Пример конфигурации клиента SSL VPN на IOS с помощью SDM

Содержание

- Введение
- Предварительные условия
  - Требования
  - Используемые компоненты
  - Схема сети
  - Предварительные действия
  - Условные обозначения
- Общие сведения
- Настройка SVC на IOS
  - Шаг 1. Установки и включение программного обеспечения SVC на маршрутизаторе IOS
  - Шаг 2. Настройте контекст WebVPN и шлюз с помощью мастера SDM
  - Шаг 3. Настройка базы данных пользователей SVC
  - Шаг 4. Настройка ресурсов, предоставляемых пользователям
  - Результаты
- Проверка
  - Процедура
  - Команды
- Устранение неполадок
  - Осуществление SSL соединения
  - Отладочные команды
- Дополнительные сведения

Введение

Клиент SSL VPN (SVC) обеспечивает работу полнофункционального туннеля для обеспечения защищенных соединений корпоративной внутренней сети. Можно настроить доступ пользователя на основе его данных, либо создать различные WebVPN-контексты и поместить в них одного или более пользователей.

Технология SSL VPN или WebVPN-технология поддерживается на следующих платформах IOS маршрутизаторов:

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

Можно настроить технологию SSL VPN на работу в следующих режимах:

- **Бесклиентная SSL VPN (WebVPN)**. Предоставляет удаленному клиенту, имеющему обозреватель с поддержкой SSL, доступ к веб-серверам HTTP или HTTPS в корпоративной локальной сети (LAN). Кроме того, бесклиентная SSL VPN обеспечивает доступ к файлам Windows через протокол CIFS. Веб-клиент Outlook (OWA) представляет собой пример клиента доступа HTTP.Дополнительную информацию о бесклиентной SSL VPN см. в документе Пример конфигурации бесклиентной SSL VPN

(WebVPN) на Cisco IOS с SDM.

- **Thin-Client SSL VPN (Port Forwarding)** (Thin-Client SSL VPN (переадресация портов)). Предоставляет удаленному клиенту с установленным Java-аплетом, защищенный доступ к приложениям, использующим статичные номера портов, по протоколу управления передачей (TCP). Поддерживается защищенный доступ к протоколам POP3, SMTP, IMAP, ssh и Telnet. Пользователю необходимы права локального администратора, так как производятся изменения в файлах локальной рабочей станции. Данный метод SSL VPN не функционирует с приложениями, использующими динамическое назначение портов, такими как некоторые приложения, использующие протокол передачи файлов (FTP).Дополнительную информацию о Thin-Client SSL VPN см. в документе Пример конфигурации Thin-Client SSL VPN (WebVPN) IOS.**Примечание.** Протокол пользовательских датаграмм (UDP) не поддерживается.
- **SSL VPN Client (SVC Full Tunnel Mode)** (SSL VPN Client (Режим полнофункционального туннеля SVC)). Загружает небольшой клиент для удаленной рабочей станции и предоставляет полный защищенный доступ к ресурсам внутренней корпоративной сети. Возможно выполнение загрузки SVC для постоянного использования или удаление клиента после завершения защищенной сессии.

В данном документе описана конфигурация маршрутизатора Cisco IOS для использования клиентом SSL VPN.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию.

- Microsoft Windows 2000 или XP
- Обозреватель с поддержкой SUN JRE 1.4 или более поздней или браузер под управлением ActiveX
- Права локального администратора у клиента
- Один из маршрутизаторов, перечисленных во Введении с программным обеспечением Advanced Security версии 12.4(6)T или более поздней
- Менеджер устройств безопасности CISCO (SDM) версии 2.3Если Cisco SDM не установлен на маршрутизаторе, можно загрузить бесплатную копию с Software Download (только для зарегистрированных пользователей). Для этого необходима учетная запись CCO и контракт на обслуживание. Дополнительную информацию об установке и настройке SDM см. в документе Маршрутизатор Cisco и менеджер устройств безопасности.
- Цифровой сертификат маршрутизатораВ данном случае можно использовать самозаверяющий сертификат или сертификат выданный сертифицирующим органом (CA). Дополнительную информацию о постоянных самозаверяющих сертификатах см. в документе Постоянные самозаверяющие сертификаты.

Используемые компоненты

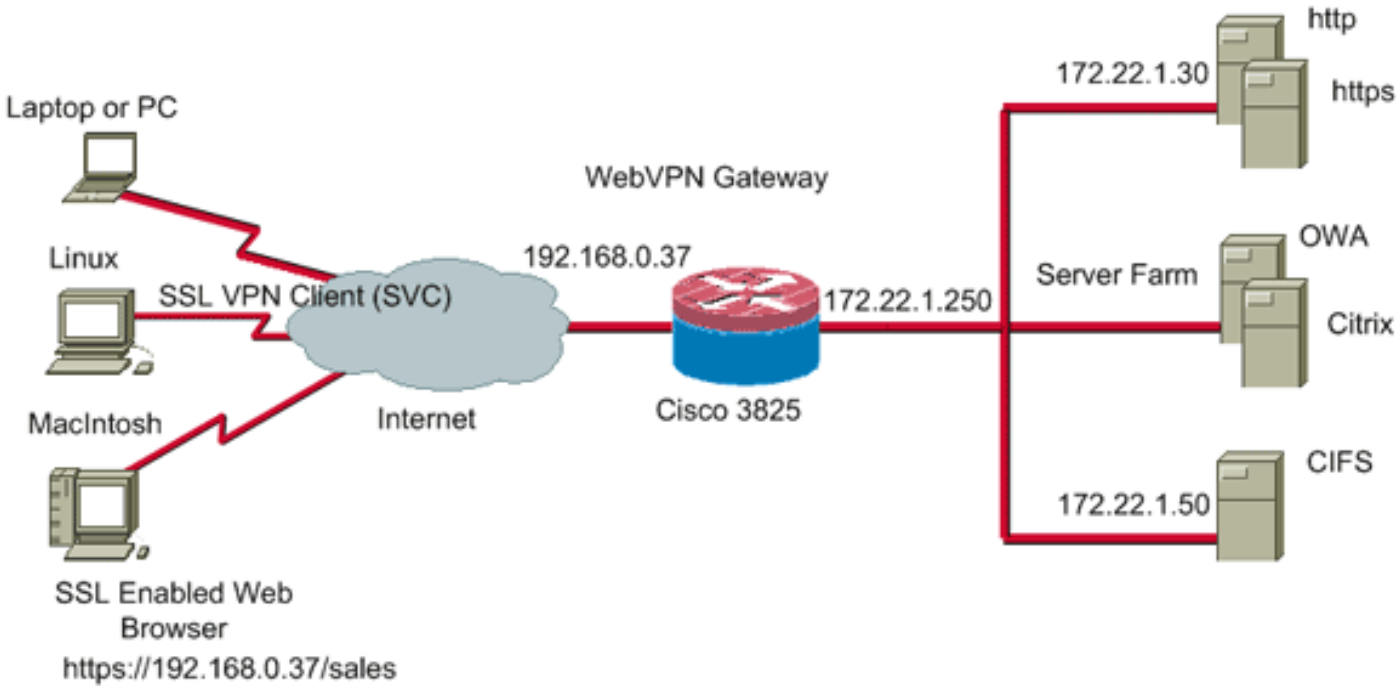
Ниже указаны версии программного обеспечения и аппаратного оборудования, сведения о которых содержатся в данном документе:

- Маршрутизатор Cisco IOS серии 3825 с программным обеспечением 12.4(9)T
- Менеджер устройств безопасности CISCO (SDM) версии 2.3.1

Примечание. Данные для этого документа были получены при тестировании указанных устройств в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, обладают ненастроенной (заданной по умолчанию) конфигурацией. При работе в действующей сети необходимо изучить все возможные последствия каждой команды.

Схема сети

В данном документе используется следующая настройка сети.



Предварительные действия

1. Настройте маршрутизатор на использование SDM. (Опционально)Маршрутизаторы с соответствующей лицензией пакета безопасности уже имеют загруженное во флеш-память приложение SDM. Дополнительную информацию о получении и настройке программного обеспечения см. в документе Загрузка и установка маршрутизатора Cisco и менеджера устройств безопасности (SDM).
2. Загрузите копию клиента (SVC) на ваш управляющий компьютер.Вы можете получить копию программного обеспечения SVC с Software Download: Cisco SSL VPN Client (Загрузка программного обеспечения: клиент Cisco SSL VPN) (только для зарегистрированных пользователей). Для этого необходима действующая учетная запись CCO и контракт на обслуживание.
3. Установите дату, время, часовой пояс и настройте цифровой сертификат на маршрутизаторе.

Условные обозначения

Дополнительную информацию о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

Общие сведения

В начальной стадии клиент SVC загружается в маршрутизатор шлюза WebVPN. При каждом подключении клиента копия SVC загружается на персональный компьютер. Для изменения этого режима настройте маршрутизатор на постоянное присутствие программного обеспечения на компьютере клиента.

Настройка SVC на IOS

В данном разделе описаны действия, необходимые для настройки функций, описанных в документе. В данном примере конфигурации используется мастер SDM для активации SVC на маршрутизаторе IOS.

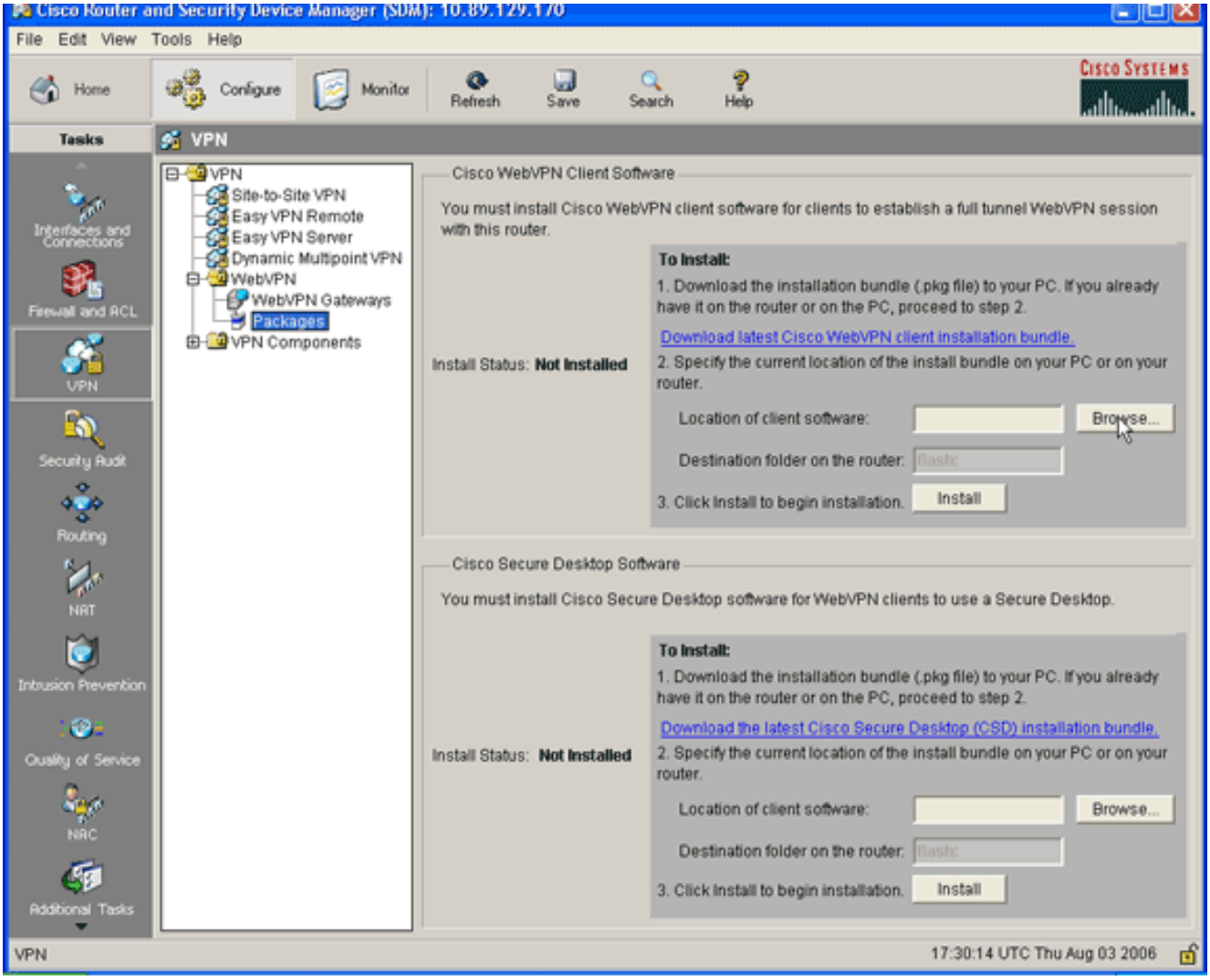
Для настройки SVC-клиента на маршрутизаторе IOS выполните следующие действия:

1. Установите и активируйте программное обеспечение SVC на маршрутизаторе IOS
2. С помощью мастера SDM настройте WebVPN-контекст и WebVPN-шлюз
3. Настройте базу данных пользователей SVC
4. Настройте ресурсы, предоставляемые пользователям

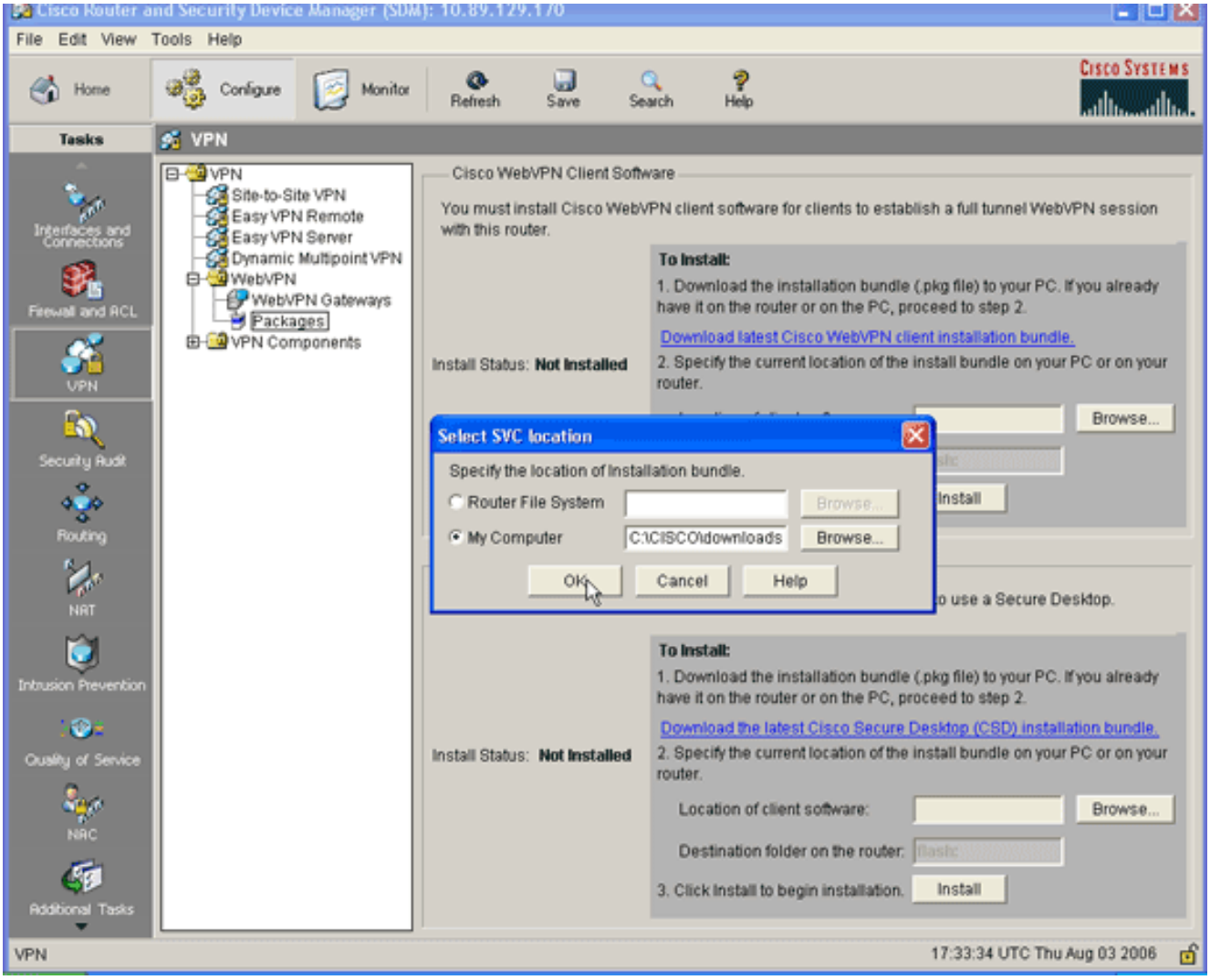
Шаг 1. Установите и активируйте программное обеспечение SVC на маршрутизаторе IOS

Для установки и активации программного обеспечения SVC на маршрутизаторе IOS выполните следующие действия.

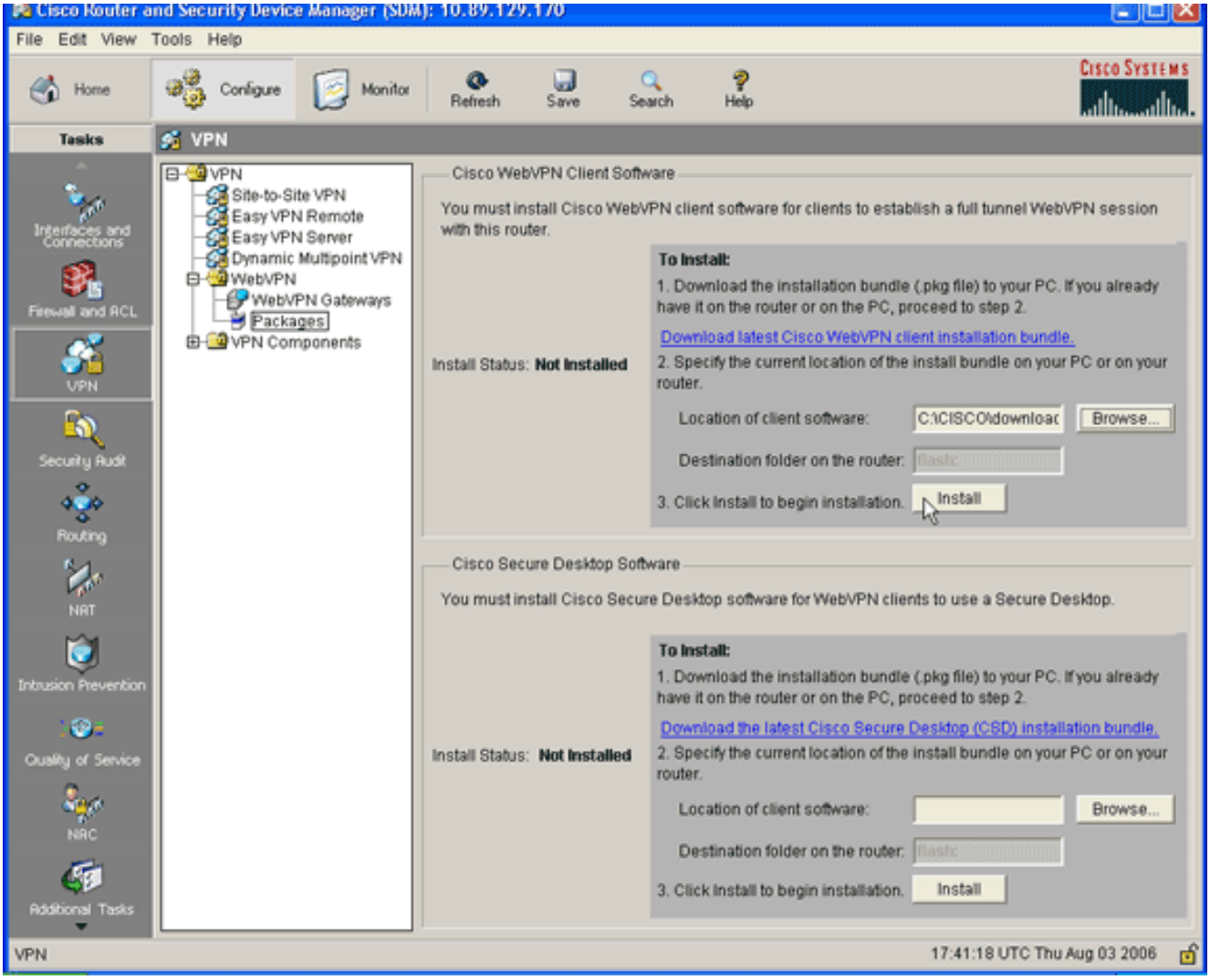
1. Запустите приложение SDM, нажмите **Configure** и затем нажмите **VPN**.
2. Разверните **WebVPN**, и выберите **Packages**.



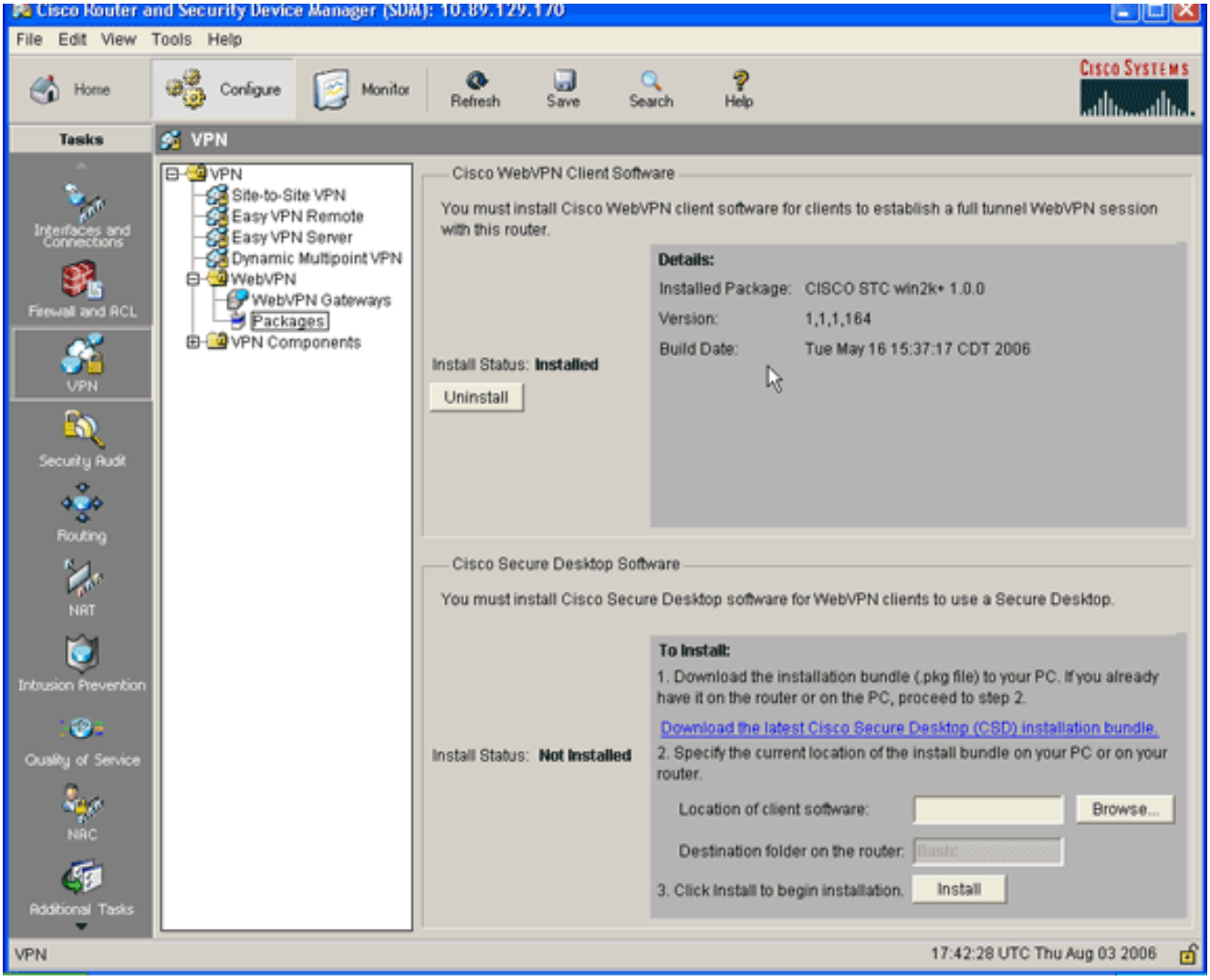
3. В области "Cisco WebVPN Client Software" нажмите кнопку **Browse**.Отобразится диалоговое окно "Select SVC location".



4. Нажмите селективную кнопку **My Computer** и затем кнопку **Browse** и найдите пакет программ SVC на управляющем компьютере.
5. Нажмите **OK** и затем кнопку **Install**.



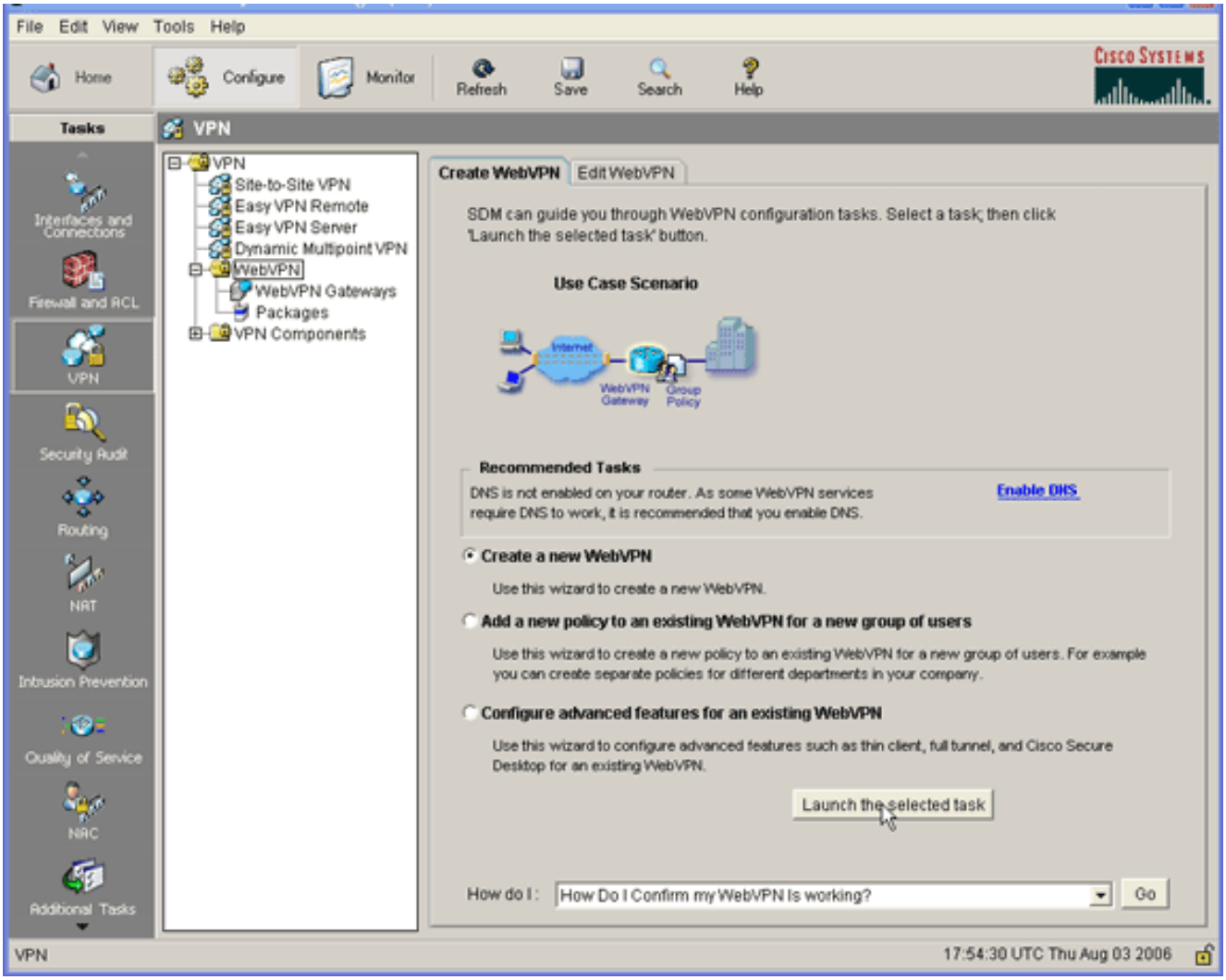
6. Нажмите **Yes** и затем **OK**.Пример успешной установки пакета программ SVC показан на
рисунке:



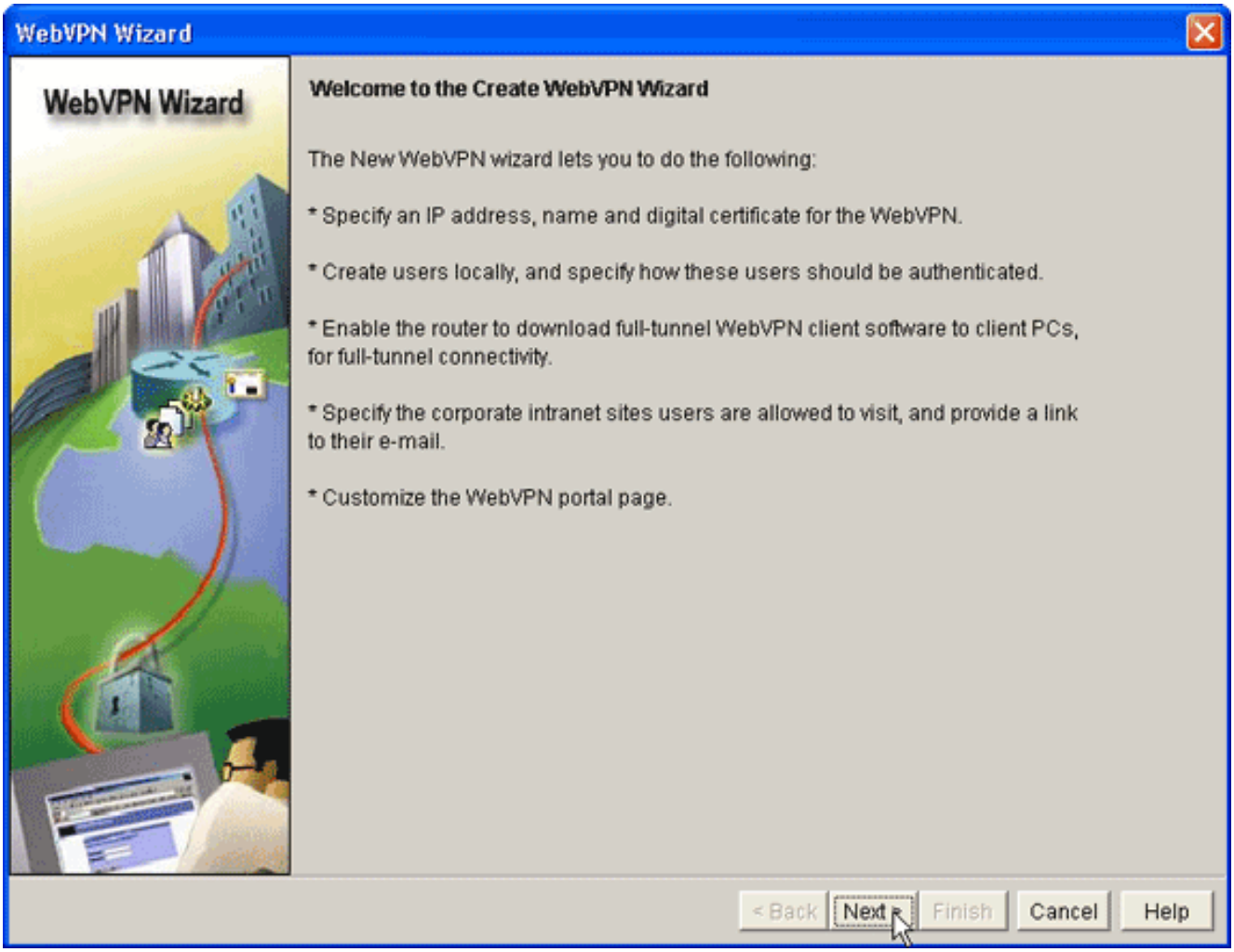
Шаг 2. Настройте WebVPN-контекст и WebVPN-шлюз с помощью мастера SDM

Для настройки WebVPN-контекста и WebVPN-шлюза выполните следующие действия:

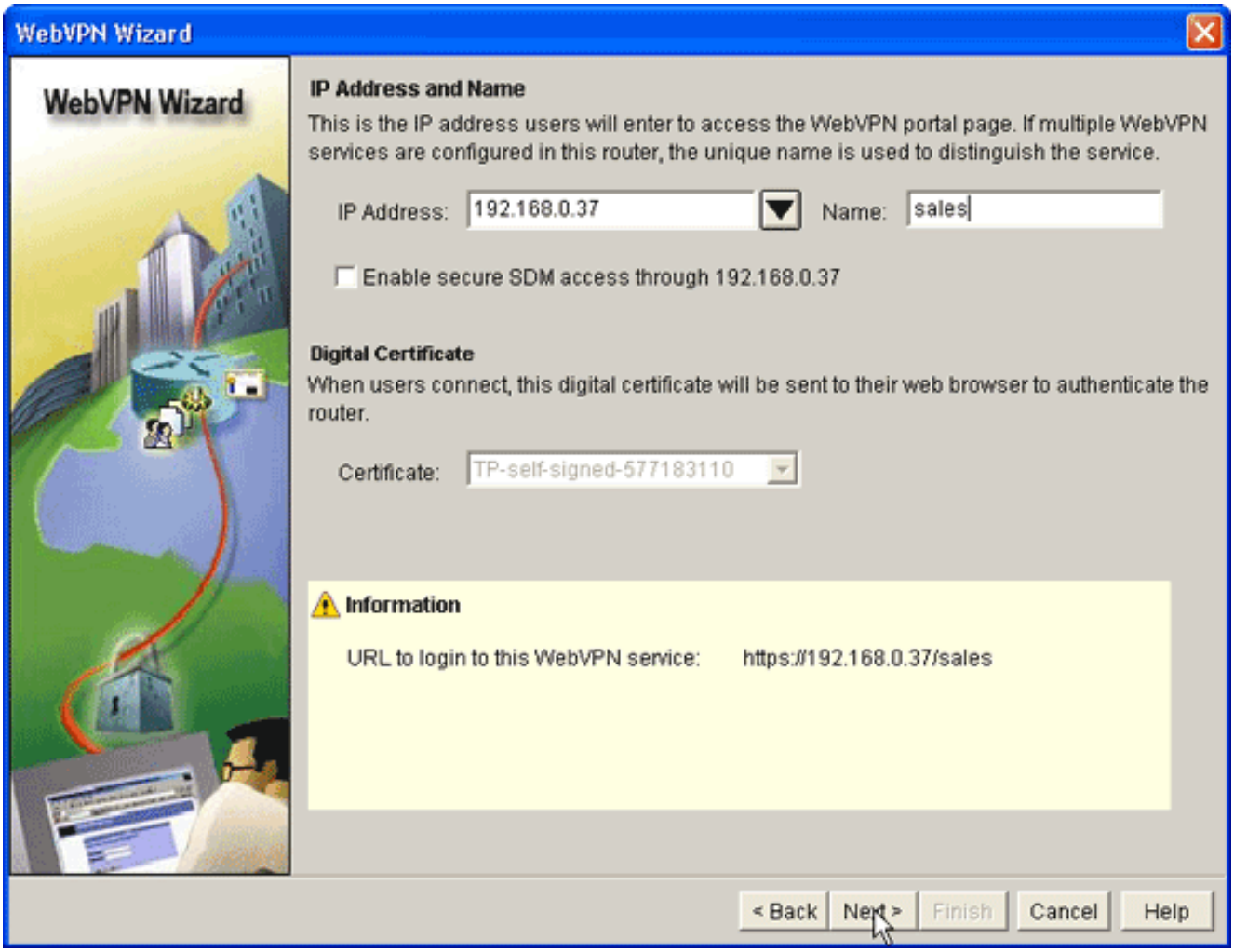
1. После установки SVC на маршрутизатор нажмите **Configure** и затем нажмите **VPN**.
2. Нажмите **WebVPN** и перейдите на вкладку **Create WebVPN**.



3. Нажмите селективную кнопку **Create a New WebVPN** и затем нажмите **Launch the selected task**.Отобразится диалоговое окно "WebVPN Wizard".



4. Нажмите **Next**.



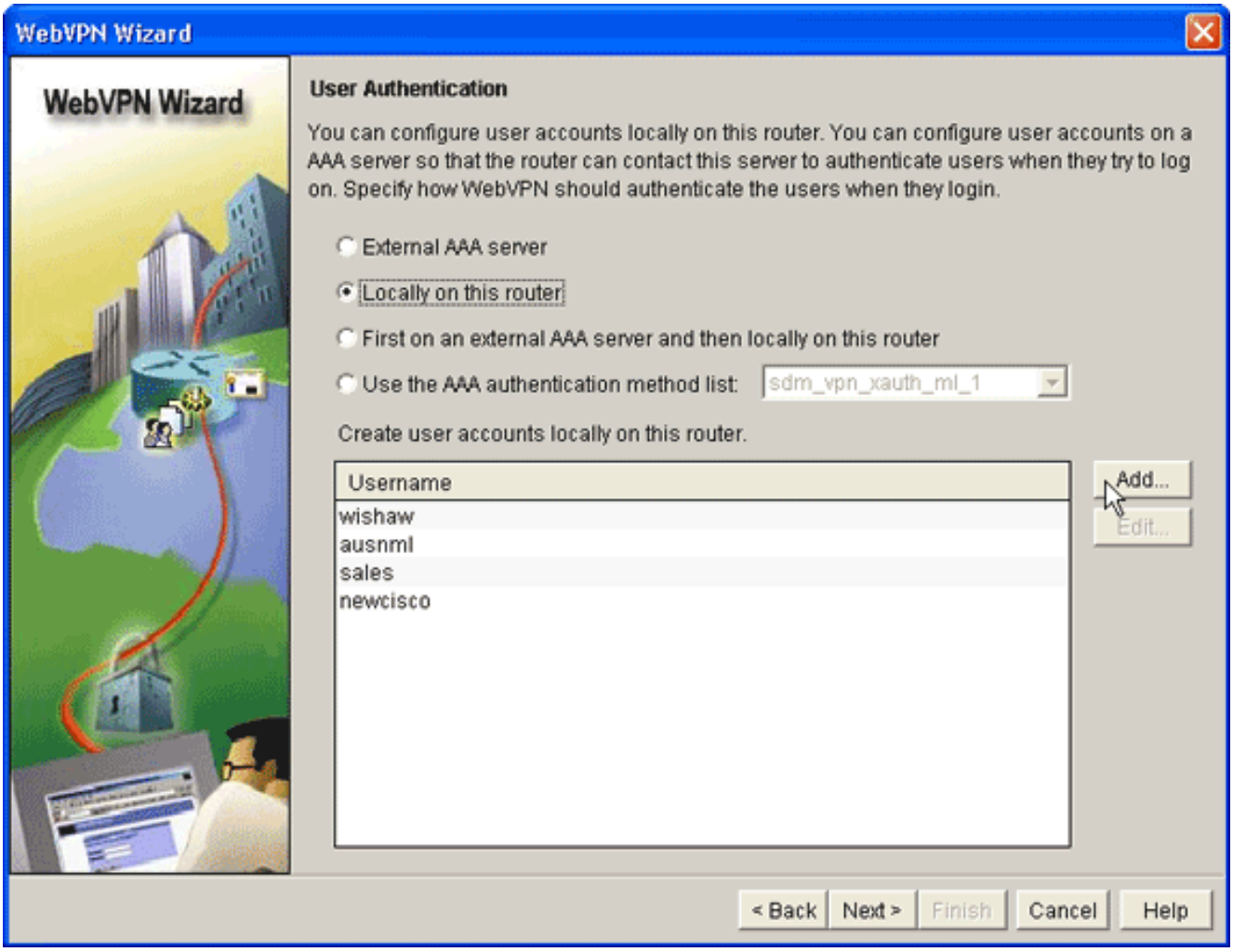
5. Введите IP-адрес нового WebVPN-шлюза и уникальное имя WebVPN-контекста.Можно создать различные WebVPN-контексты для одного IP-адреса (WebVPN-шлюза), но каждое имя должно быть уникальным. В данном примере используется IP-адрес: *https://192.168.0.37/sales*
6. Нажмите **Next** и перейдите к Шагу 3.

Шаг 3. Настройте базу данных пользователей SVC

Для аутентификации можно использовать сервер AAA и/или локальных пользователей. В данном примере конфигурации для аутентификации используются локально созданные учетные записи пользователей.

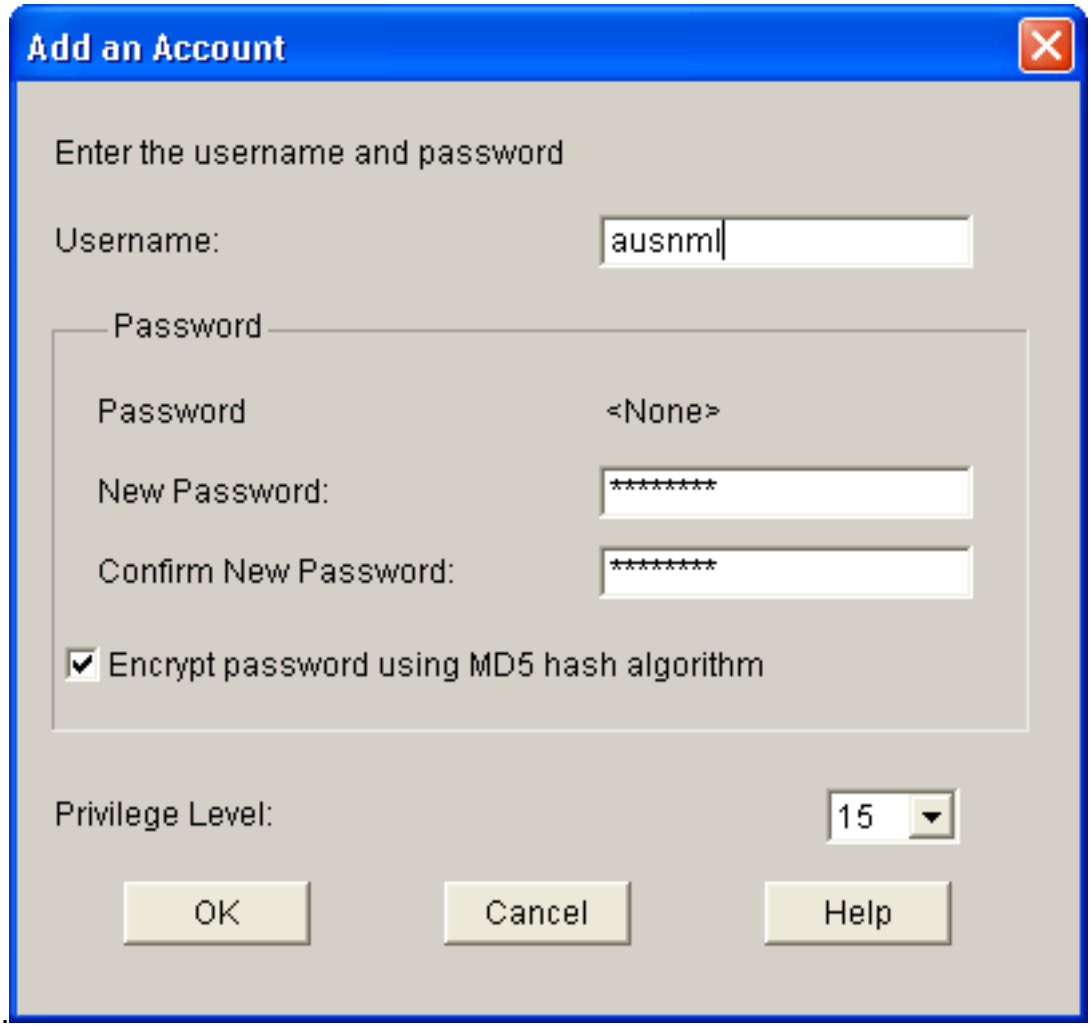
Для настройки базы данных пользователей SVC выполните следующие действия.

1. После выполнения Шага 2 нажмите селективную кнопку **Locally on this router**, расположенную в диалоговом окне мастера WebVPN "User Authentication".



Данное диалоговое окно предназначено для внесения пользователей в локальную базу данных.

2. Нажмите **Add** и введите данные



пользователя.

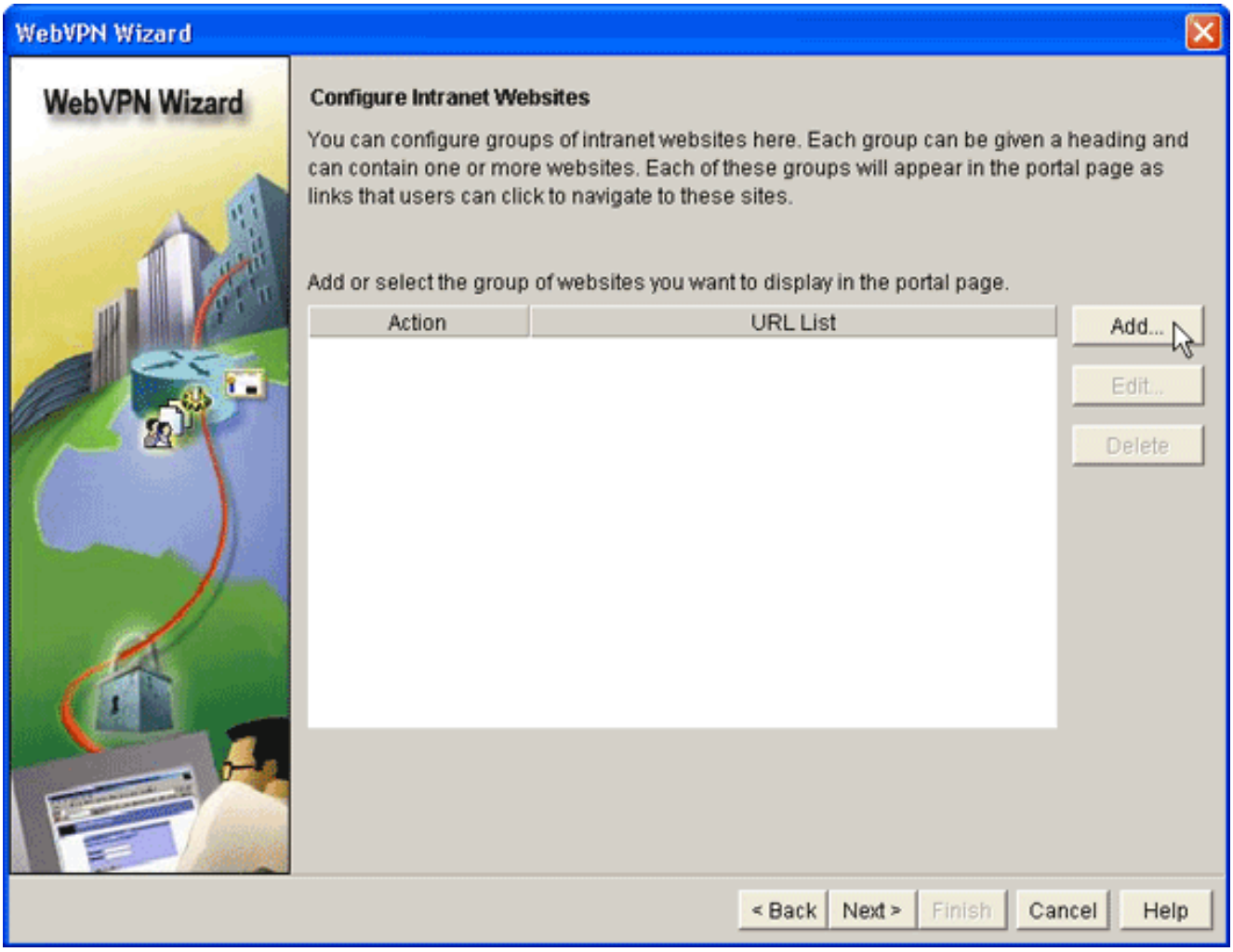
3. Нажмите **OK** и при необходимости внесите дополнительных пользователей.
4. После завершения добавления пользователей нажмите **Next** и перейдите к Шагу 4.

Шаг 4. Настройка ресурсов, предоставляемых пользователям

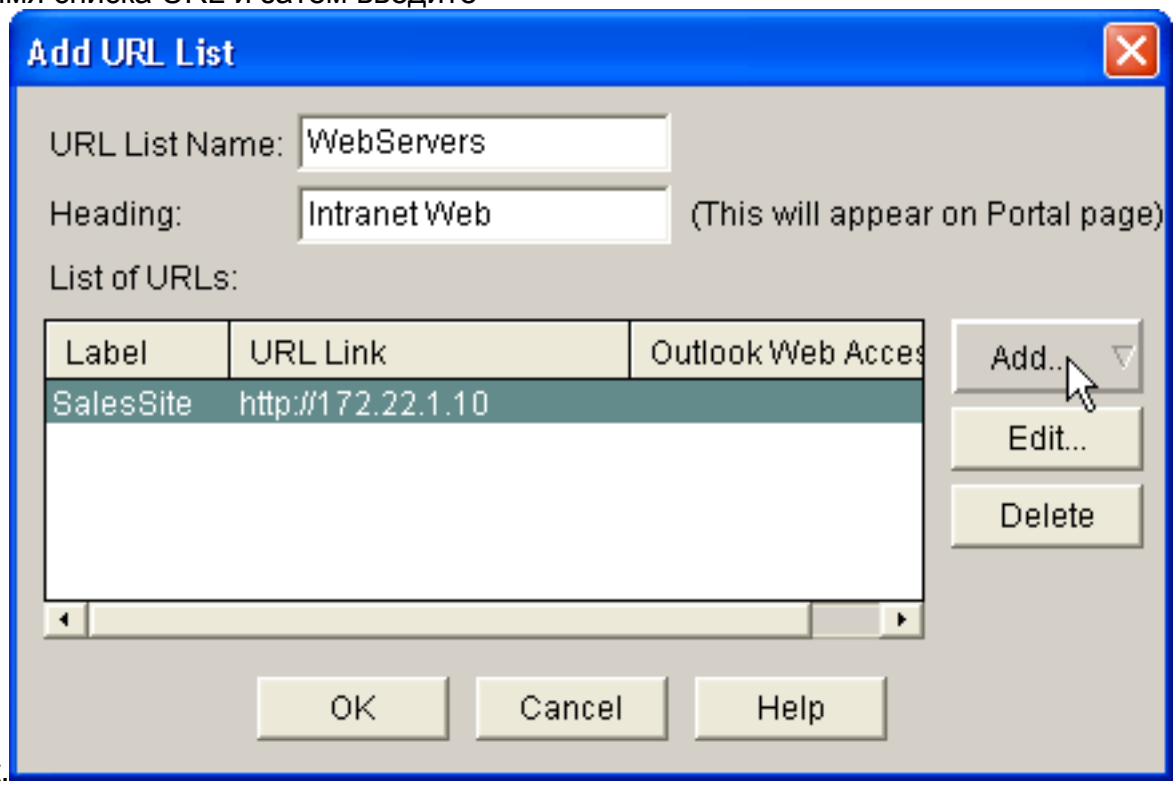
Диалоговое окно мастера WebVPN "Configure Intranet Websites" (Настройка веб-сайтов внутрикорпоративной сети (Интранет)) позволяет выбрать ресурсы интранет, предоставляемые клиентам SVC.

Для настройки предоставления пользователям ресурсов выполните следующие действия:

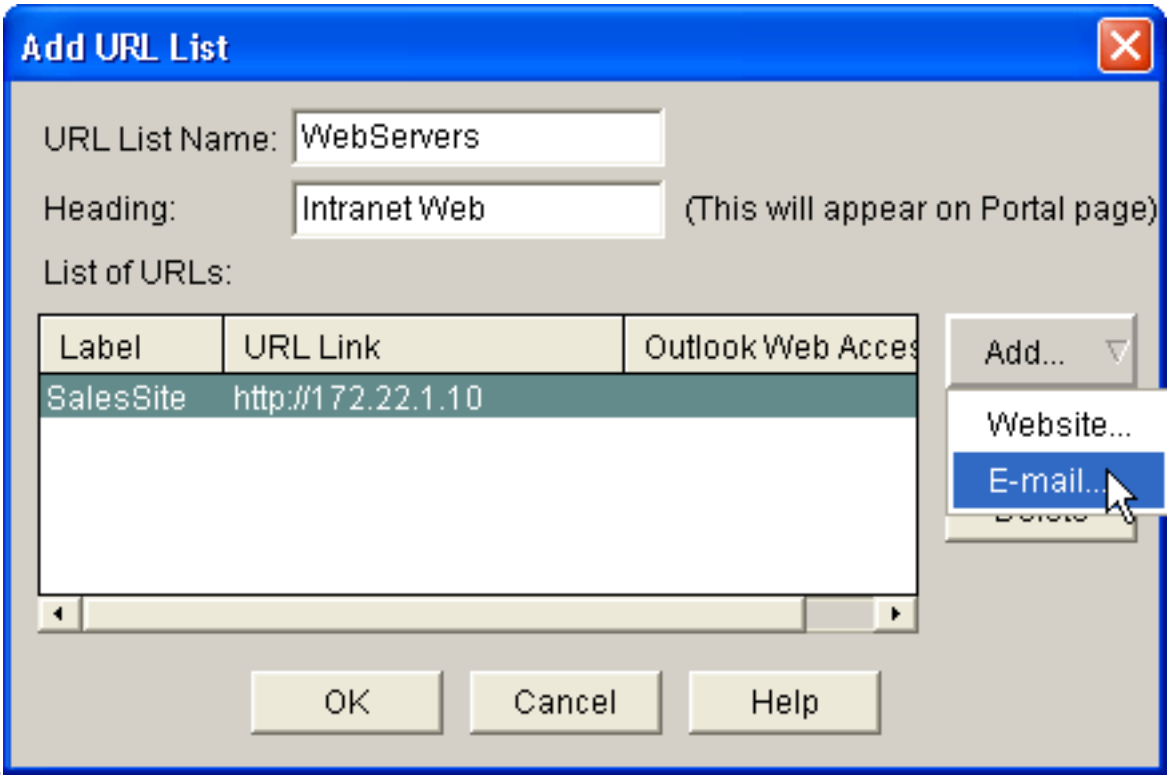
1. По завершении Шага 3 нажмите кнопку **Add**, расположенную в диалоговом окне "Configure Intranet
Websites".



2. Введите имя списка URL и затем введите заголовок.

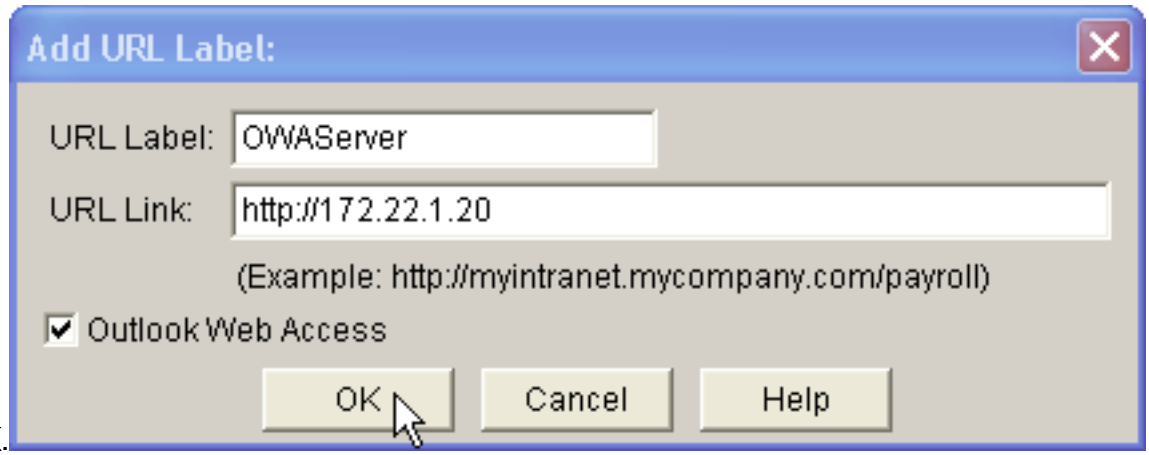


3. Нажмите кнопку **Add** и выберите **Website** для добавления веб-сайтов, доступ к которым предоставляется клиенту.
4. Введите URL и информацию о ссылке и нажмите **OK**.
5. Для предоставления доступа к серверам обмена OWA нажмите **Add** и выберите **E-**



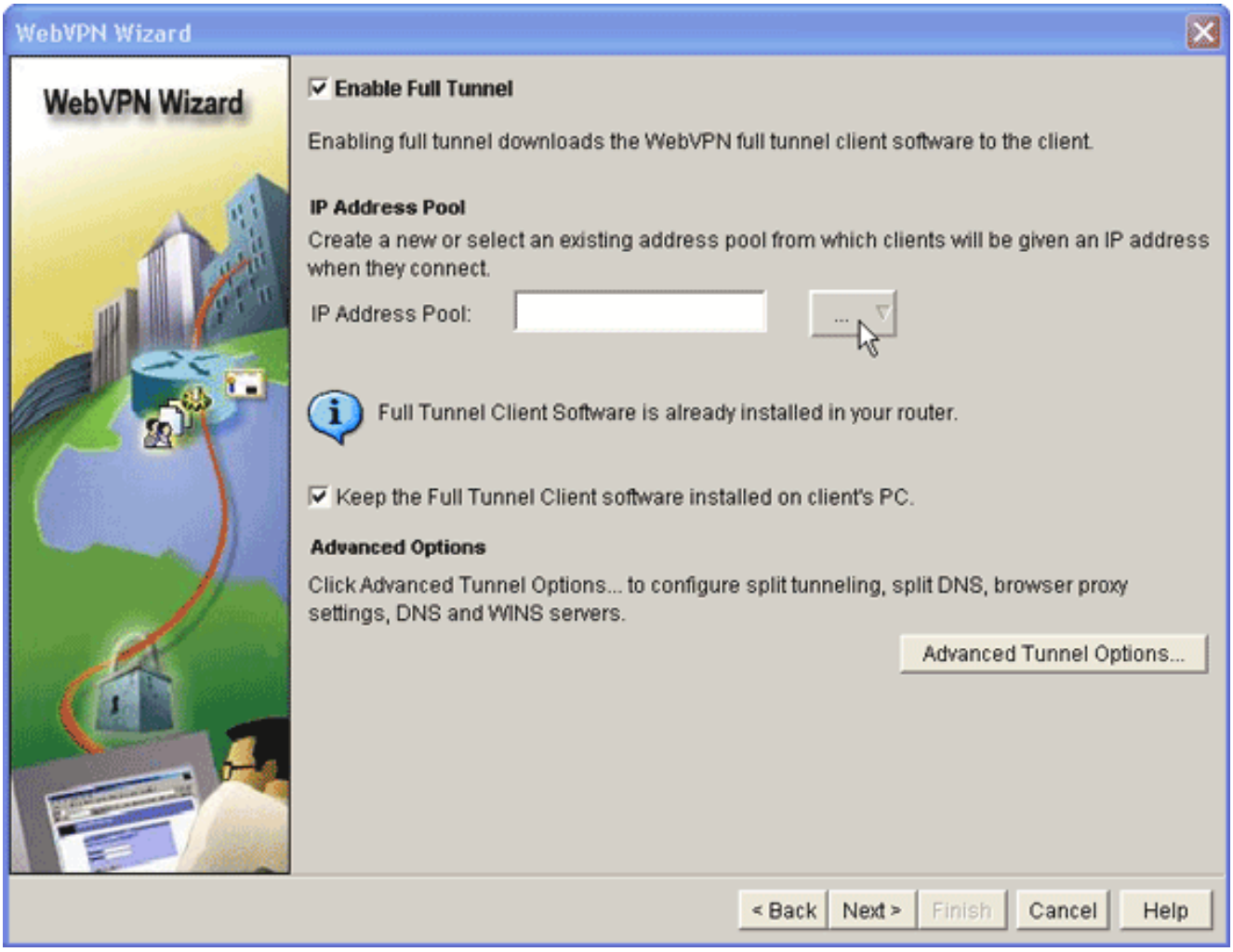
mail.

6. Установите флажок на **Outlook Web Access**, введите метку URL и информацию о ссылке и нажмите

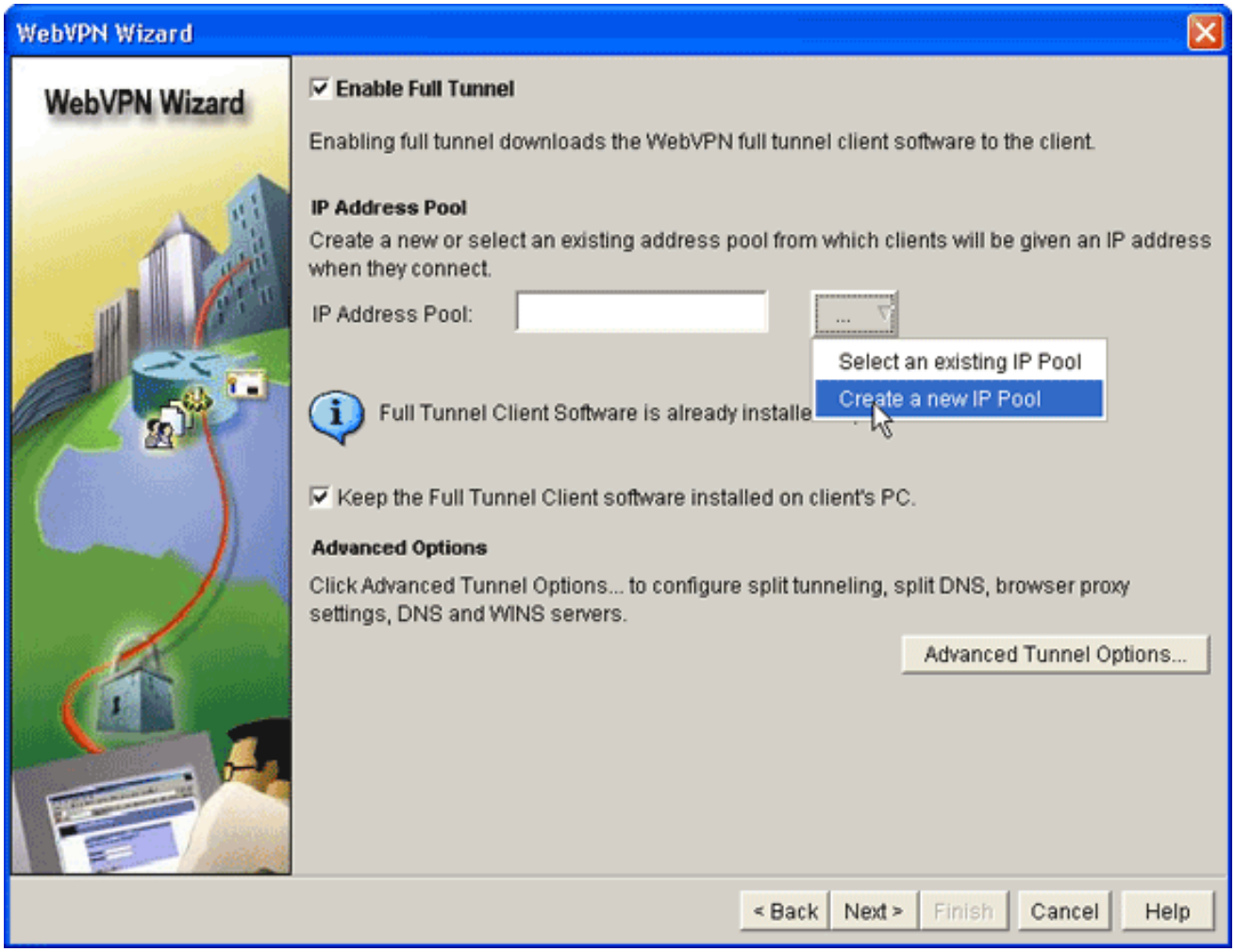


OK.

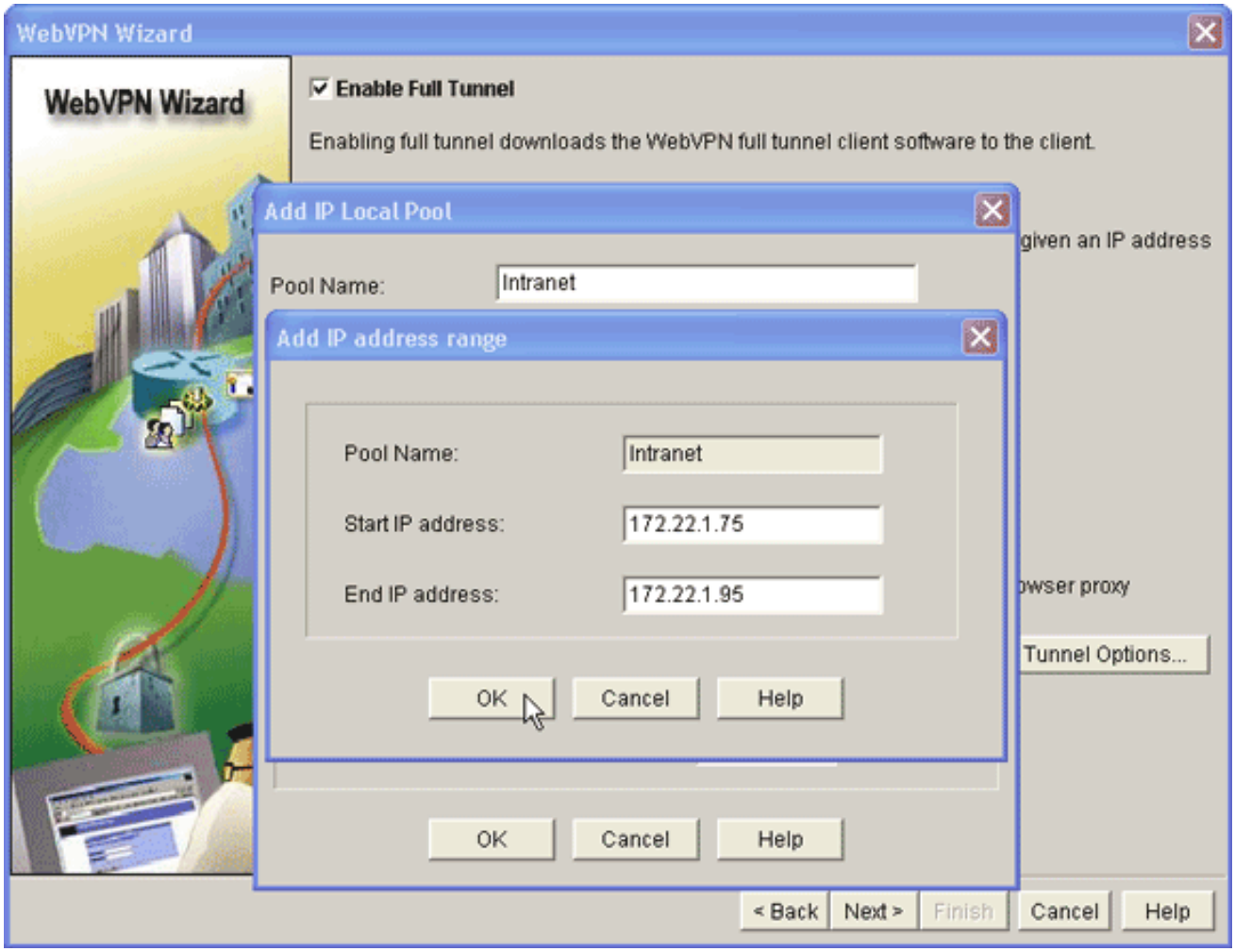
7. После добавления необходимых ресурсов нажмите **OK** и затем кнопку **Next**.Отображается диалоговое окно полнофункционального туннеля мастера WebVPN.



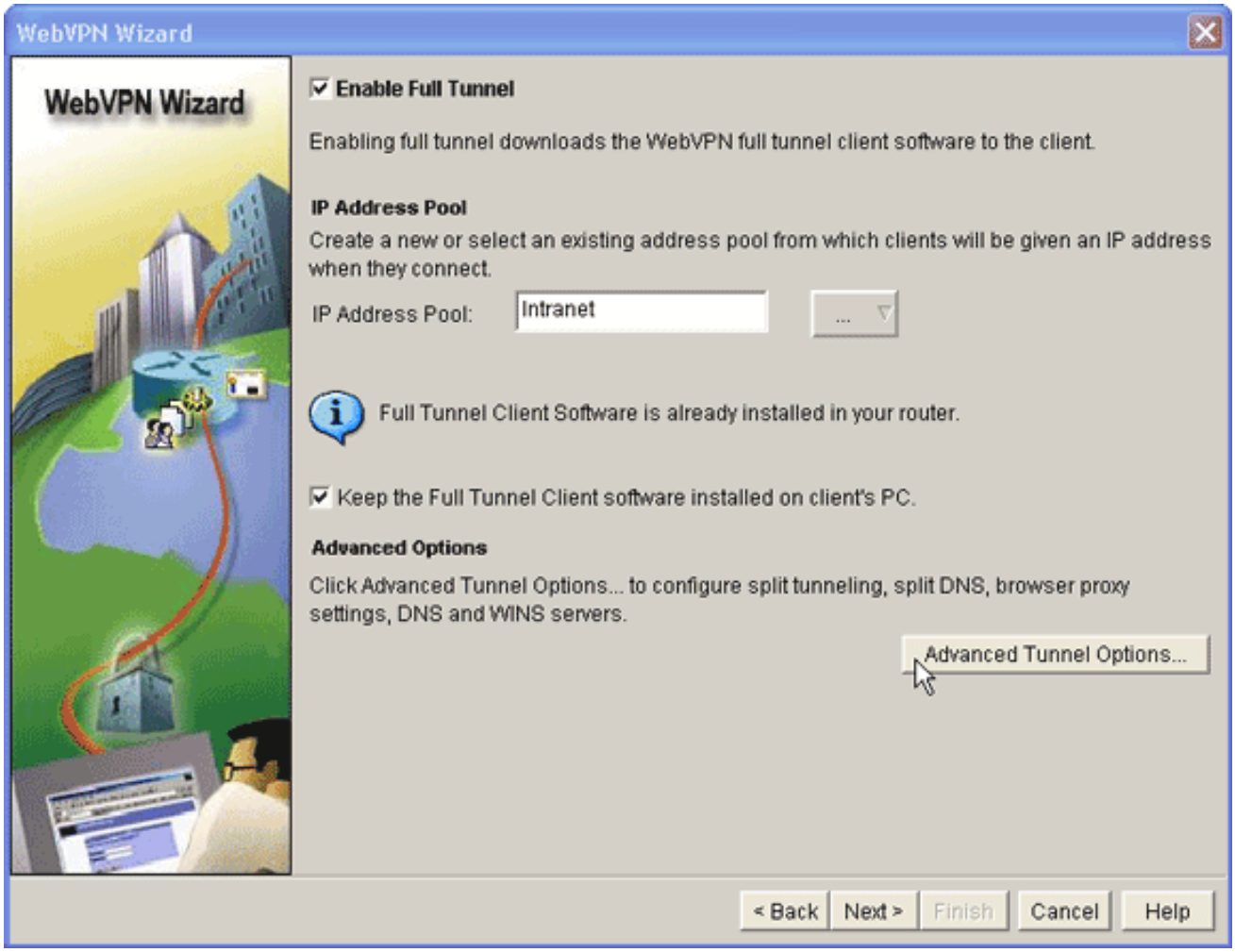
8. Убедитесь, что флажок **Enable Full Tunnel** (активировать полнофункциональный туннель) установлен.
9. Создайте пул IP-адресов, которые могут использовать клиенты данной WebVPN. Адресный пул должен соответствовать адресам, доступным и используемым в вашей сети интранет.
10. Нажмите кнопку "многоточие" (**...**), расположенную рядом с полем "IP Address Pool" и выберите **Create a new IP Pool**.



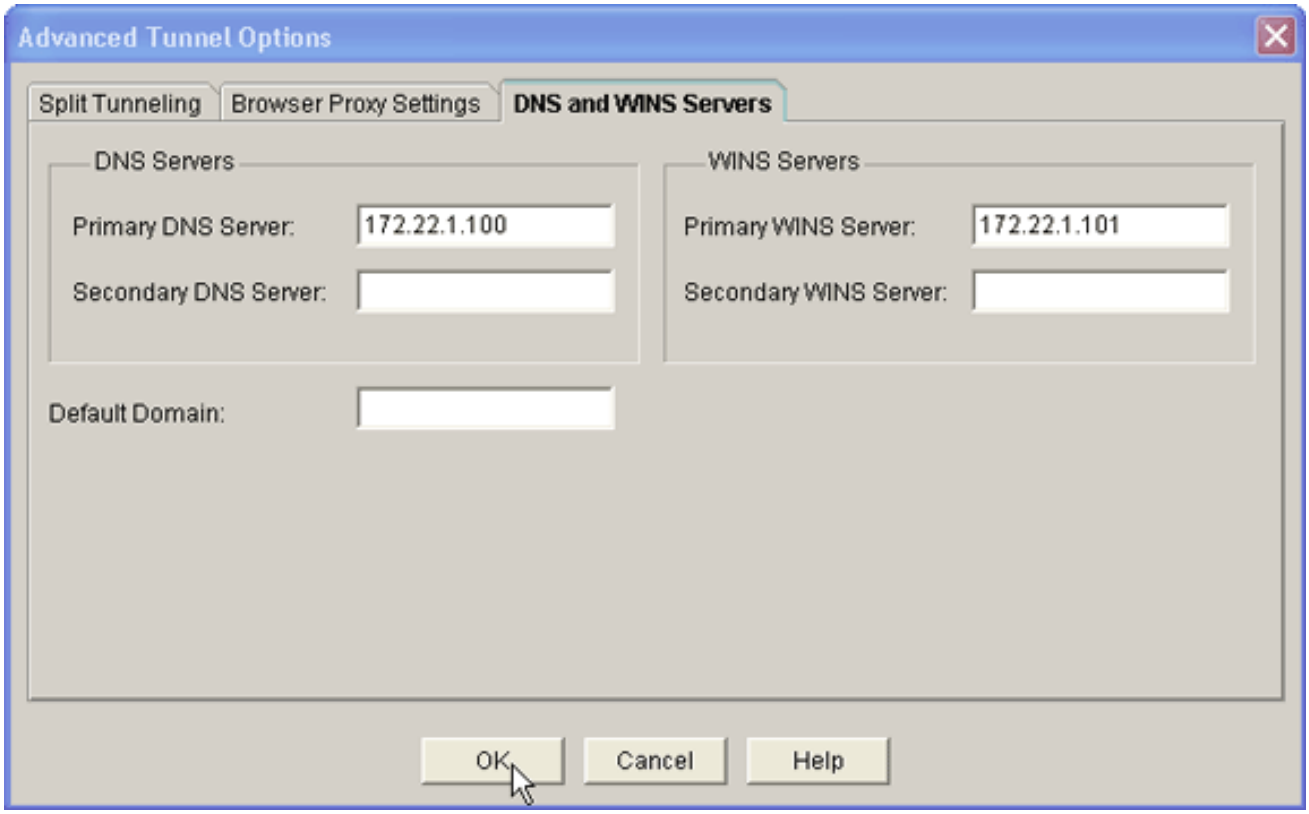
11. В диалоговом окне Add IP Local Pool введите название пула и нажмите **Add**.



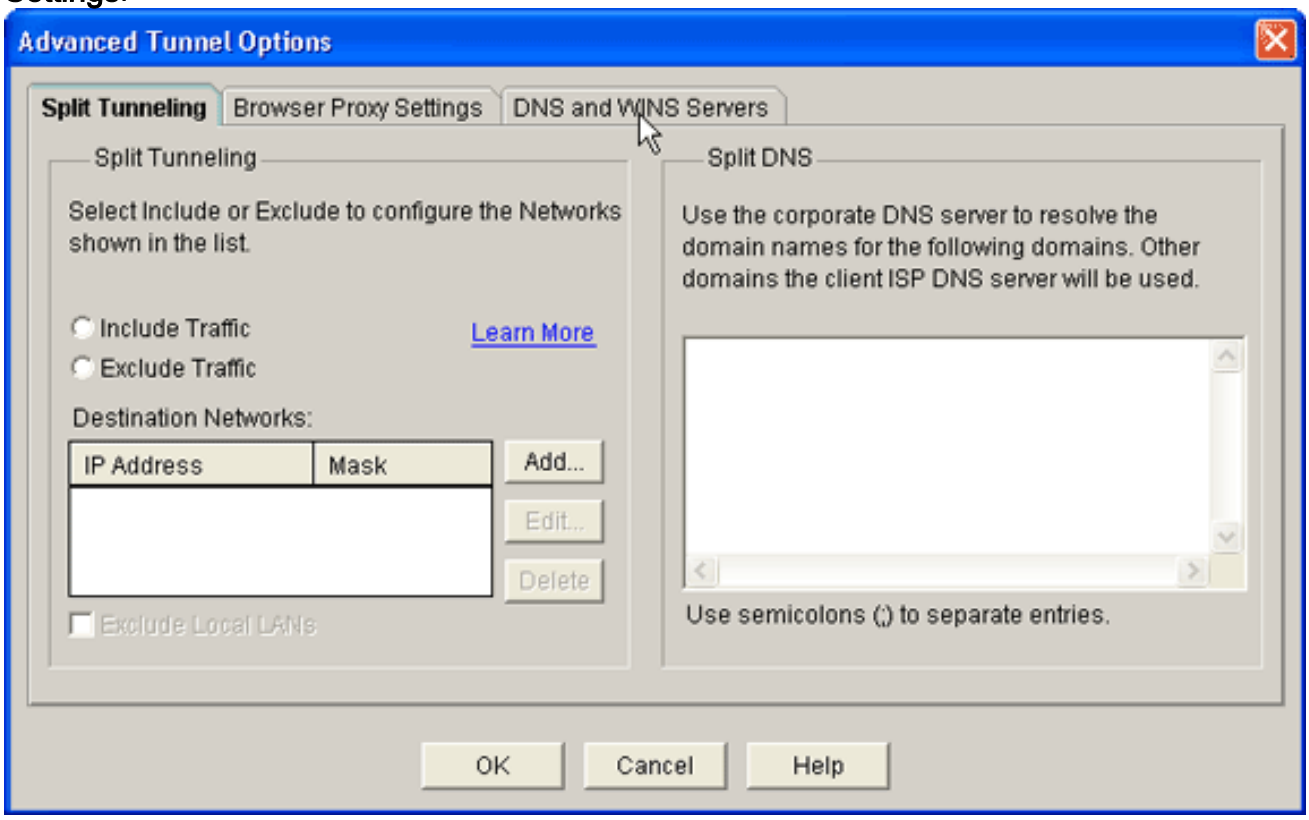
12. В диалоговом окне "Add IP address range" введите диапазон адресов для клиентов SVC и нажмите **OK**.**Примечание.** Пул IP-адресов должен входит в диапазон интерфейса, напрямую соединенного с маршрутизатором. Если вы хотите использовать диапазон пула, не входящий в диапазон вышеназванного интерфейса, вы можете создать адрес обратной связи, ассоциированный с созданным вами новым пулом, для удовлетворения данным требованиям.
13. Нажмите
    OK.



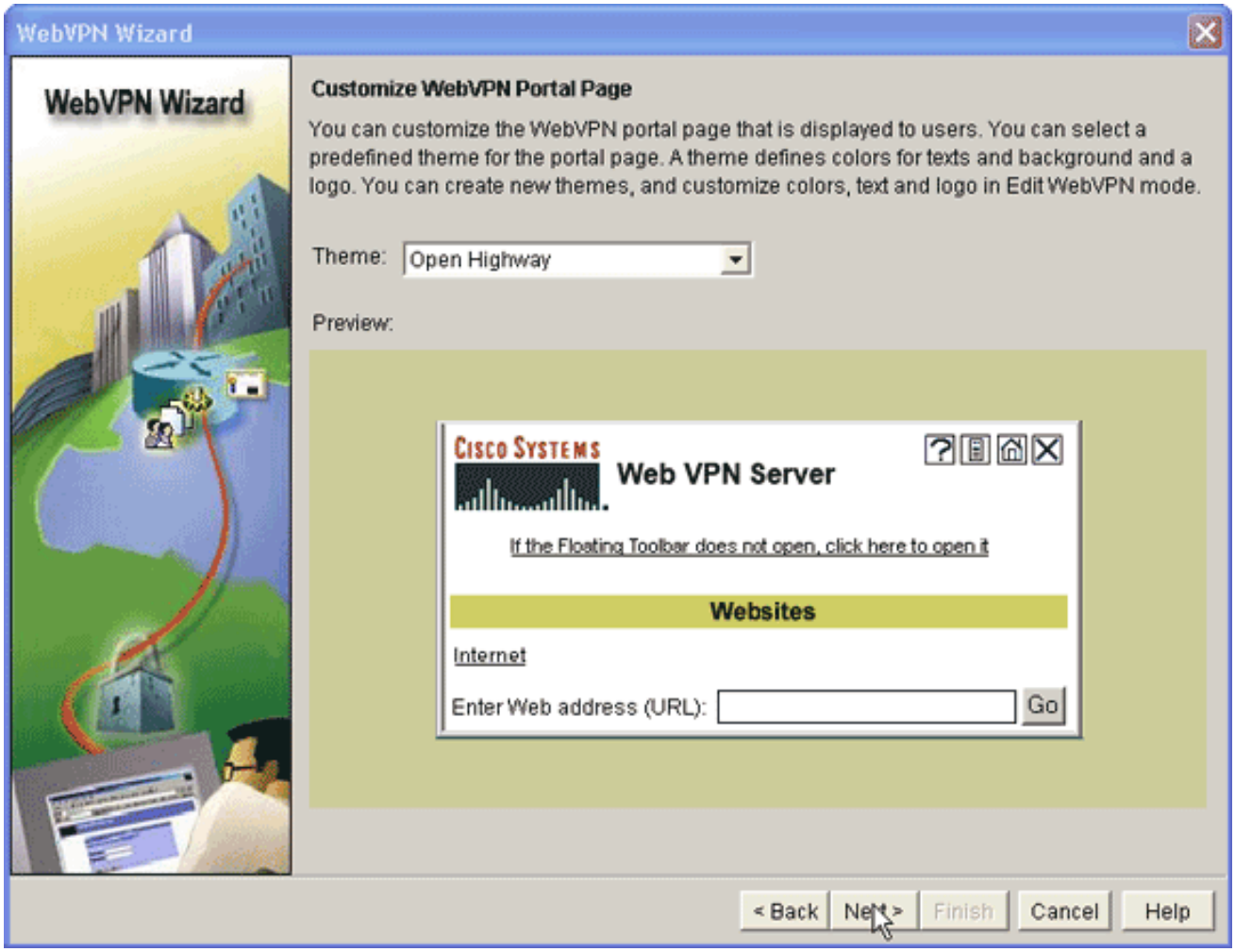
14. Если вы хотите, чтобы удаленные клиенты сохраняли копию SVC, установите флажок **Keep the Full Tunnel Client Software installed on client's PC** (Оставлять программное обеспечение полнофункционального туннеля клиента установленным на компьютере клиента). Снимите флажок для скачивания клиентами программного обеспечения SVC при каждом подключении.
15. Настройте дополнительные параметры туннеля, такие как раздельное туннелирование, раздельный DNS, настройки обозревателя для прокси-сервера, а также серверы DNS и WINS. Компания Cisco рекомендует произвести настройку как минимум серверов DNS и WINS.Для настройки дополнительных параметров туннеля выполните следующие действия:Нажмите кнопку **Advanced Tunnel Options**.



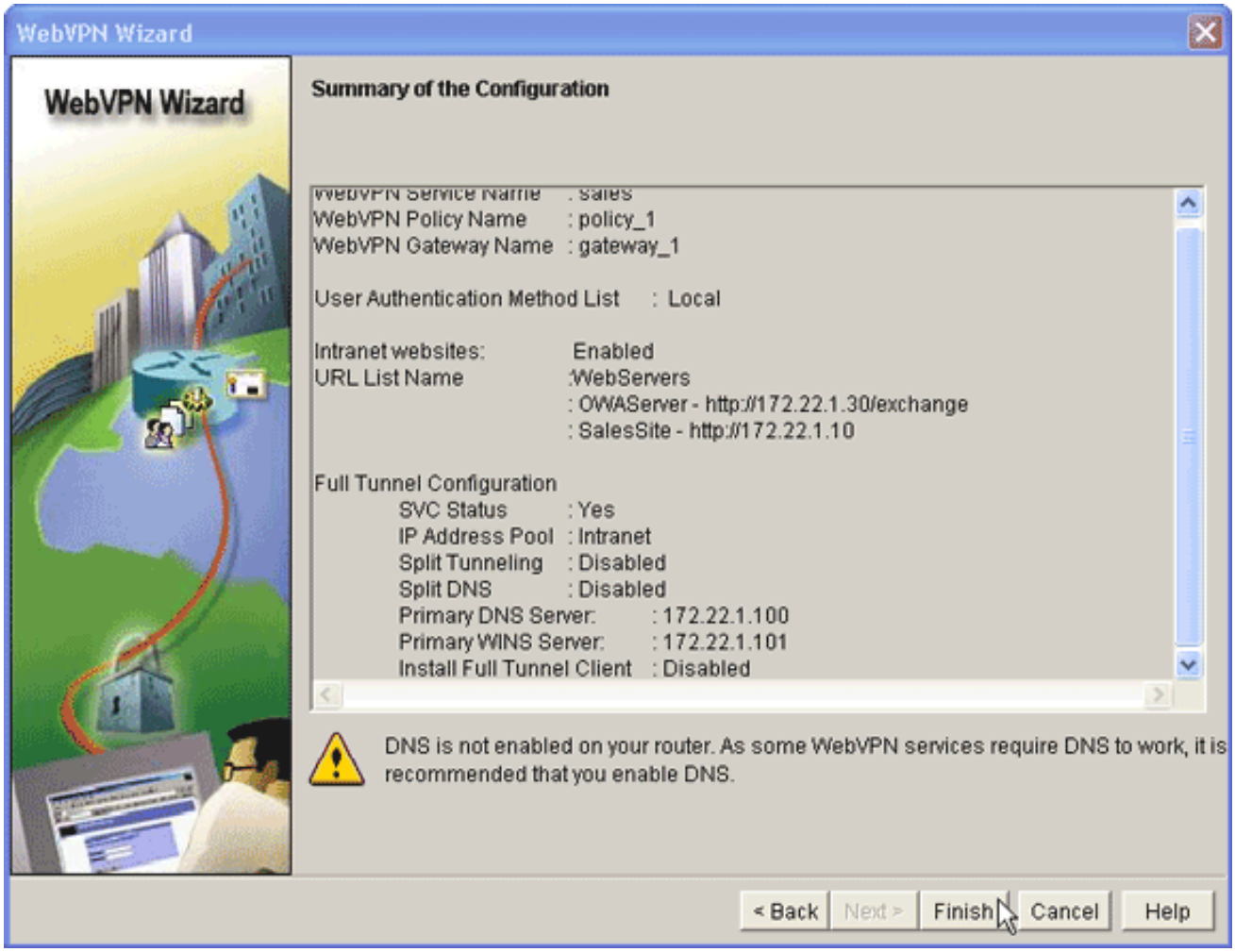
Перейдите на вкладку **DNS and WINS Servers** и введите первичные IP-адреса серверов DNS и WINS.Для настройки раздельного туннелирования и настроек обозревателя для прокси-сервера перейдите на вкладки **Split Tunneling** или **Browser Proxy Settings**.



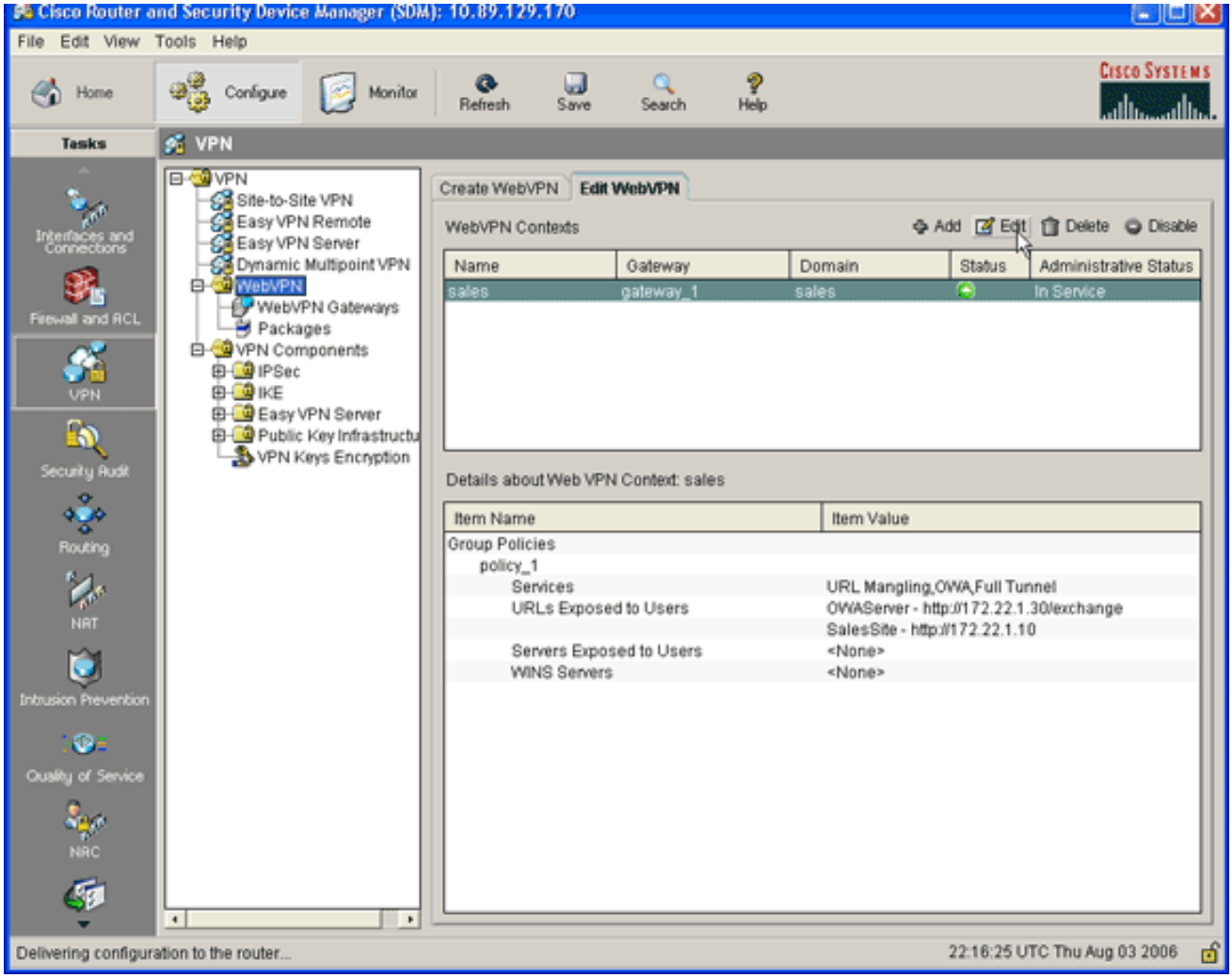
16. После настройки необходимых параметров нажмите **Next**.
17. Измените страницу портала WebVPN или выберите значения по умолчанию.Окно "Customize WebVPN Portal Page" позволяет вам изменить внешний вид страницы портала.



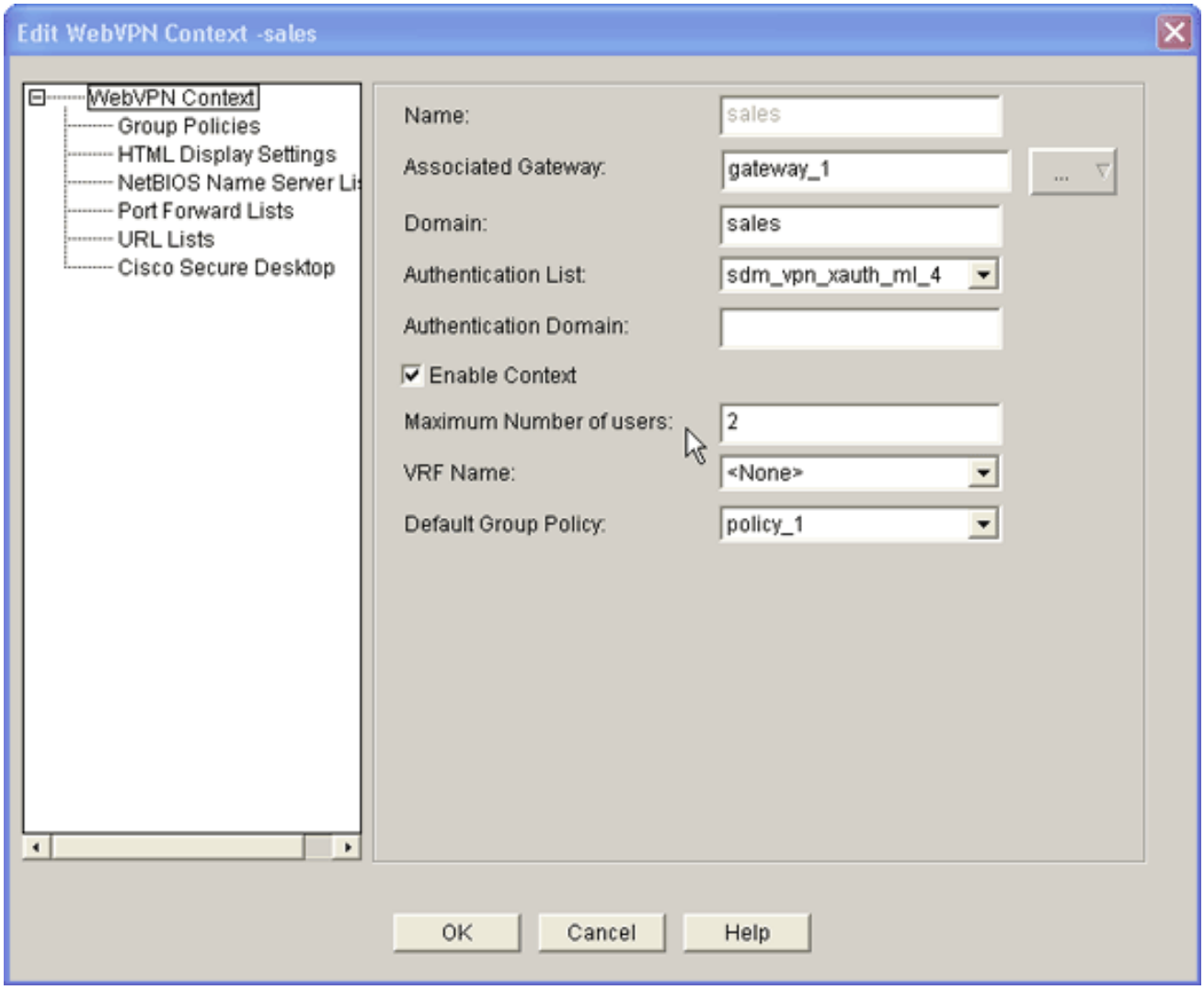
18. После настройки страницы портала WebVPN нажмите **Next**, **Finish** и нажмите **OK**.Мастер WebVPN представит список совершенных настроек.
19. Нажмите **OK** для сохранения конфигурации.**Примечание.** Если вы получили сообщение об ошибке, возможно, что лицензия WebVPN недействительна. Пример сообщения об ошибке показан на следующем
рисунке:



Для решения проблемы с лицензией выполните следующие шаги:Нажмите **Configure** и затем **VPN**.Разверните меню **WebVPN** и перейдите на вкладку **Edit WebVPN**.



Выделите созданный контекст и нажмите кнопку **Edit**.



В поле "Maximum Number of users" введите правильное количество пользователей для вашей лицензии.Нажмите **OK** и затем **OK**.Ваши команды сохранены в конфигурационный файл.Нажмите **Save** и затем кнопку **Yes** для принятия сделанных изменений.

Результаты

ASDM создает следующие конфигурации командных строк:

ausnml-3825-01

```
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
!
!---  SDM   aaa  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 !---    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 !-
--  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 !---       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 !---     webvpn gateway
gateway_1 ip address 192.168.0.37 port 443 http-redirect
port 80 ssl trustpoint TP-self-signed-577183110
inservice !---    SVC webvpn install svc
flash:/webvpn/svc.pkg ! !---  WebVPN webvpn context
sales title-color #CCCC66 secondary-color white text-
color black ssl authenticate verify all ! !--- ,
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 !-
--      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
```

Проверка

Используйте этот раздел для того, чтобы подтвердить, что ваша конфигурация функционирует должным образом.

Процедура

Для проверки конфигурации введите *http://192.168.0.37/sales* в веб-обозревателе клиента с поддержкой SSL.

Команды

Некоторые команды **show** ассоциированы с WebVPN. Эти команды можно ввести в интерфейсе командной строке (CLI) для отображения статистики и другой информации. Дополнительную информацию о командах **show** см. в документе Проверка конфигурации WebVPN.

Примечание. Интерпретатор выходных данных (только для зарегистрированных заказчиков) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитики выходных данных команды **show**.

Поиск и устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Неполадки с подключением SSL

Проблема. Клиенты SSL VPN не могут подключиться к маршрутизатору.

Решение. Недостаточное количество IP-адресов в адресном пуле может вызвать подобную проблему. Для решения данной проблемы увеличьте количество IP-адресов в адресном пуле маршрутизатора.

Команды отладки

Некоторые команды **clear** ассоциированы с WebVPN. Дополнительную информацию о данных командах см. в документе Использование команд WebVPN "clear".

Некоторые команды **debug** ассоциированы с WebVPN. Дополнительную информацию о данных командах см. в документе Использование команд WebVPN "debug".

Примечание. Использование команд **debug** может неблагоприятно сказаться на производительности модуля Cisco. Перед использованием команд **debug** ознакомьтесь с документом Важная информация по командам "debug".

Дополнительные сведения

- Cisco IOS SSLVPN

- SSL VPN – WebVPN
- Пример конфигурации бесклиентной SSL VPN (WebVPN) на Cisco IOS с SDM
- Пример конфигурации Thin-Client SSL VPN (WebVPN) IOS с SDM
- Инструкции по осуществлению конвергенции совмещения WebVPN и DMVPN
- Cisco Systems – техническая поддержка и документация