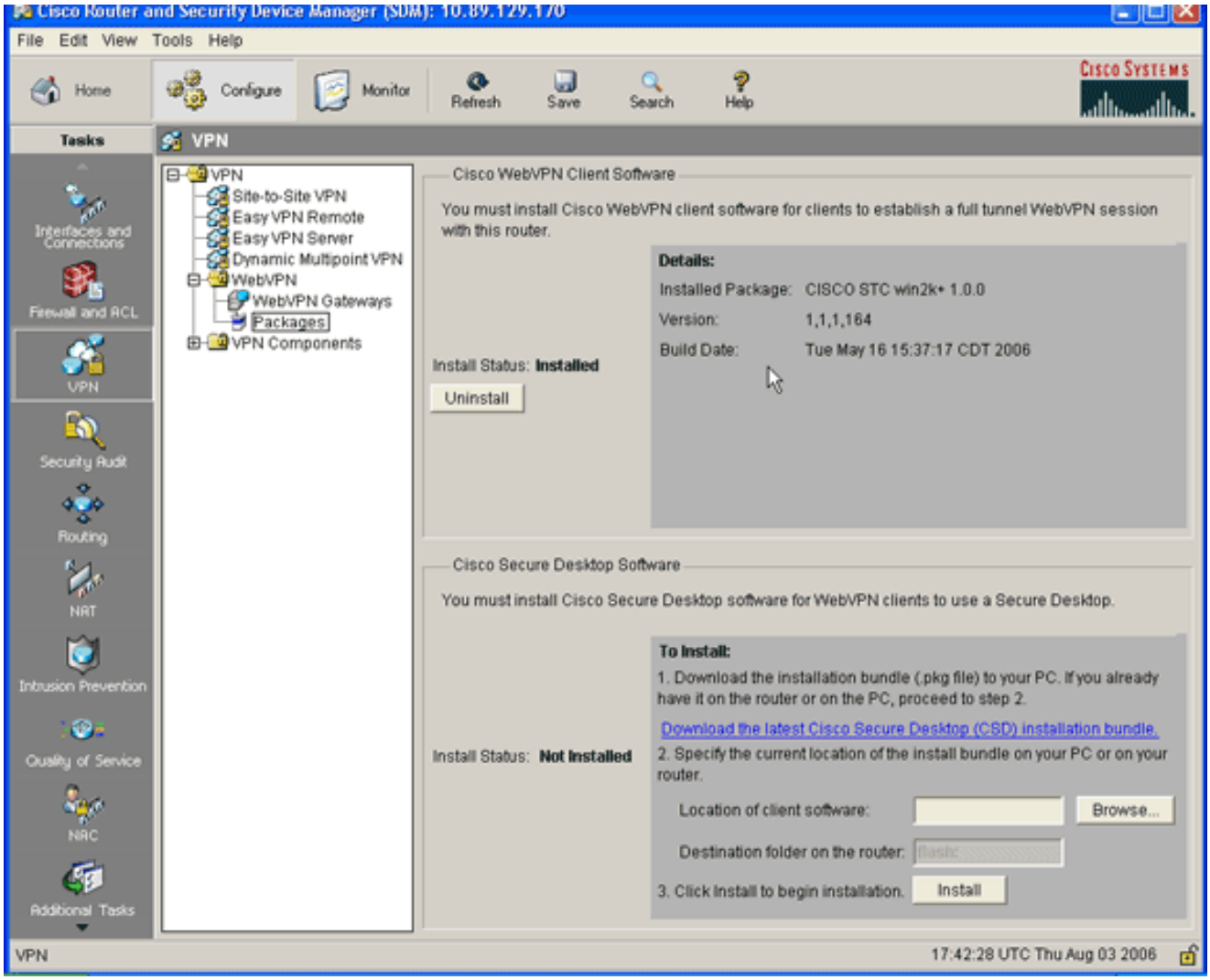
4. Cliquez sur la case d'option Poste de travail, puis cliquez sur Parcourir pour localiser le package SVC sur votre PC de gestion.

5. Cliquez sur OK, puis sur le bouton Install.



6. Cliquez sur Yes, puis cliquez sur OK.

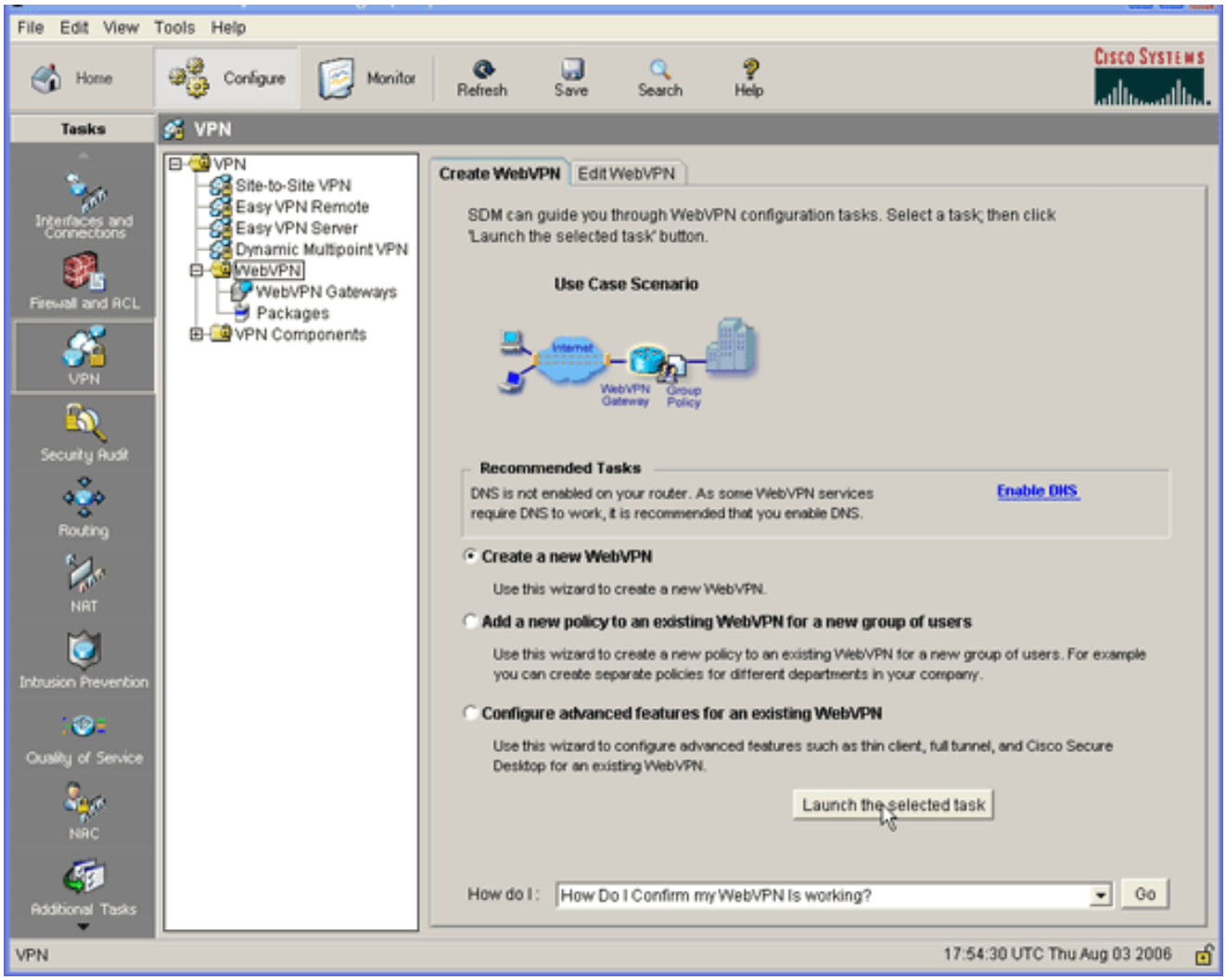
   Une installation réussie du package SVC est illustrée dans cette image :



Étape 2. Configuration d'un contexte WebVPN et d'une passerelle WebVPN avec l'Assistant SDM

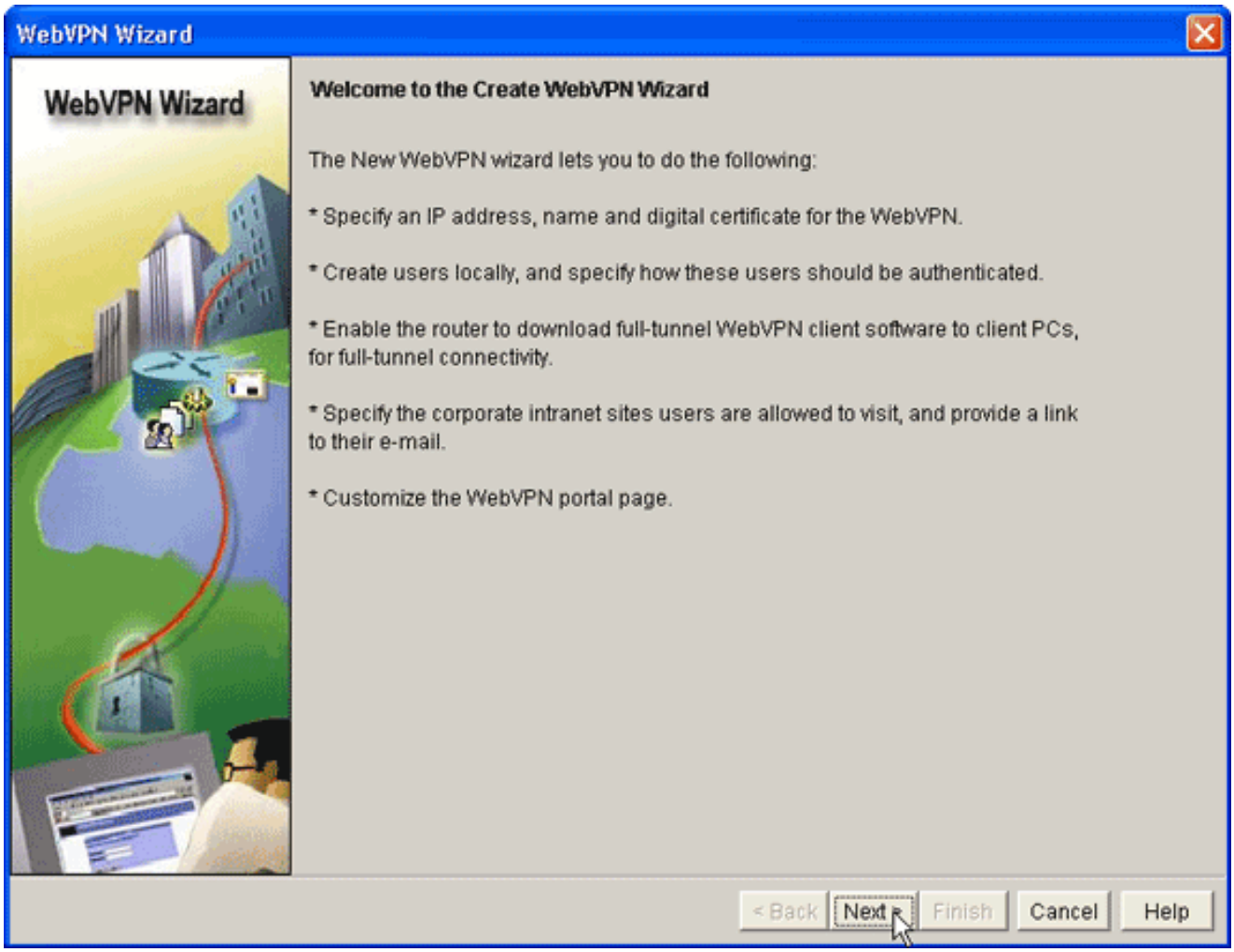
Complétez ces étapes afin de configurer un contexte WebVPN et une passerelle WebVPN :

1. Une fois le SVC installé sur le routeur, cliquez sur Configure, puis cliquez sur VPN.
2. Cliquez sur WebVPN, puis sur l'onglet Create WebVPN.

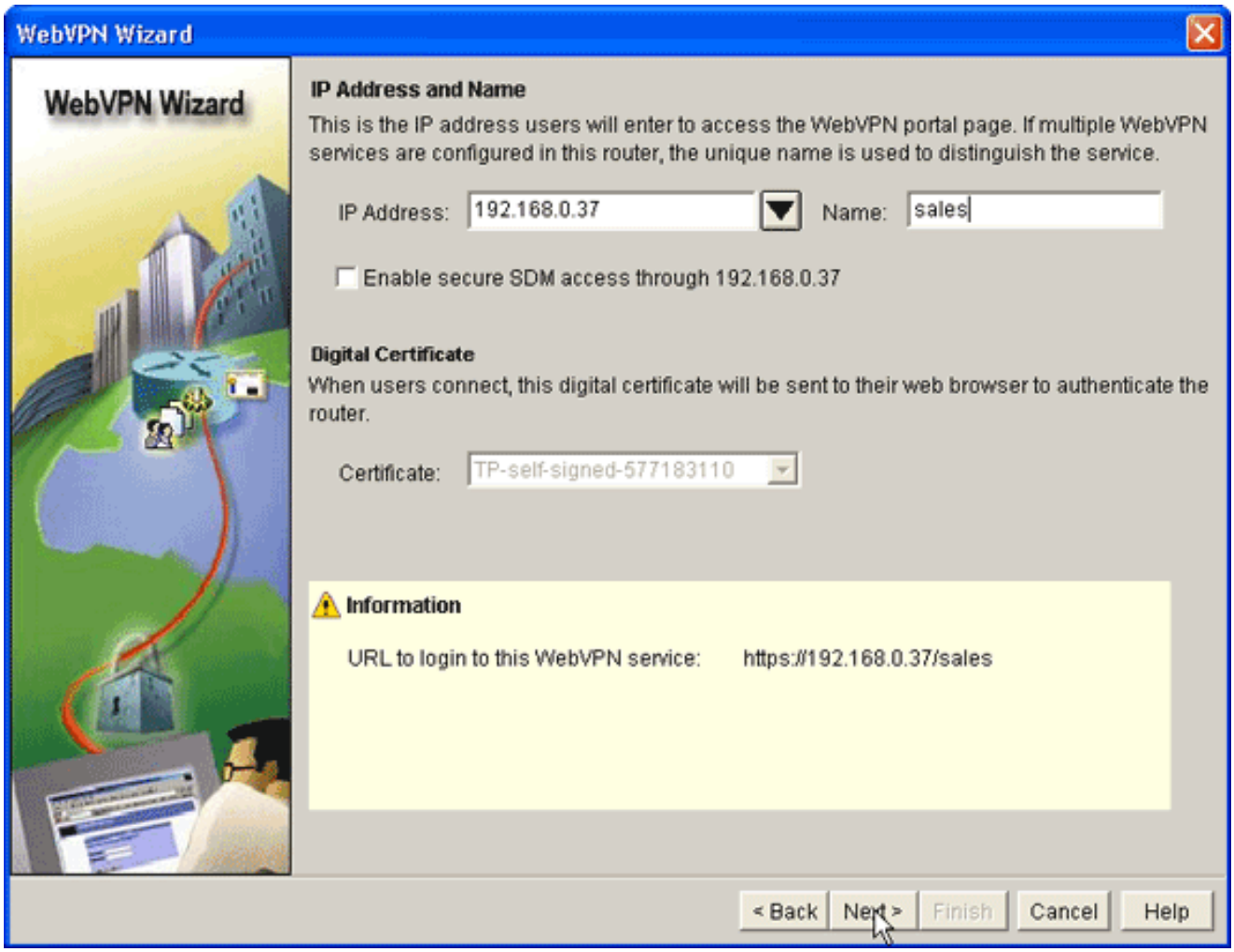


3. Cochez la case d'option Create a New WebVPN, puis cliquez sur Launch the selected task.

   La boîte de dialogue WebVPN Wizard s'affiche.



4. Cliquez sur Next (Suivant).



5. Entrez l'adresse IP de la nouvelle passerelle WebVPN et entrez un nom unique pour ce contexte WebVPN.

   Vous pouvez créer différents contextes WebVPN pour la même adresse IP (passerelle WebVPN), mais chaque nom doit être unique. Cet exemple utilise cette adresse IP : https://192.168.0.37/sales

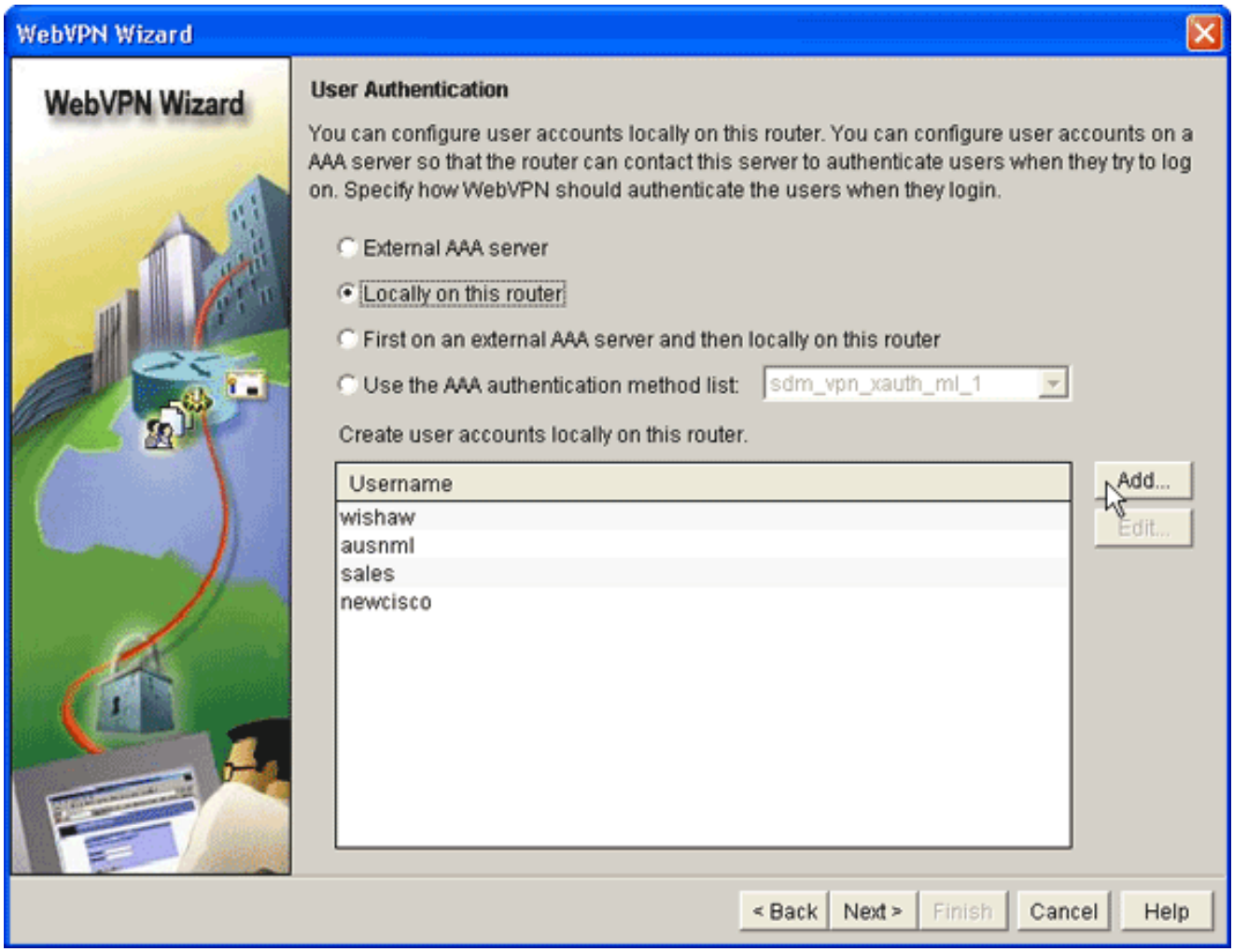
6. Cliquez sur Next, puis passez à l'Étape 3.

Étape 3. Configuration de la base de données utilisateur pour les utilisateurs SVC

Pour l'authentification, vous pouvez utiliser un serveur AAA, des utilisateurs locaux ou les deux. Cet exemple de configuration utilise des utilisateurs créés localement pour l'identification.

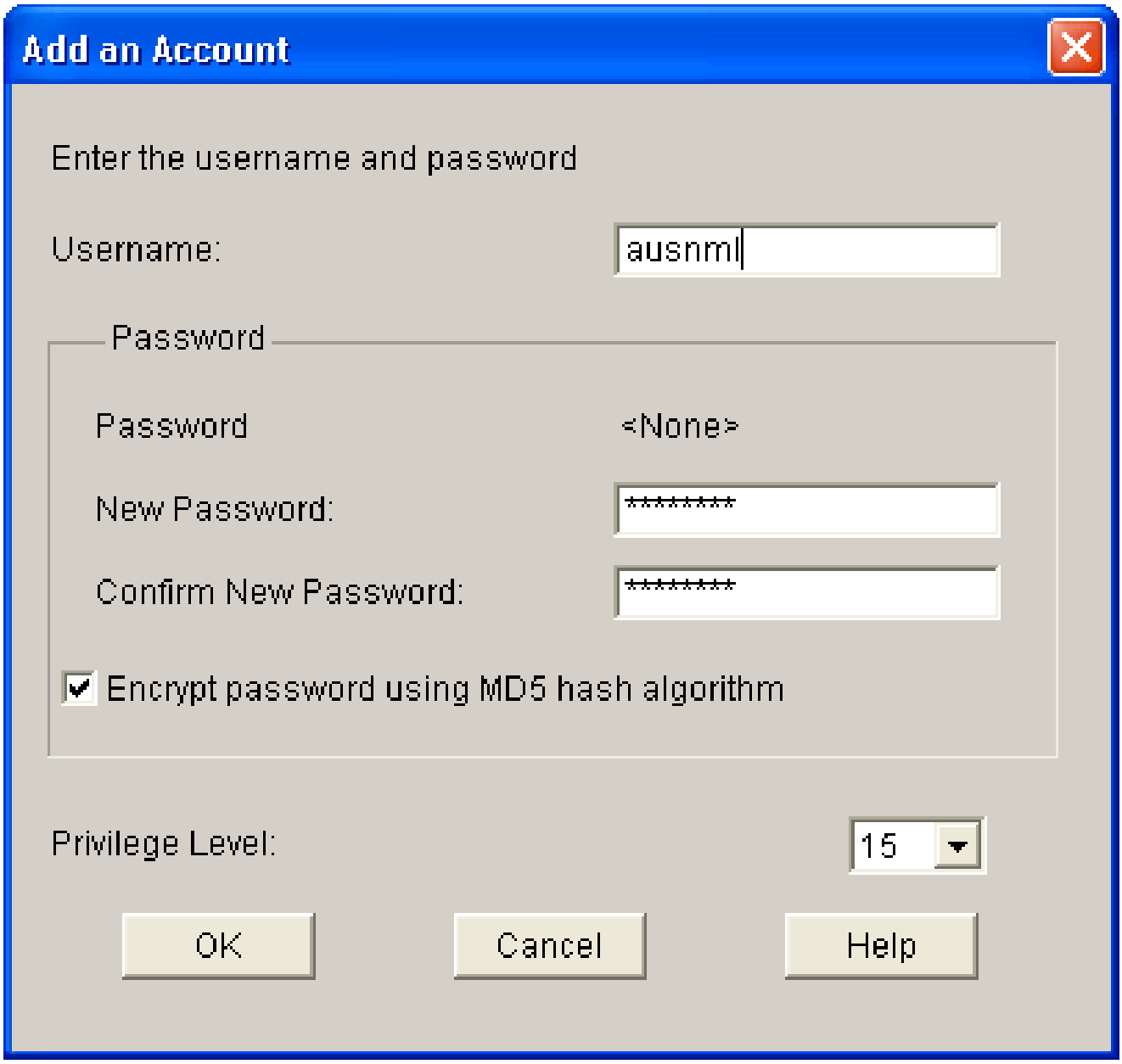
Complétez ces étapes afin de configurer la base de données utilisateur pour les utilisateurs SVC :

1. Une fois l'étape 2 terminée, cliquez sur la case d'option Locally on this router située dans la boîte de dialogue User Authentication de l'Assistant WebVPN.



Cette boîte de dialogue vous permet d'ajouter des utilisateurs à la base de données locale.

2. Cliquez sur Add, puis saisissez les informations utilisateur.



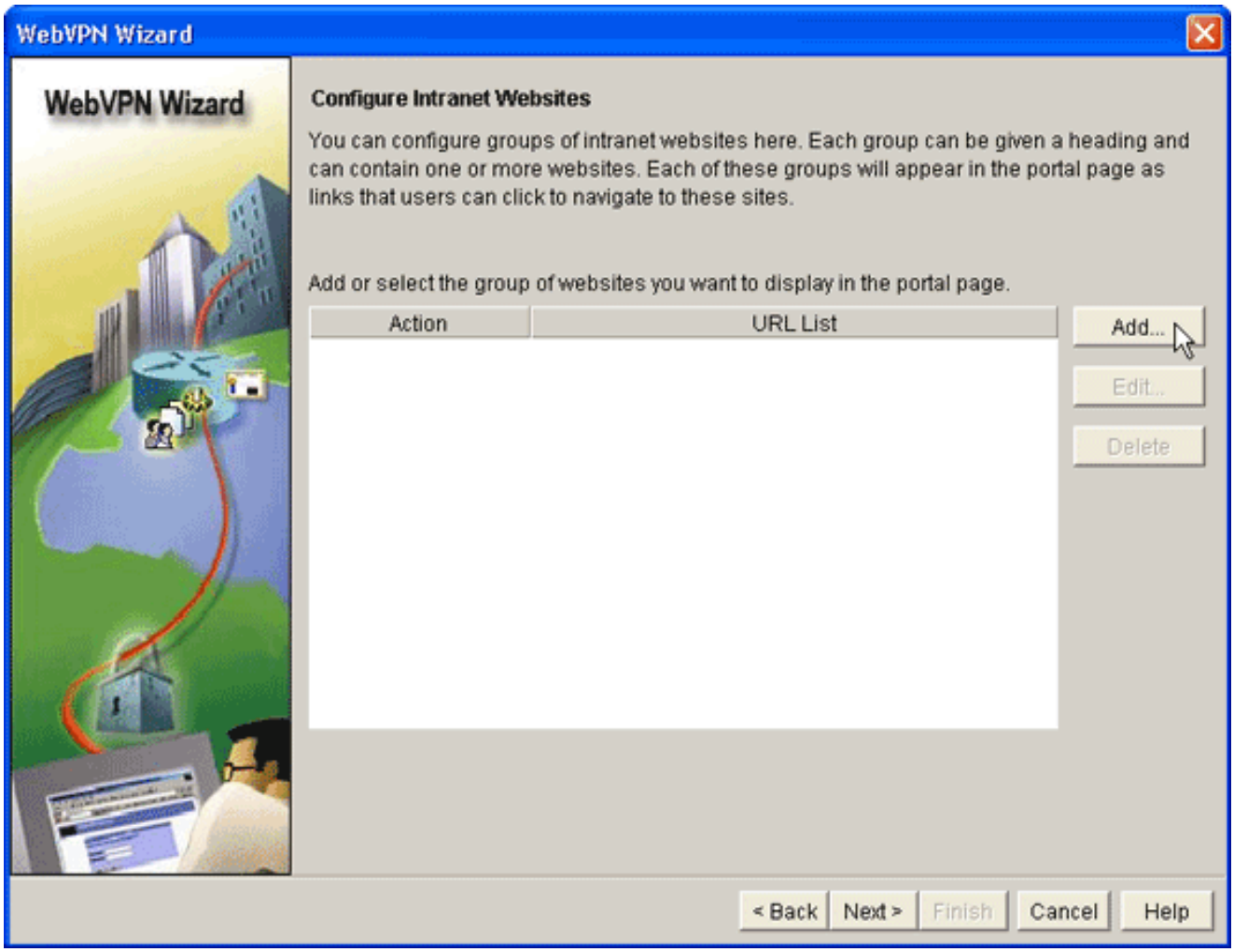
3. Cliquez sur OK, puis ajoutez des utilisateurs supplémentaires selon les besoins.
4. Après avoir ajouté les utilisateurs nécessaires, cliquez sur le bouton Next, puis passez à l'Étape 4.

Étape 4. Configurer les ressources à présenter aux utilisateurs

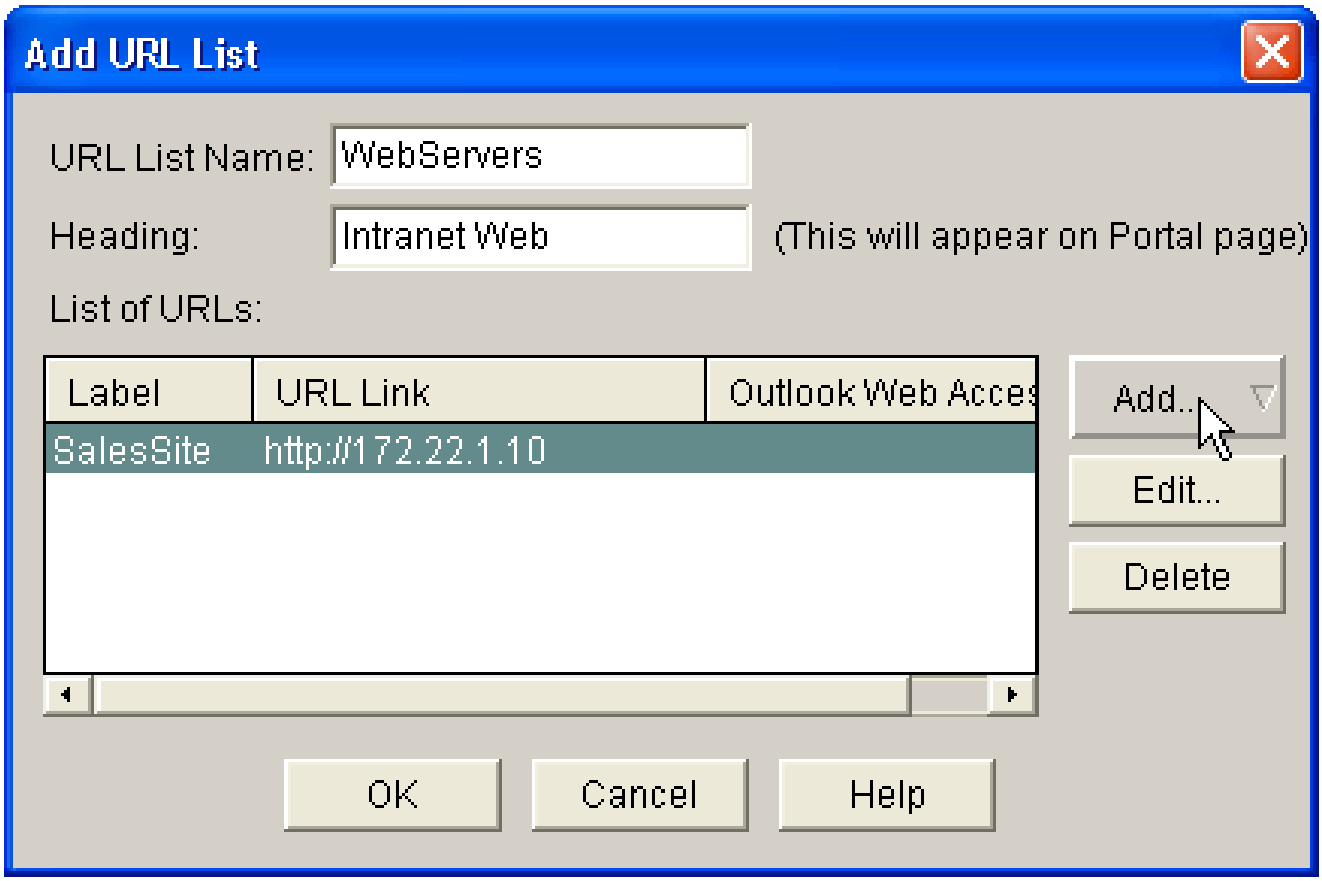
La boîte de dialogue Configurer l'Assistant WebVPN Sites intranet vous permet de sélectionner les ressources intranet que vous souhaitez exposer à vos clients SVC.

Complétez ces étapes afin de configurer les ressources à exposer aux utilisateurs :

1. Une fois que vous avez terminé l'étape 3, cliquez sur le bouton Add situé dans la boîte de dialogue Configure Intranet Websites.



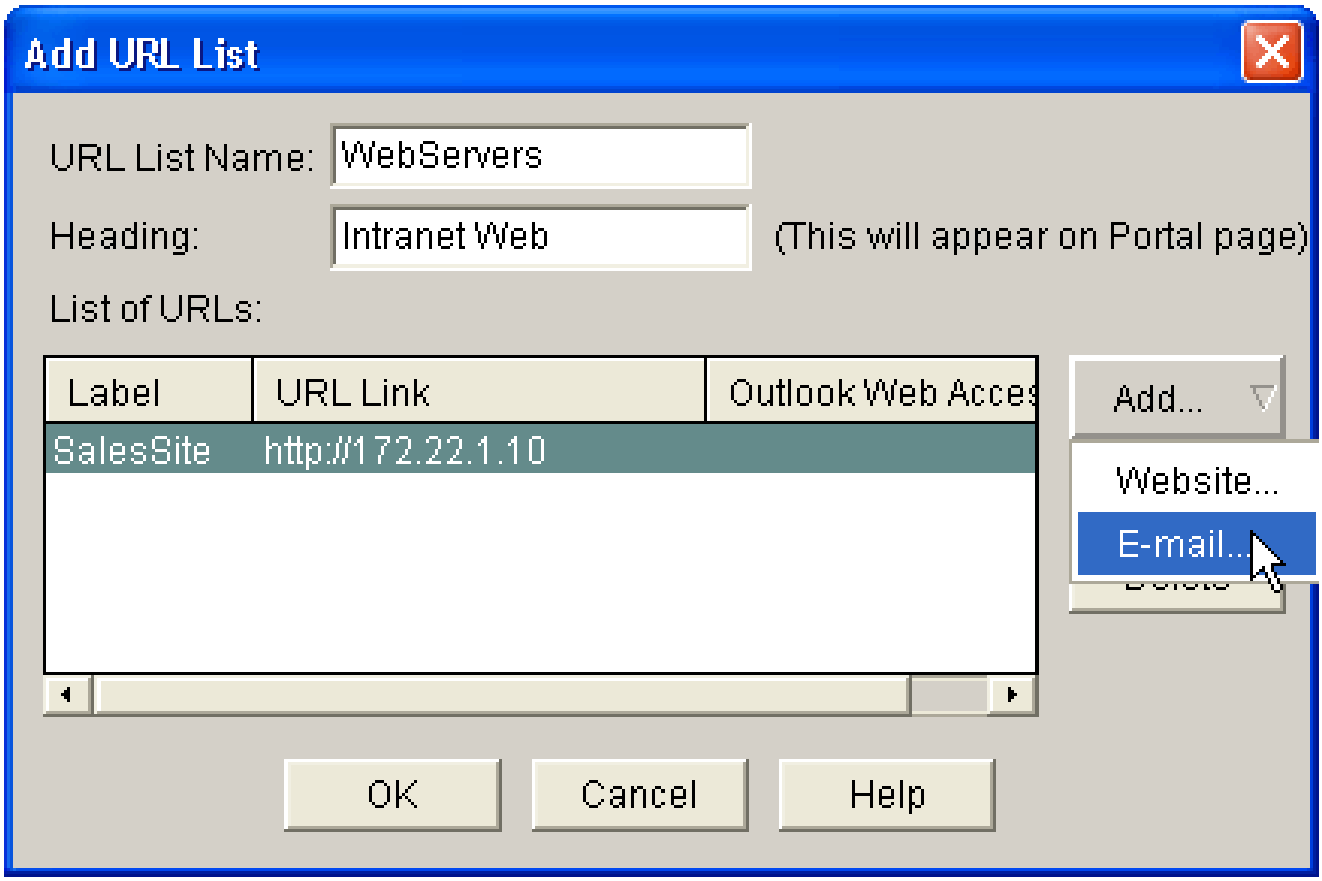
2. Entrez un nom de liste d'URL, puis un en-tête.



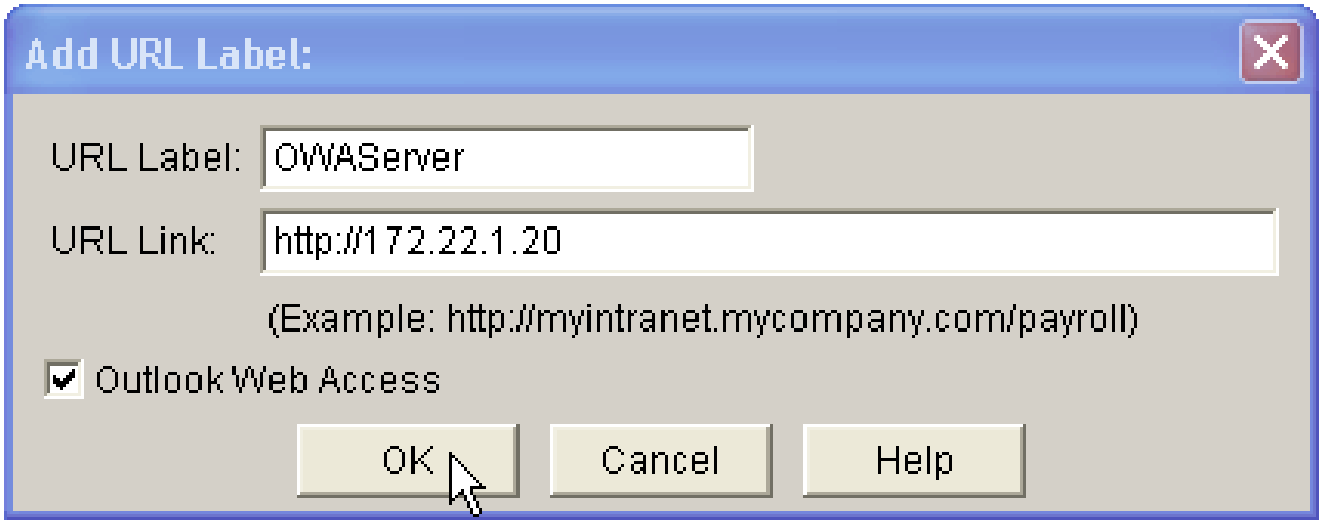
3. Cliquez sur Add, et choisissez Website pour ajouter les sites Web que vous souhaitez exposer à ce client.

4. Entrez l'URL et les informations de lien, puis cliquez sur OK.

5. Pour ajouter l'accès aux serveurs Exchange OWA, cliquez sur Add et choisissez E-mail.

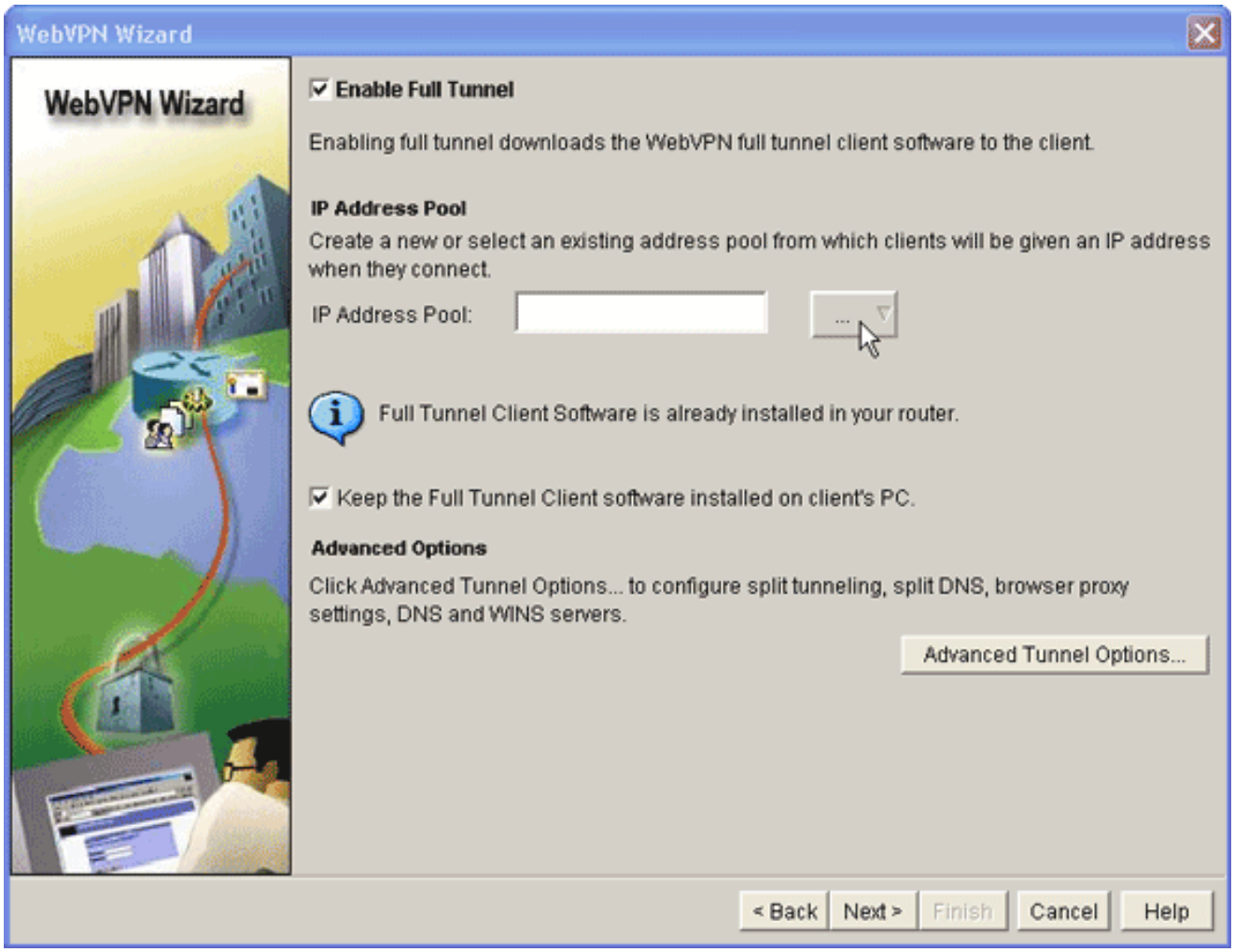


6. Activez la case à cocher Outlook Web Access, entrez l'étiquette d'URL et les informations de lien, puis cliquez sur OK.

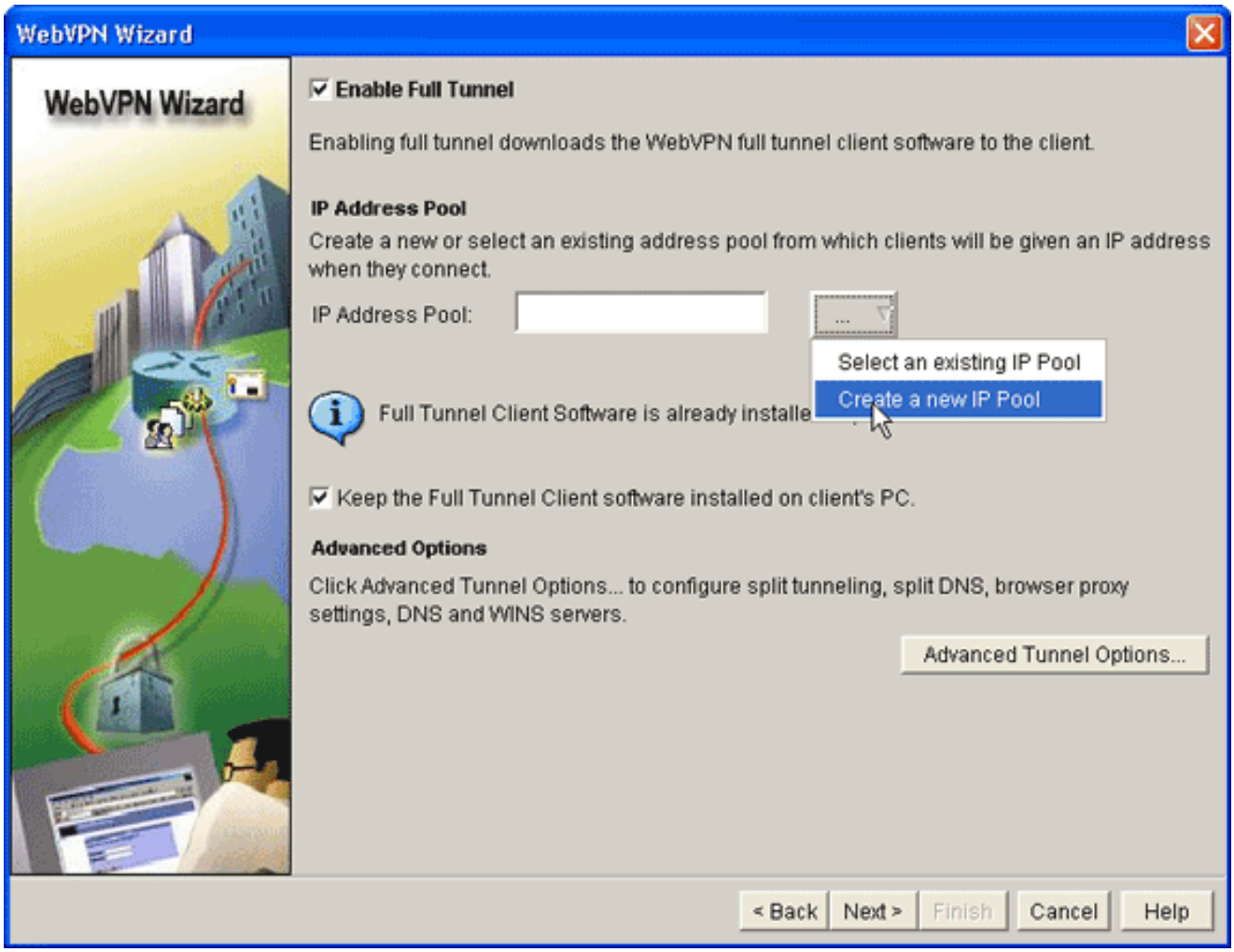


7. Après avoir ajouté les ressources souhaitées, cliquez sur OK, puis sur Next.

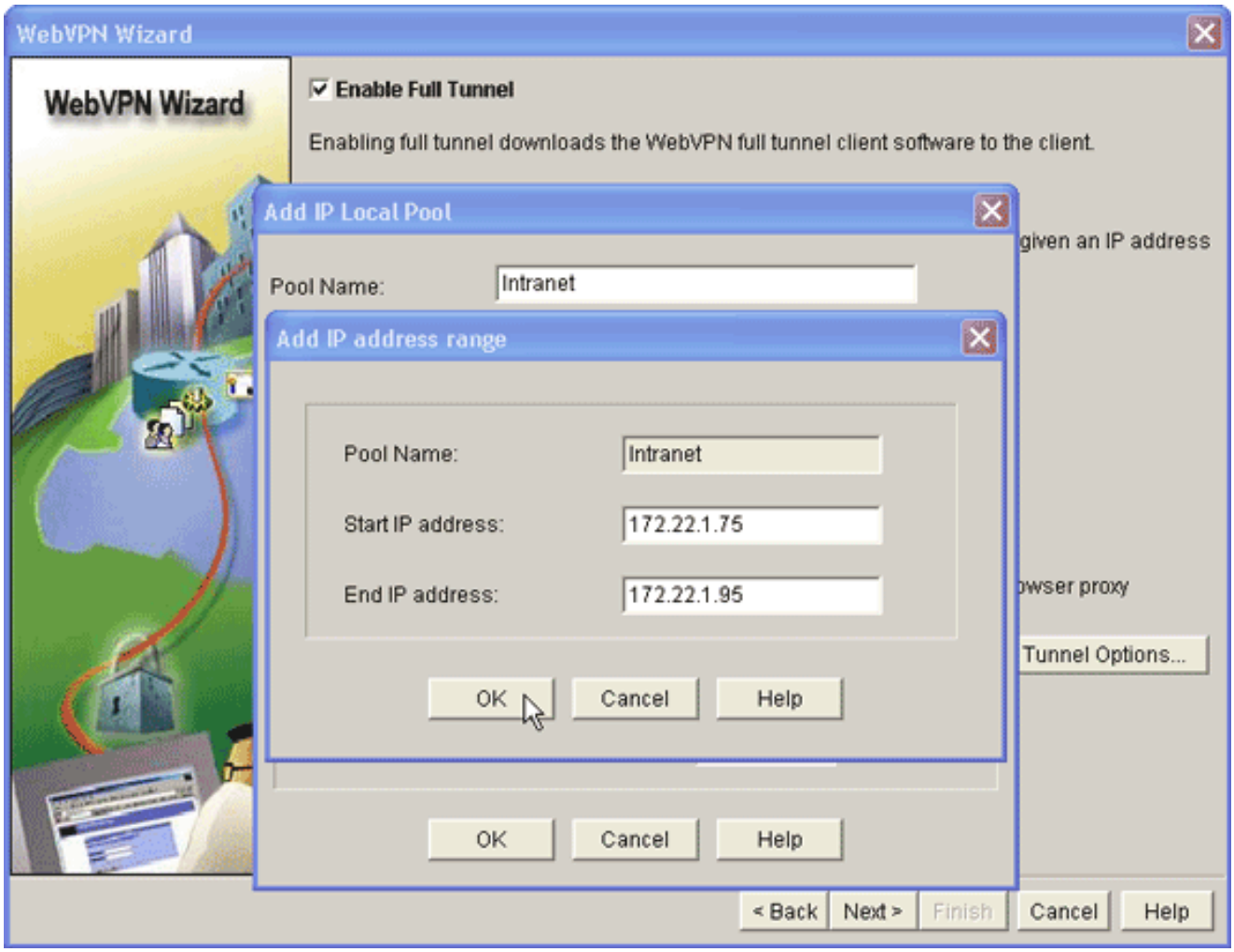
   La boîte de dialogue Tunnel complet de l'Assistant WebVPN apparaît.



8. Vérifiez que la case Enable Full Tunnel est cochée.
9. Créez un pool d'adresses IP que les clients de ce contexte WebVPN peuvent utiliser. Le pool d’adresses doit correspondre aux adresses disponibles et routables sur votre Intranet.
10. Cliquez sur les ellipses (...) situées à côté du champ IP Address Pool, puis sélectionnez Create a new IP Pool.



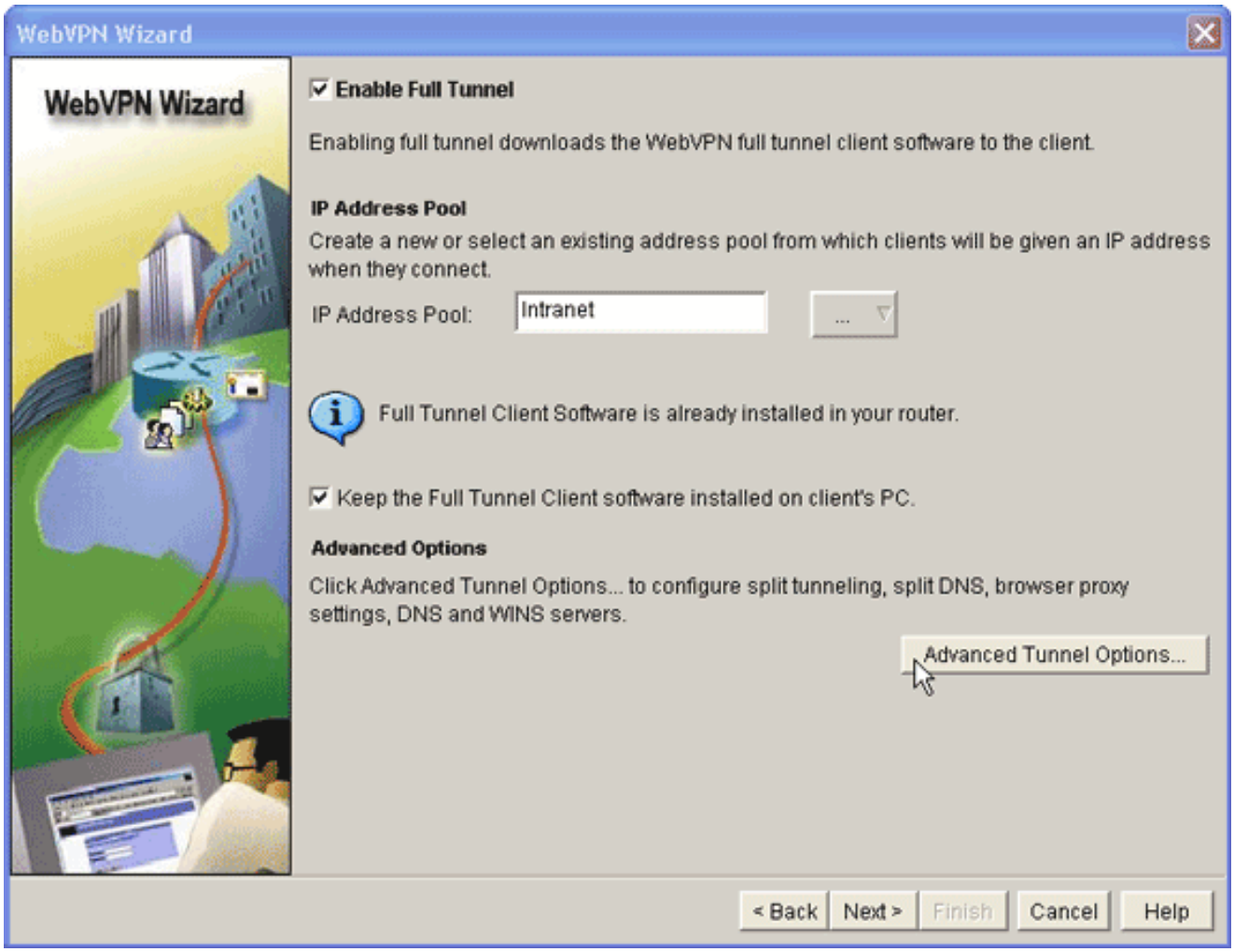
11. Dans la boîte de dialogue Add IP Local Pool, entrez un nom pour le pool, puis cliquez sur Add.



12. Dans la boîte de dialogue Ajouter une plage d'adresses IP, entrez la plage du pool d'adresses pour les clients SVC, puis cliquez sur OK.

    Remarque : le pool d'adresses IP doit se trouver dans une plage d'une interface directement connectée au routeur. Si vous souhaitez utiliser une plage de pool différente, vous pouvez créer une adresse de bouclage associée à votre nouveau pool pour répondre à cette exigence.

13. Click OK.

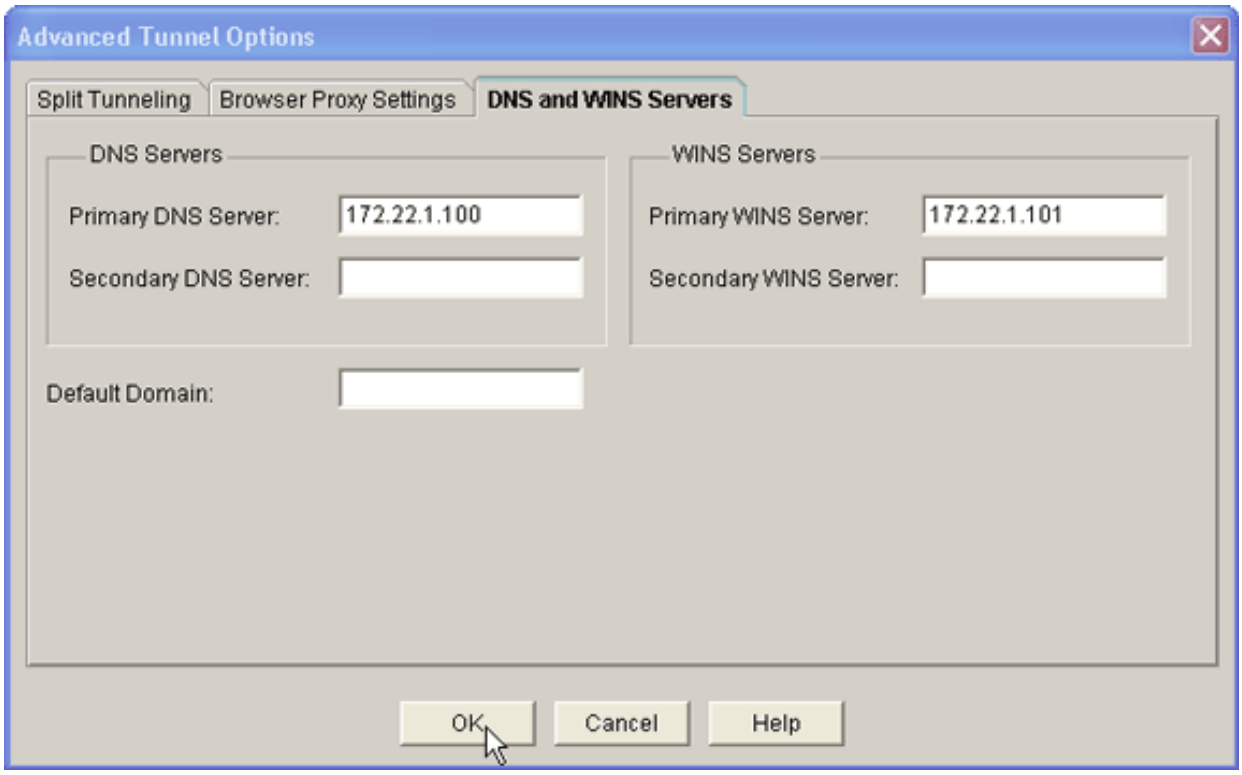


14. Si vous souhaitez que vos clients distants stockent définitivement une copie du SVC, cochez la case Keep the Full Tunnel Client Software installed on client's PC. Désactivez cette option pour demander au client de télécharger le logiciel SVC chaque fois qu'un client se connecte.

15. Configurez les options de tunnel avancées, notamment la transmission de tunnel partagée, le partage de DNS, les paramètres de proxy du navigateur ainsi que les serveurs DNS et WNS. Cisco vous recommande de configurer au minimum les serveurs DNS et WINS.

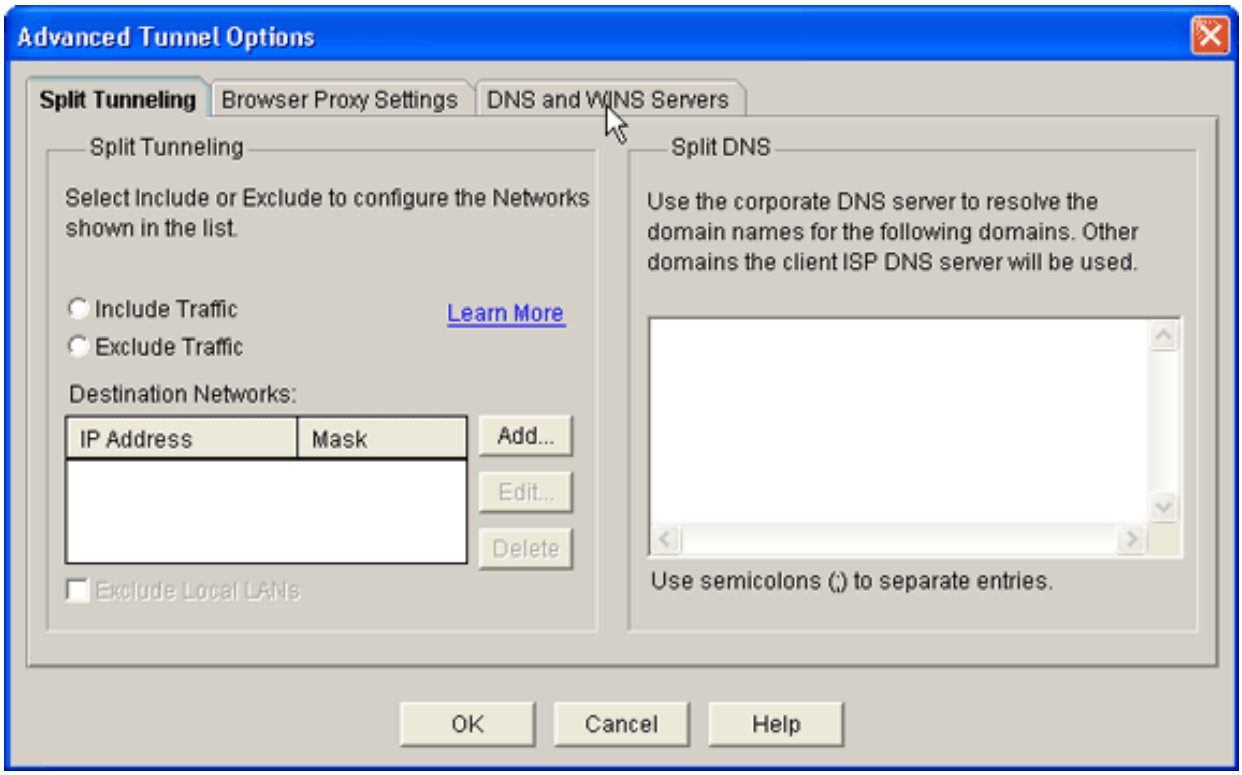
    Exécutez les étapes suivantes pour configurer les options de tunnel avancées :

    a. Cliquez sur le bouton Advanced Tunnel Options (Options de tunnel avancées).



b. Cliquez sur l'onglet DNS and WINS Servers, puis saisissez les adresses IP principales des serveurs DNS et WINS.

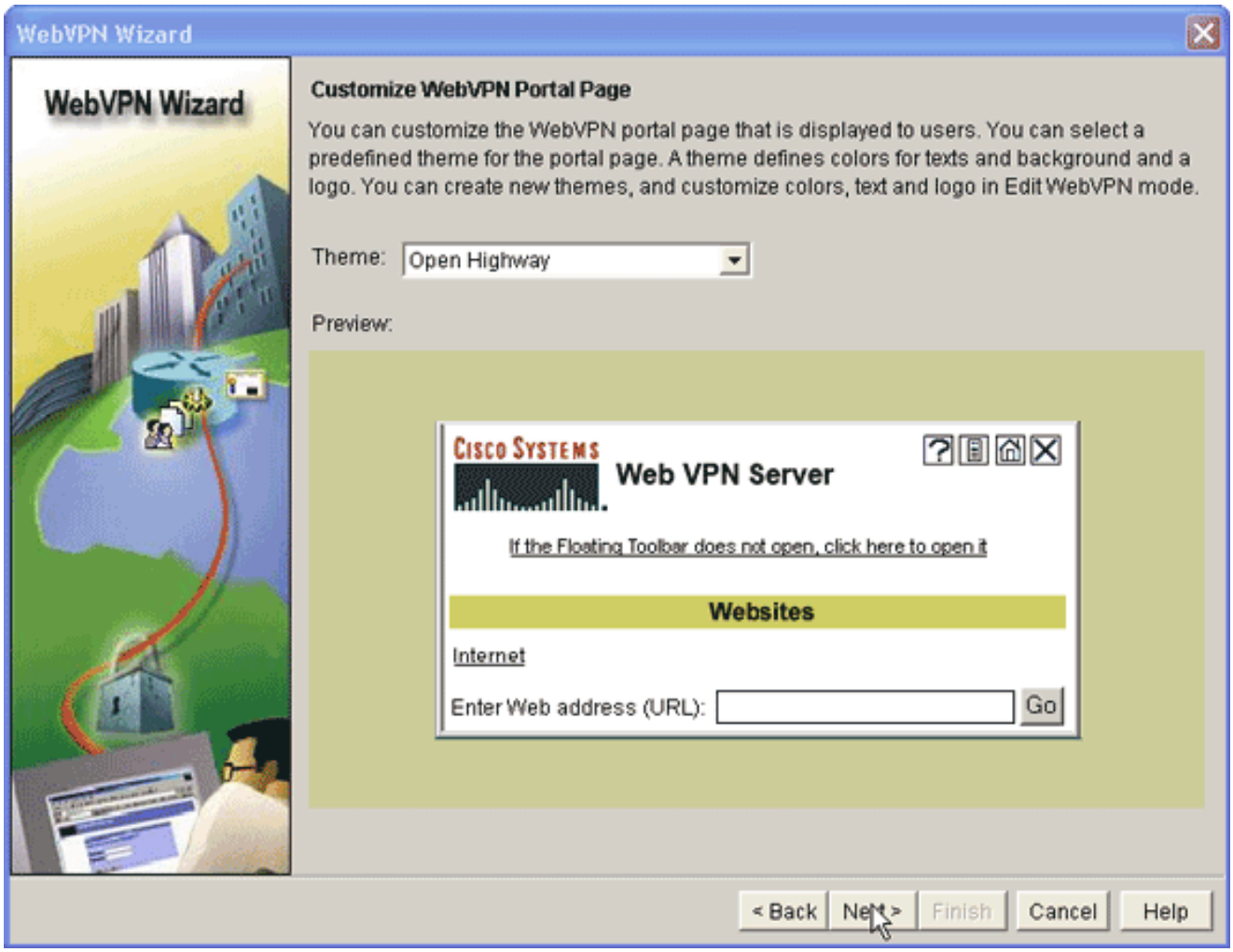
c. Pour configurer la transmission tunnel partagée et les paramètres du navigateur proxy, cliquez sur l'onglet Transmission tunnel partagée ou Paramètres du navigateur proxy.



16. Après avoir configuré les options nécessaires, cliquez sur Next.

17. Personnalisez la page WebVPN Portal ou sélectionnez les valeurs par défaut.

La page Customize WebVPN Portal vous permet de personnaliser l'apparence de la page WebVPN Portal pour vos clients.

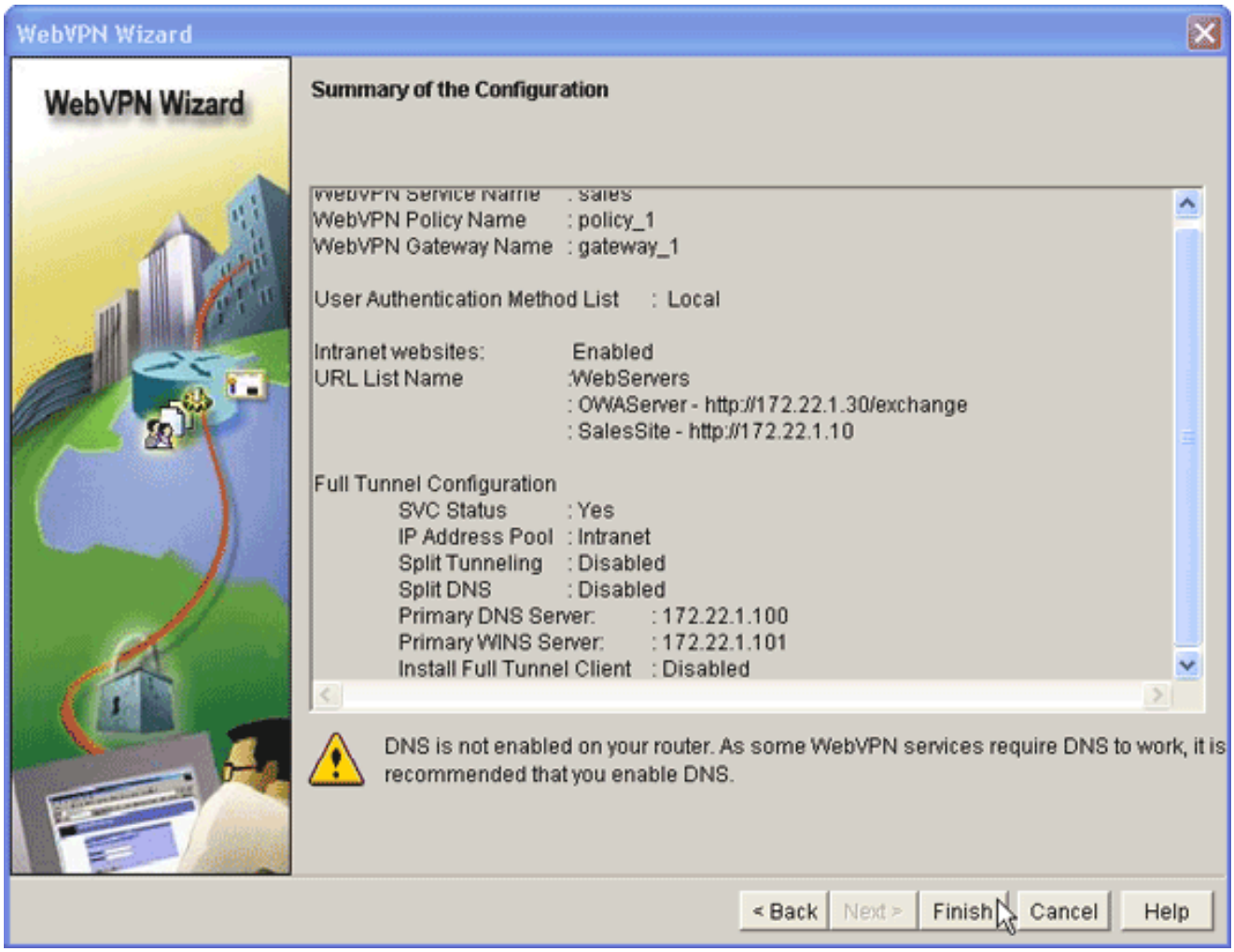


18. Après avoir configuré la page WebVPN Portal, cliquez sur Next, cliquez sur Finish, puis cliquez sur OK.

    L'assistant WebVPN envoie des commandes de visite au routeur.

19. Cliquez sur OK pour enregistrer votre configuration.

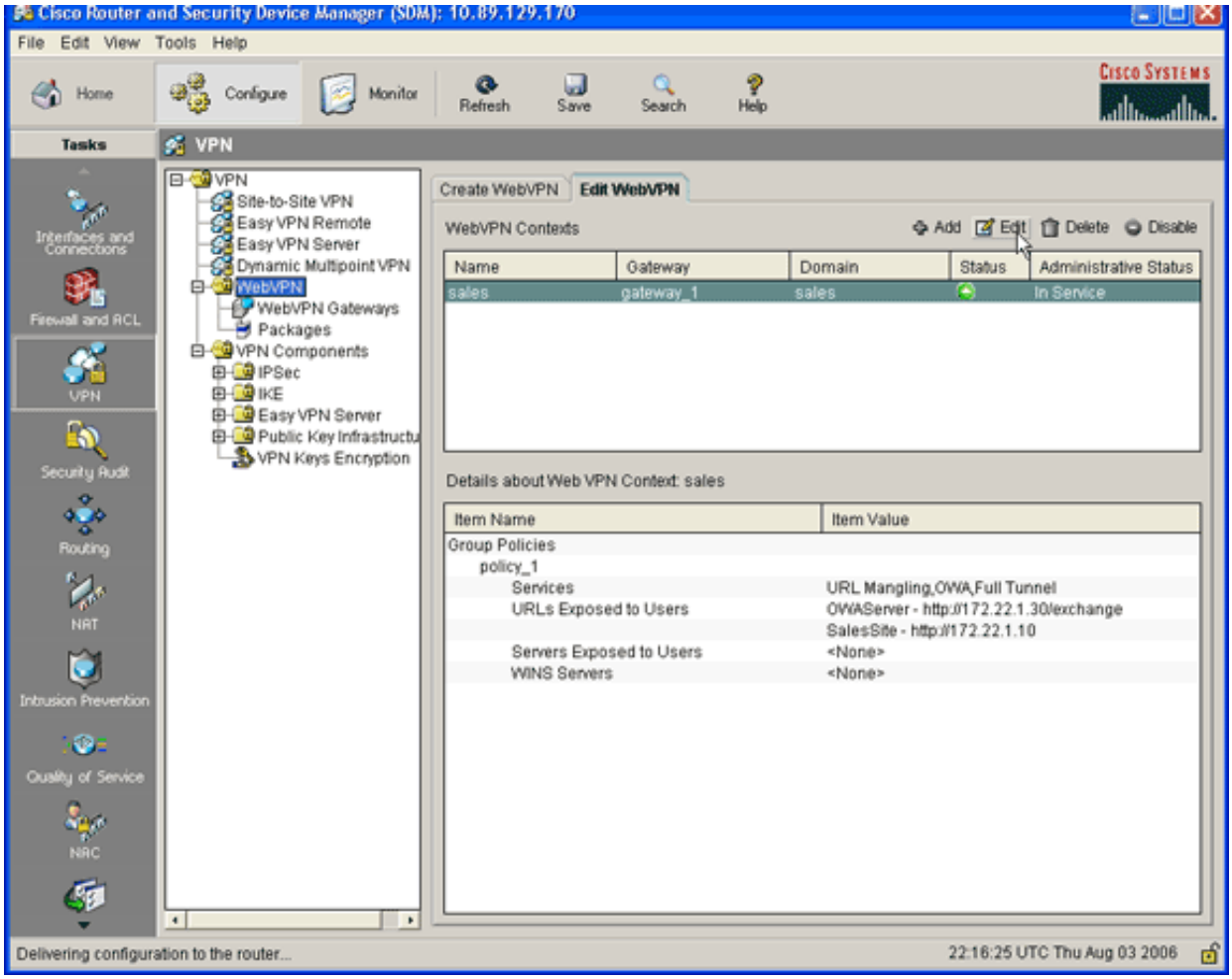
    Remarque : si vous recevez un message d'erreur, la licence WebVPN est peut-être incorrecte. Un exemple de message d'erreur s'affiche dans cette image :



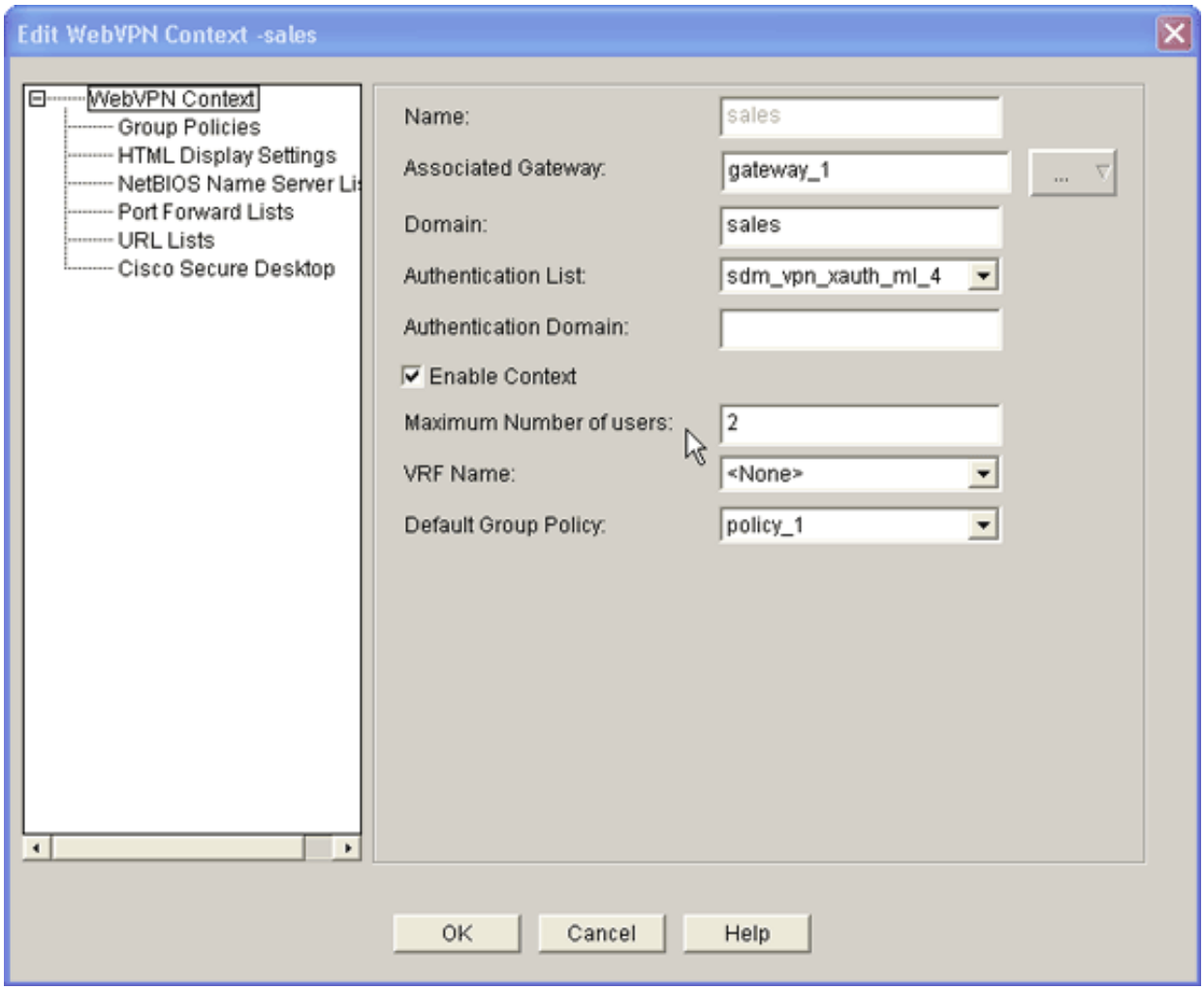
Pour corriger le problème de licence, exécutez les étapes suivantes :

a. Cliquez sur Configure, puis sur VPN.

b. Développez WebVPN, puis cliquez sur l'onglet Edit WebVPN.



c. Mettez le contexte que vous venez de créer en surbrillance, puis cliquez sur le bouton Edit (Modifier).



d. Dans le champ « Maximum Number of users » (Nombre maximal d'utilisateurs), saisissez le nombre correct d'utilisateurs de votre licence.

e. Cliquez sur OK, puis sur OK.

Vos commandes sont enregistrées dans le fichier de configuration.

f. Cliquez sur Save, puis sur Yes pour accepter les modifications.

Résultats

L'ASDM crée les configurations de ligne de commande suivantes :

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
```

Vérifier

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

Procédure

Pour tester votre configuration, entrez http://192.168.0.37/sales dans un navigateur Web client compatible SSL.

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 obtenir des informations détaillées à propos des commandes show, reportez-vous à Vérification de la configuration de WebVPN.

Remarque : l'outil Output Interpreter Tool (réservé aux clients enregistrés) (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.

Problème de connectivité SSL

Problème : les clients VPN SSL ne peuvent pas se connecter au routeur.

Solution : ce problème peut provenir d'adresses IP insuffisantes dans le pool d'adresses IP. Pour résoudre ce problème, augmentez le nombre d’adresses IP dans le pool d’adresses IP du routeur.

Dépannage des commandes

Plusieurs commandes clear sont associées à WebVPN. Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Clear WebVPN.

Plusieurs commandes debug sont associées à WebVPN. Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Debug WebVPN.

Remarque : l'utilisation des commandes debug peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes debug , référez-vous à la section Informations importantes sur les commandes Debug.

Informations connexes

- Cisco IOS SSLVPN
- VPN SSL - WebVPN
- Exemple de configuration d'un VPN SSL sans client (WebVPN) sur Cisco IOS avec SDM
- Exemple de configuration de VPN SSL (WebVPN) client léger sur IOS avec SDM
- Guide de déploiement de convergence WebVPN et DMVPN
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.