Пример конфигурации "Маршрутизатор Cisco как удаленный VPN-сервер, использующий SDM"

Содержание

Введение

В этом документе описано использование Cisco Security Device Manager (SDM) для настройки маршрутизатора Cisco в качестве сервера Easy VPN. Cisco SDM позволяет настроить маршрутизатор в качестве сервера VPN для клиента Cisco VPN с помощью простого в использовании веб-интерфейса управления. После завершения настройки маршрутизатора Cisco ее можно проверить с помощью клиента Cisco VPN.

Предварительные условия

Требования

В этом документе предполагается, что маршрутизатор Cisco полностью исправен и в нем разрешено изменение конфигурации с помощью Cisco SDM.

Примечание. Чтобы разрешить настройку маршрутизатора с помощью SDM, см. раздел Включение HTTPS-доступа для SDM.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Маршрутизатор Cisco 3640 с ПО Cisco IOS версии 12.3 (14T)

Security Device Manager версия 2.31

VPN-клиент Cisco версии 4.8

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

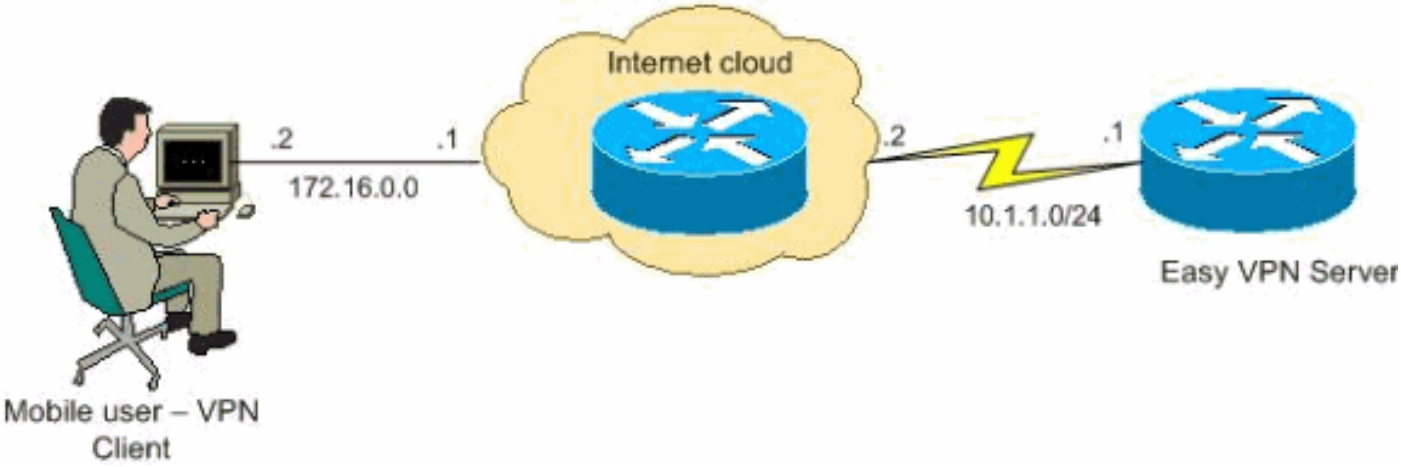
Настройка

В этом разделе представлена информация о настройке функции сервера Easy VPN, которая позволяет удаленному конечному пользователю обмениваться данными с любым VPN-шлюзом Cisco IOS®, используя протокол IPsec.

Примечание. Для поиска дополнительной информации о командах, приведенных в данном документе, используйте инструмент Средство поиска команд (только для зарегистрированных пользователей).

Схема сети

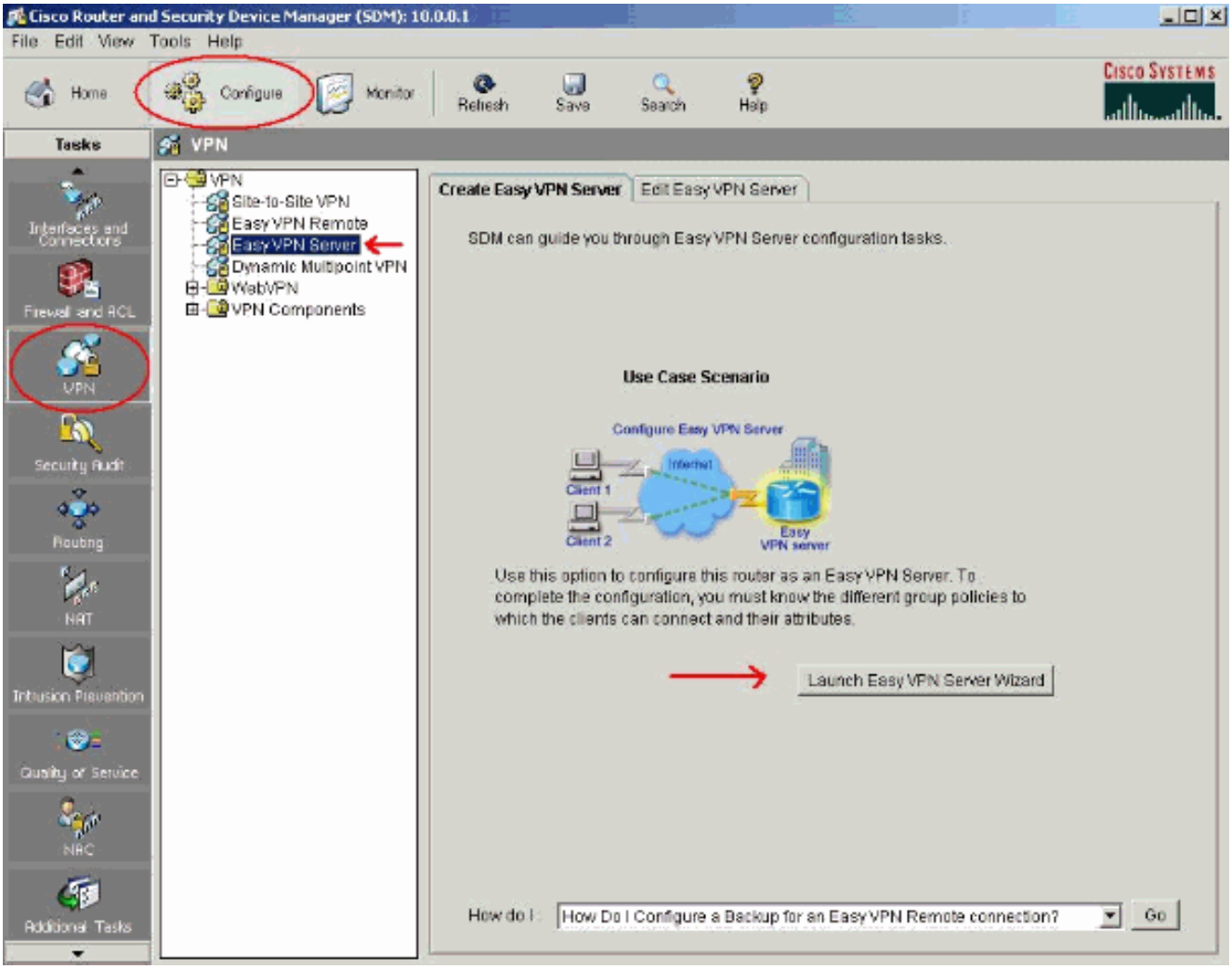
В настоящем документе используется следующая схема сети:



Процедура конфигурации

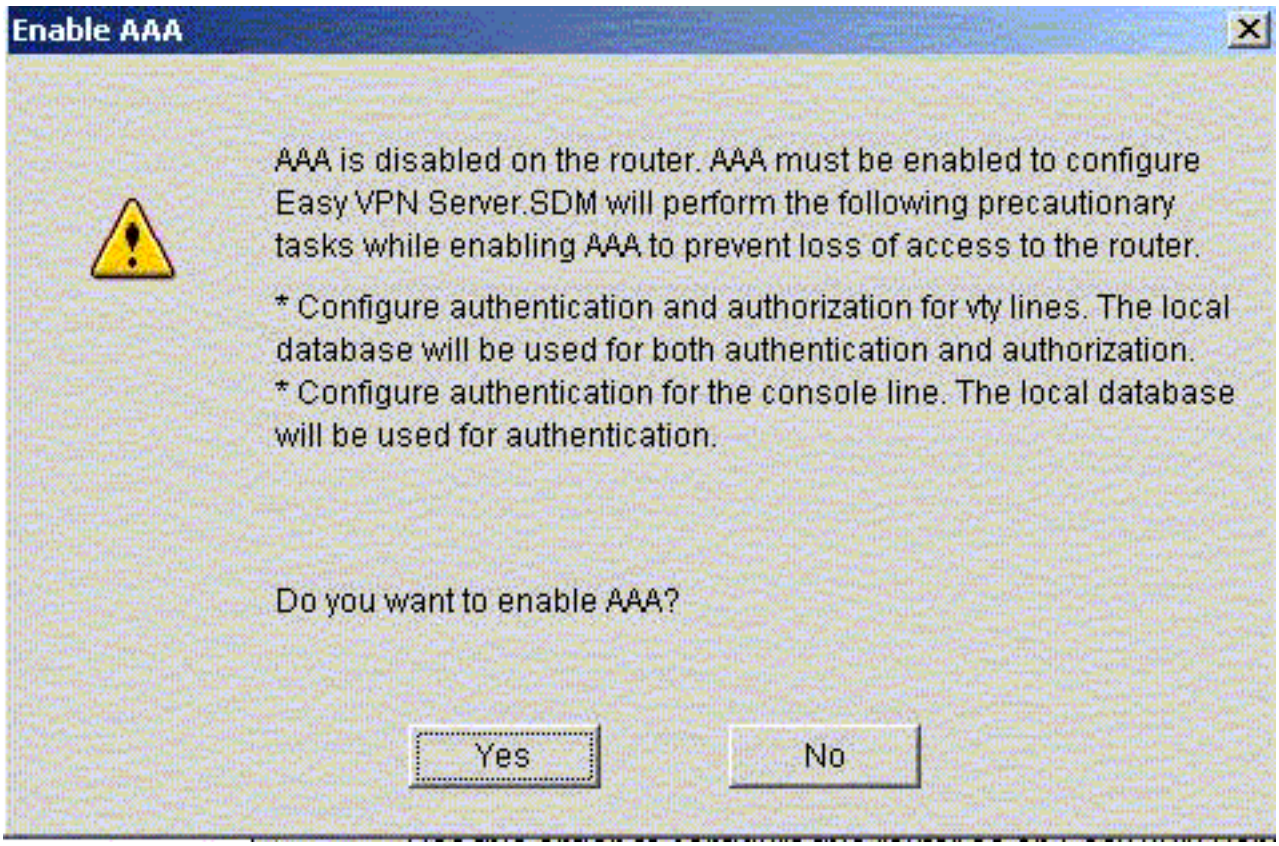
Чтобы настроить маршрутизатор Cisco в качестве удаленного VPN-сервера с помощью SDM, выполните следующие действия.

1. Выберите **Configure > VPN > Easy VPN Server** в окне Home и нажмите **Launch Easy VPN Server Wizard**.

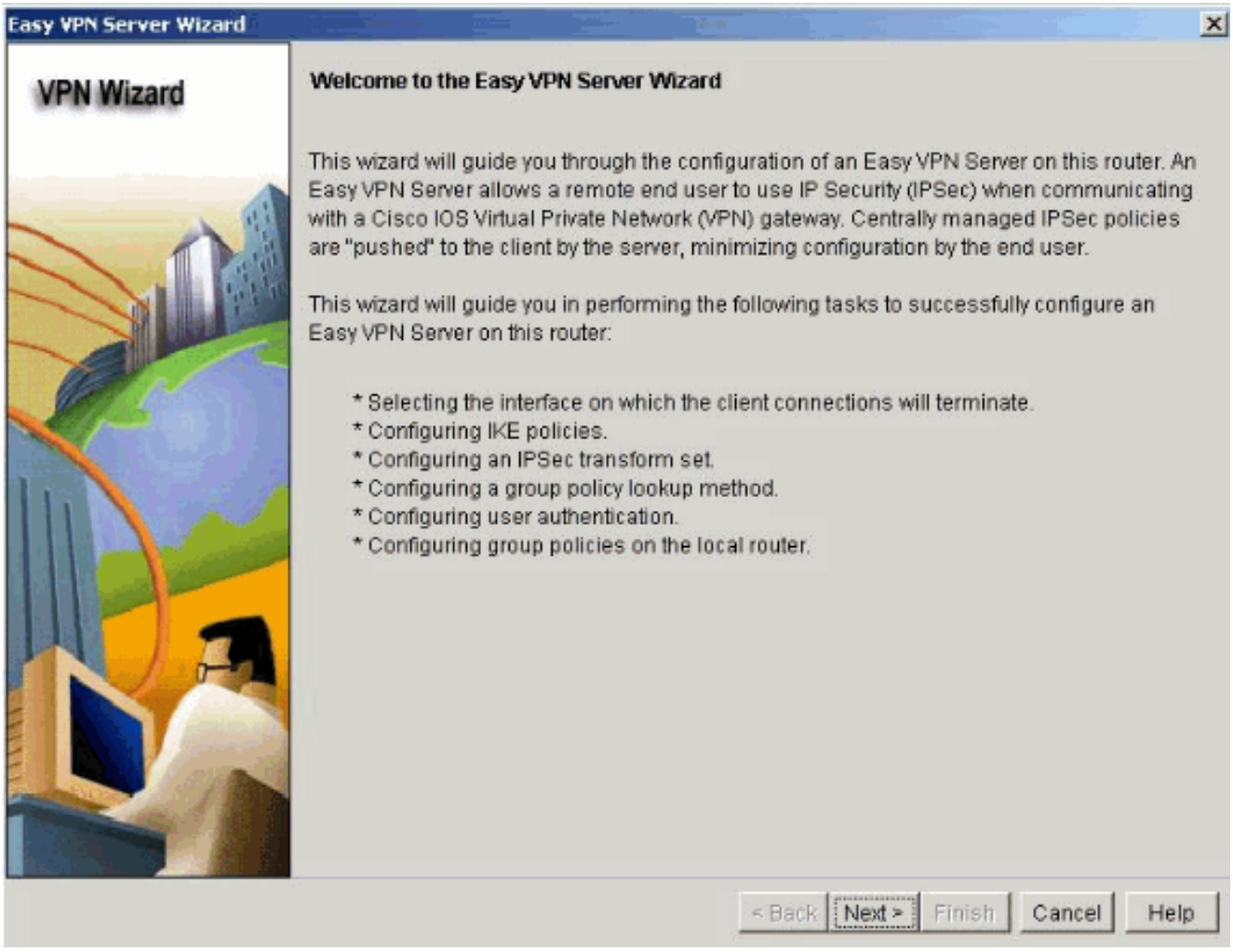


AAA должен быть включен на маршрутизаторе до начала настройки сервера Easy VPN. Нажмите **Да**, чтобы продолжить настройку.

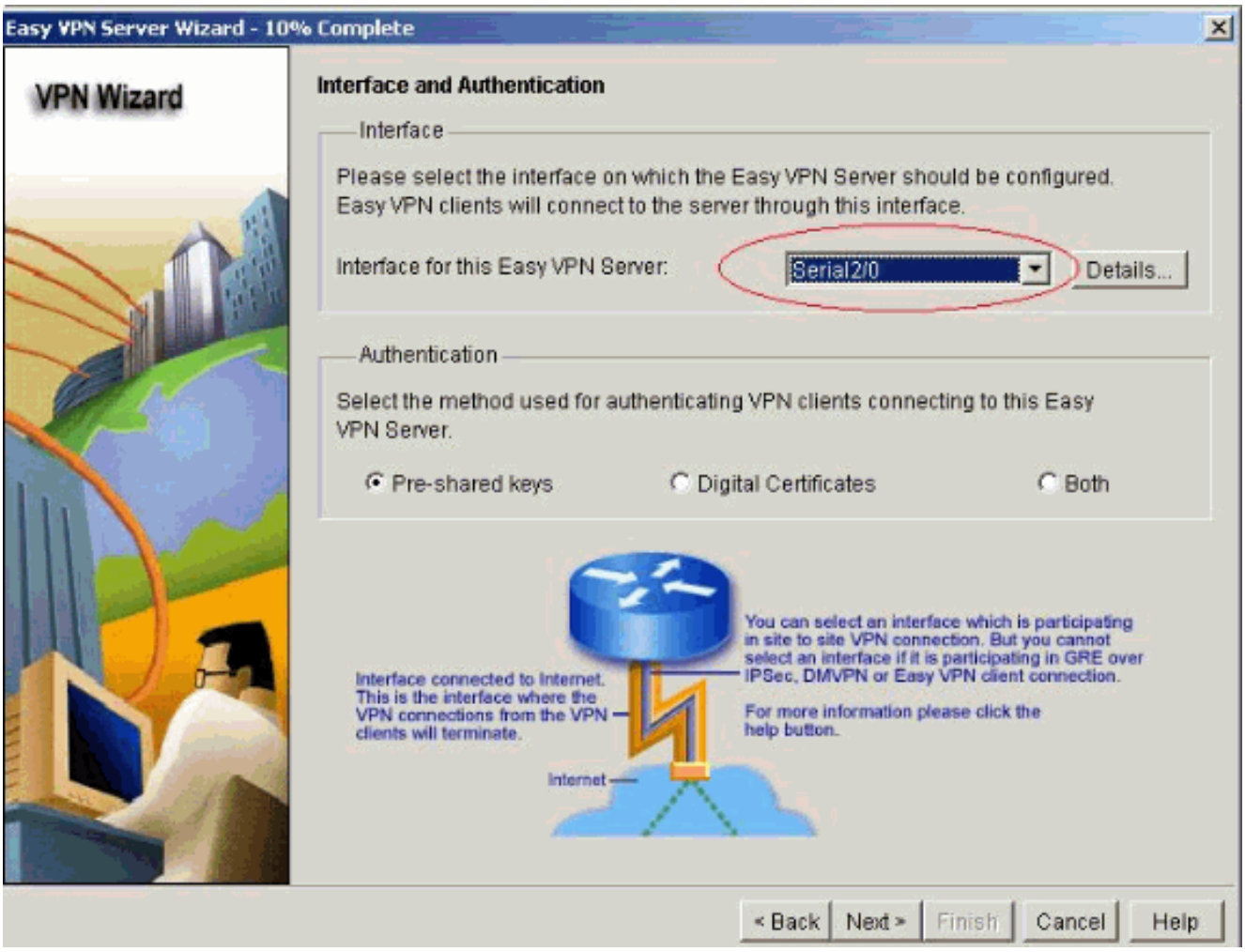
В окне отображается сообщение 'AAA has been successfully enabled on the router' ("AAA включен на маршрутизаторе"). Нажмите **OK**, чтобы начать настройку сервера Easy VPN.



Нажмите **Далее**, чтобы запустить мастер настройки сервера Easy VPN.

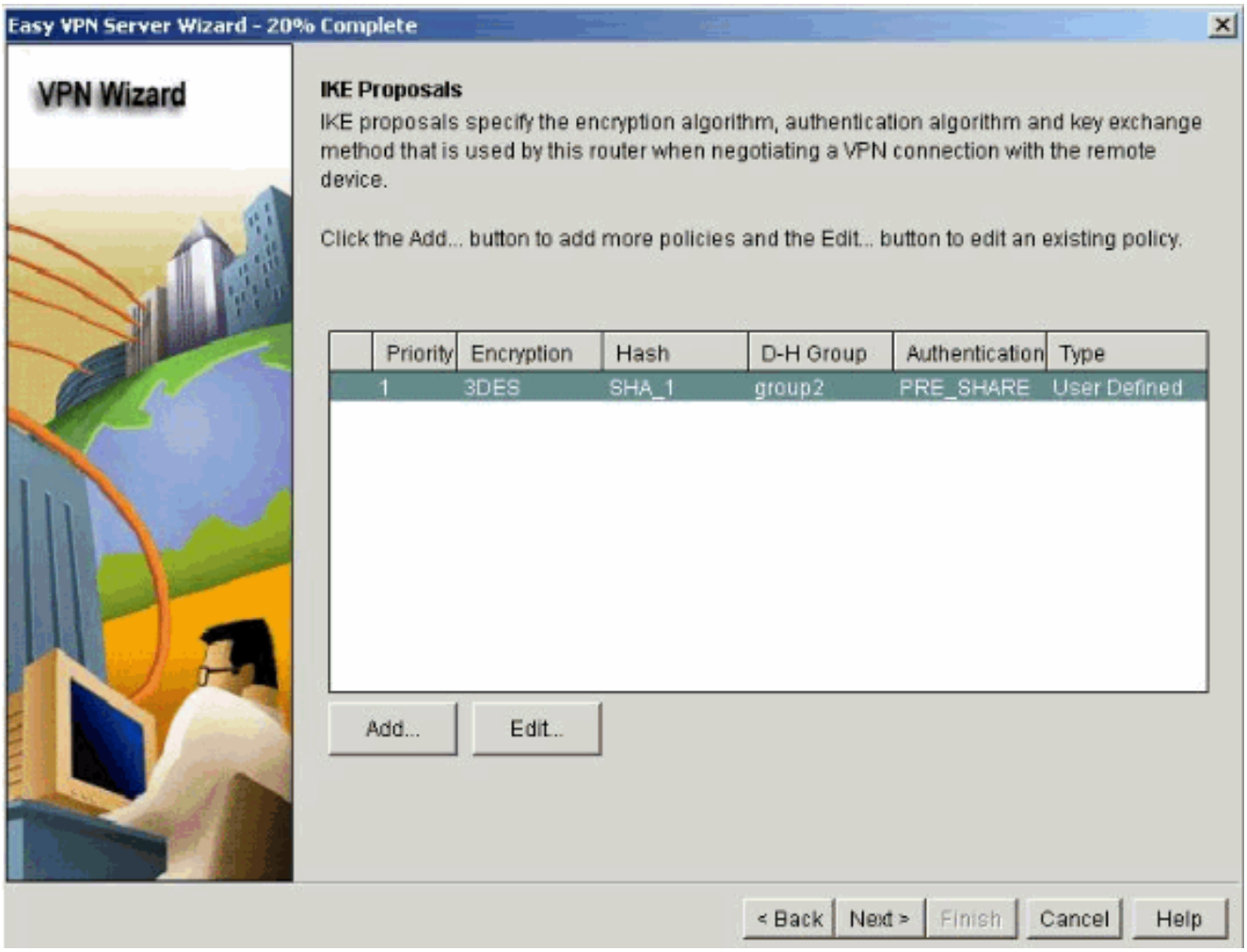


Выберите интерфейс, на котором заканчиваются клиентские подключения, и тип аутентификации.

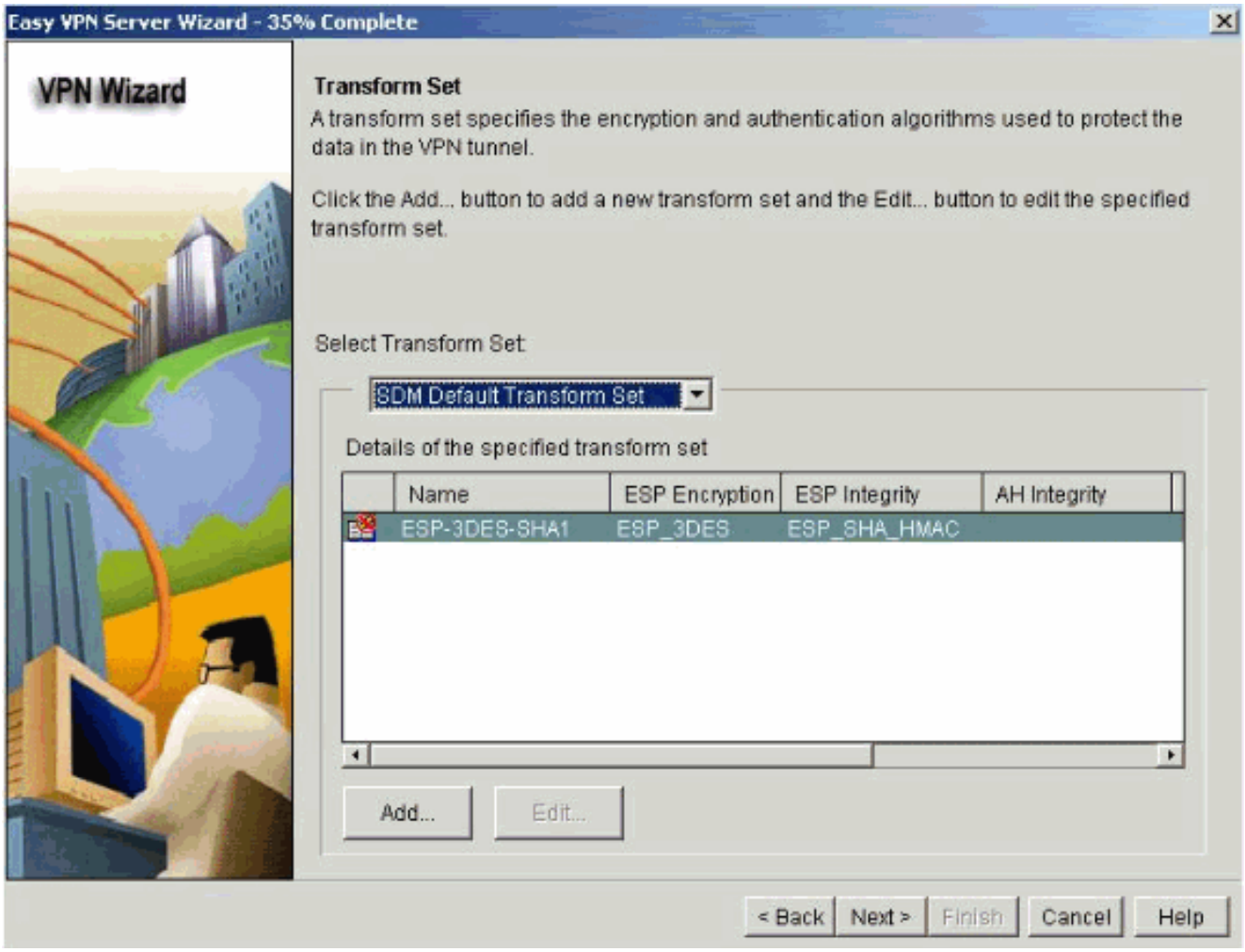


Нажмите **Далее**, чтобы настроить политики IKE, и используйте кнопку **Добавить**, чтобы создать новую политику.

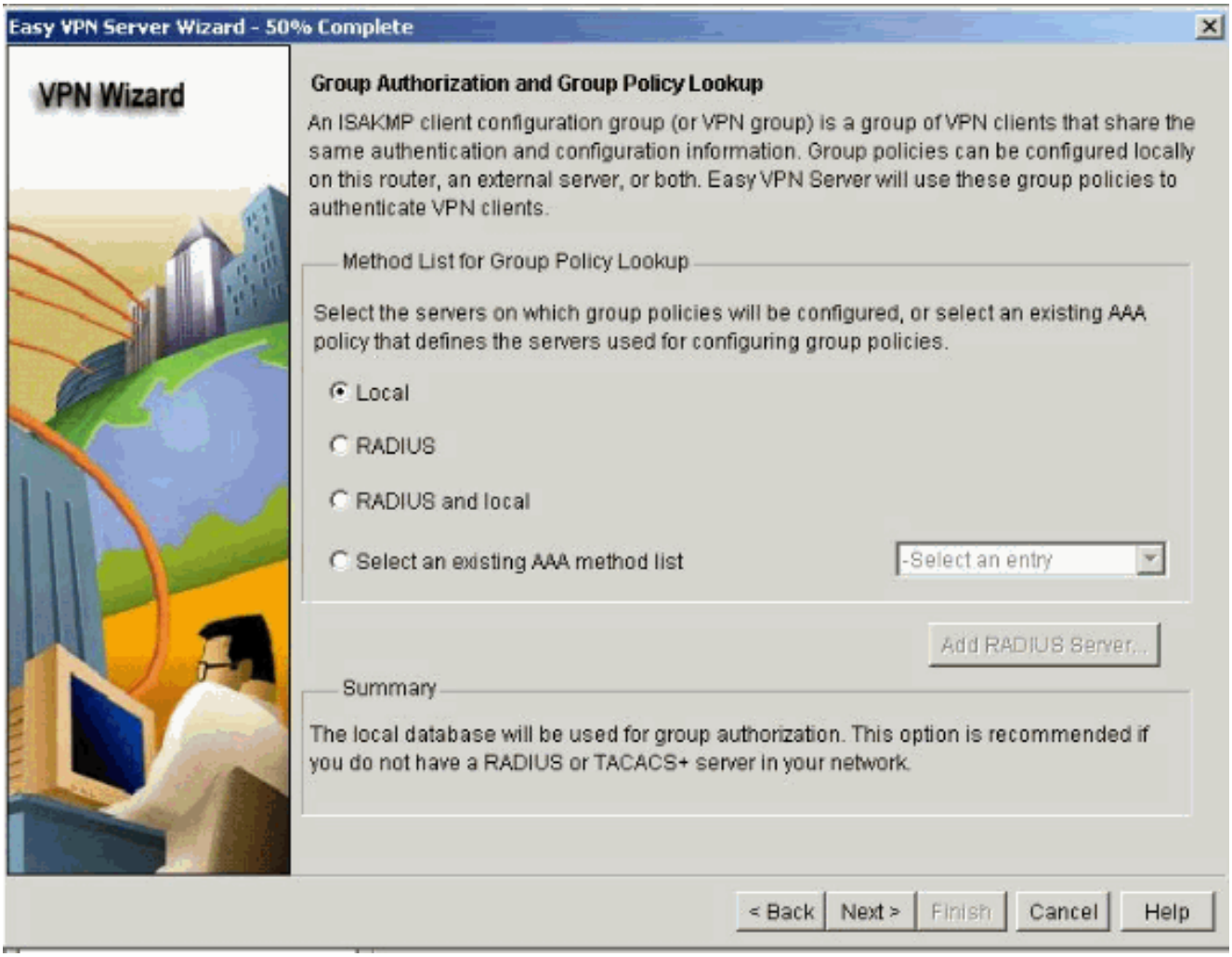
Настройки на обеих сторонах туннеля должны точно совпадать. Клиент Cisco VPN автоматически выбирает правильную конфигурацию для себя. Таким образом, настройка IKE для ПК клиента не требуется.



Нажмите **Далее**, чтобы выбрать набор преобразования по умолчанию и указать алгоритм шифрования и аутентификации. В данном случае используется набор преобразования по умолчанию.

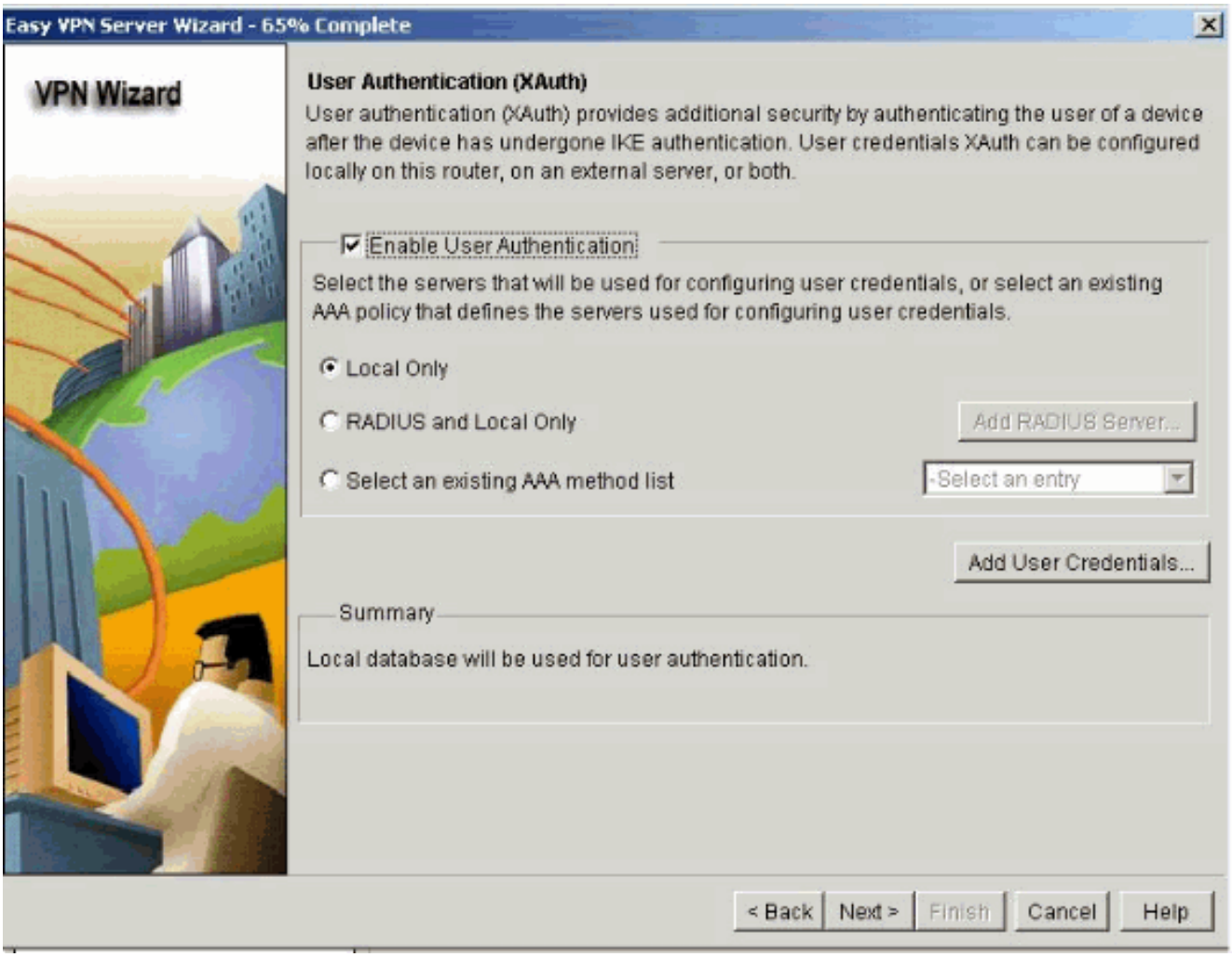


Нажмите **Далее**, чтобы создать новый список сетевых методов аутентификации, авторизации и учета (AAA) для поиска групповой политики или выберите существующий список сетевых методов, используемых для групповой авторизации.

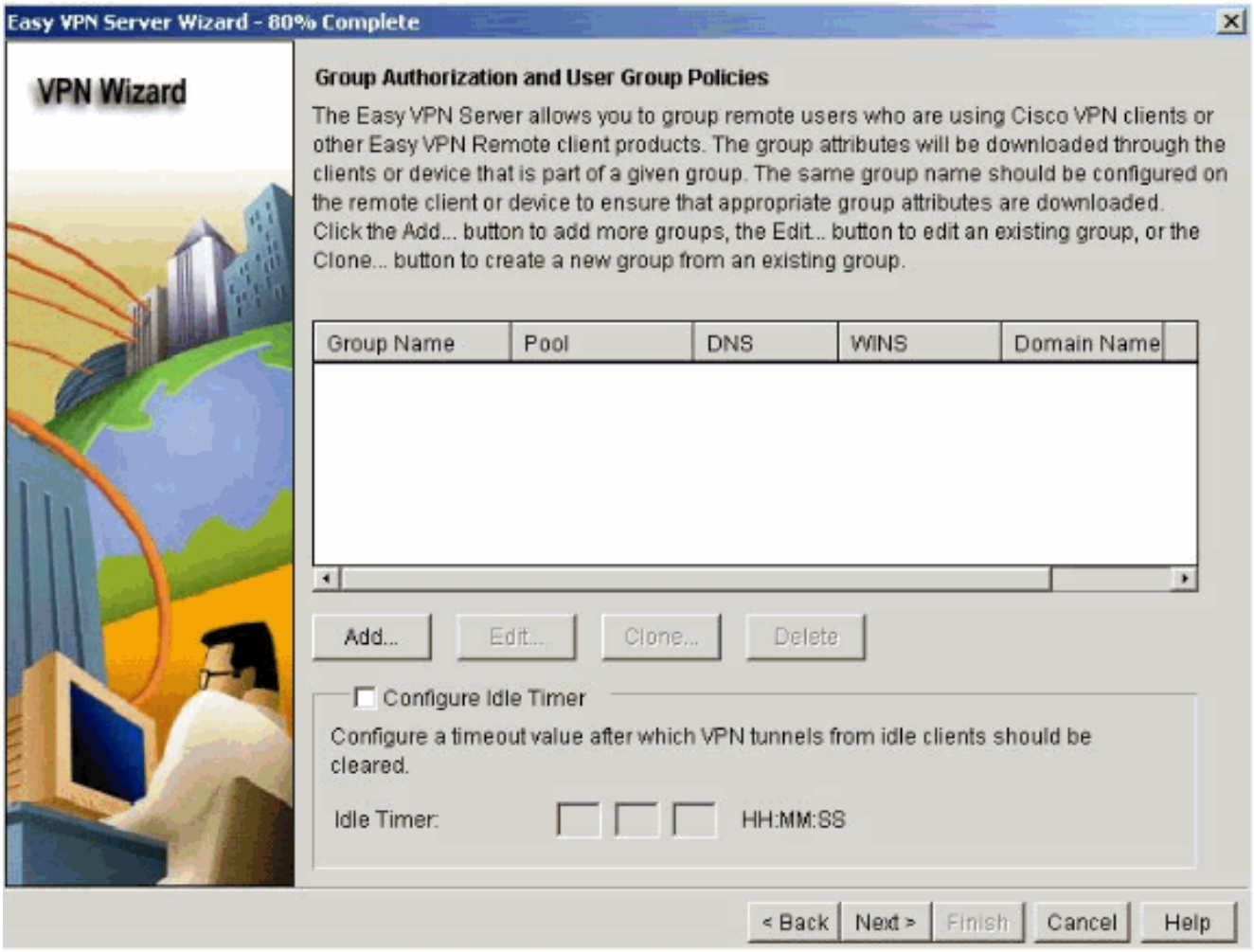


Настройте аутентификацию пользователя на сервере Easy VPN.

Данные аутентификации пользователя можно сохранить на внешнем сервере, например на сервере RADIUS, или в локальной базе данных, либо и там и там. Список методов аутентификации входа AAA используется для определения порядка поиска данных аутентификации пользователя.

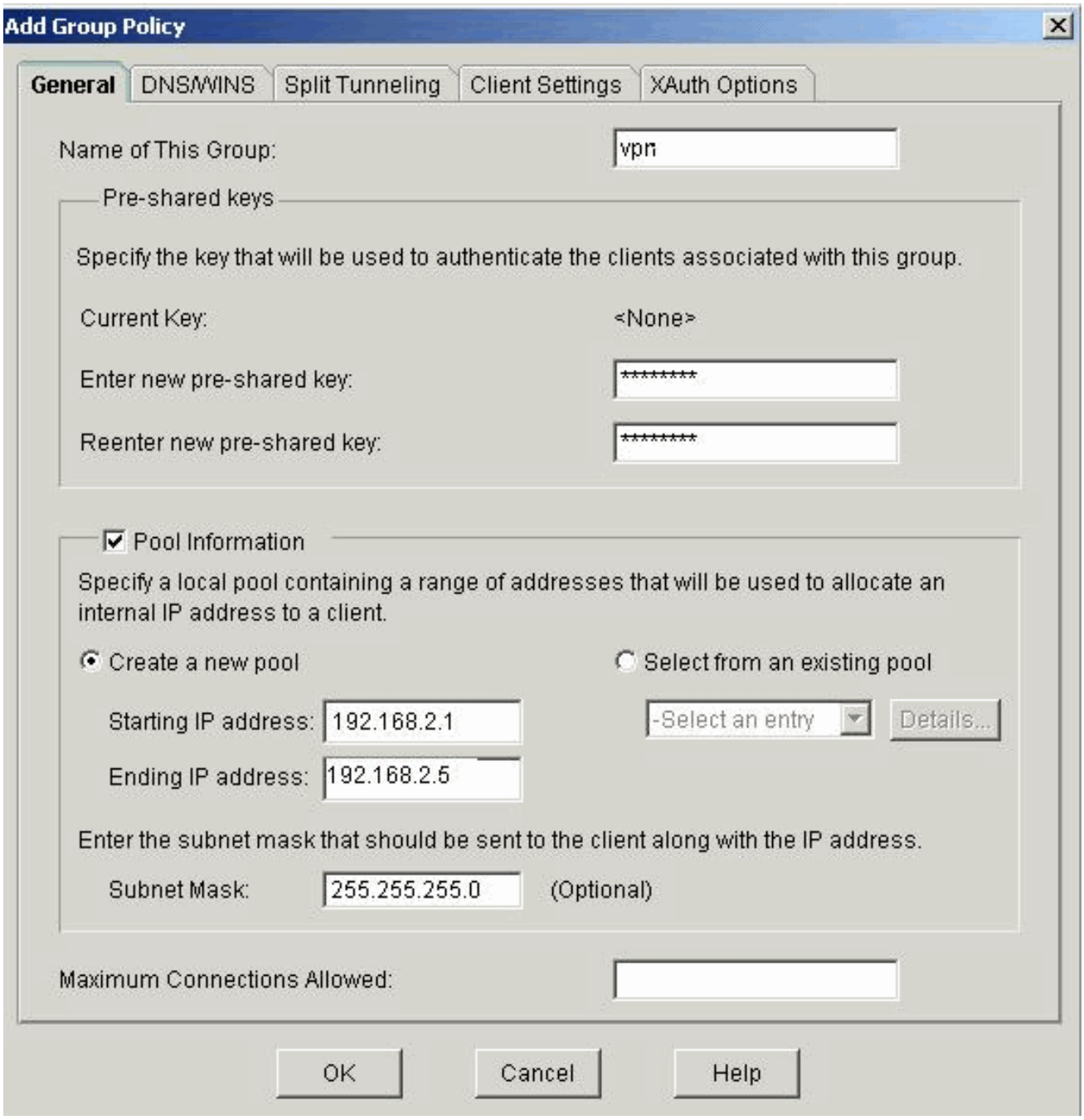


В этом окне можно добавить, изменить, скопировать или удалить групповые политики пользователя в локальной базе данных.

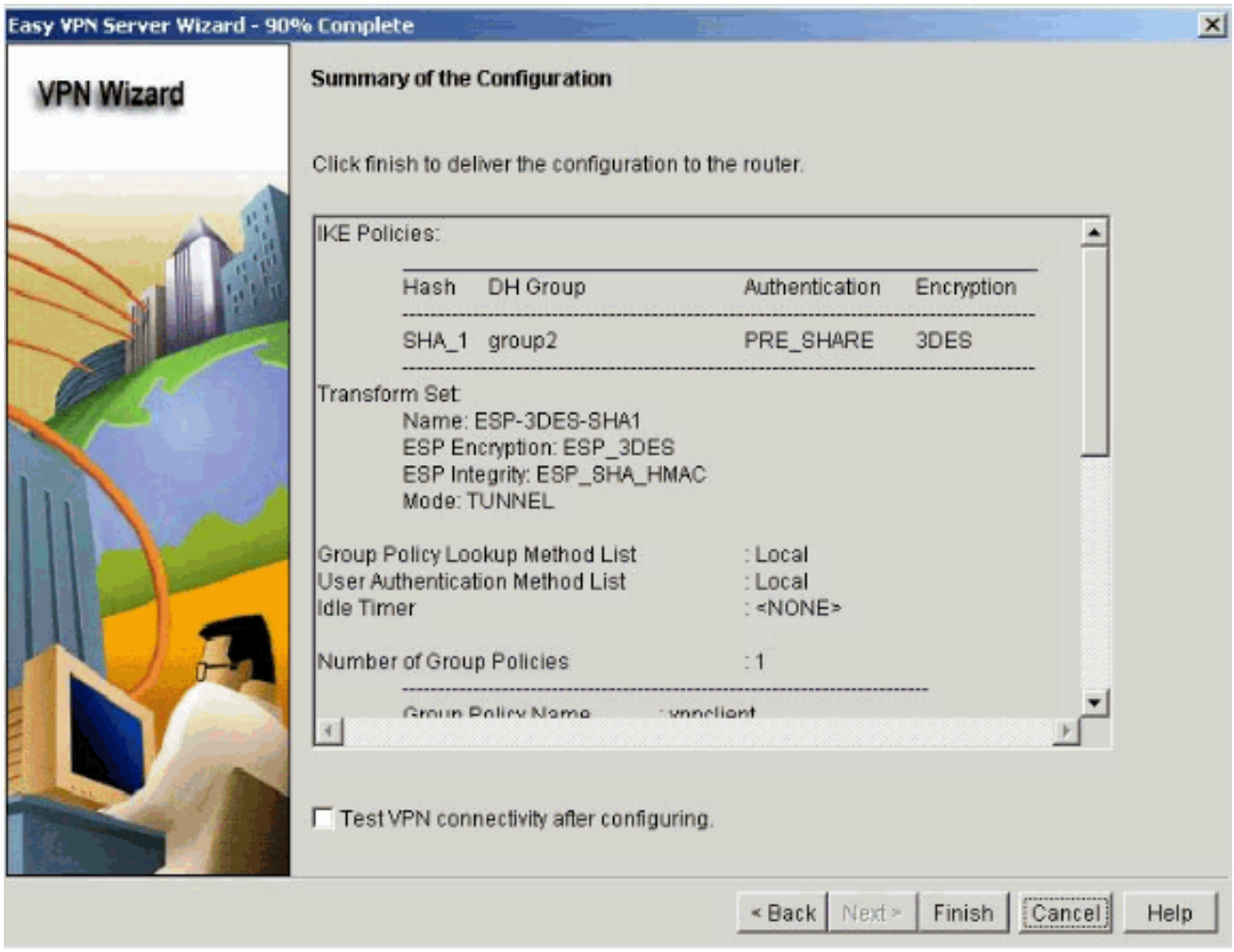


Введите имя группы туннеля. Введите предварительно разделенный ключ, используемый для данных аутентификации.

Создайте новый пул или выберите существующий пул, используемый для размещения IP-адресов клиентов VPN.



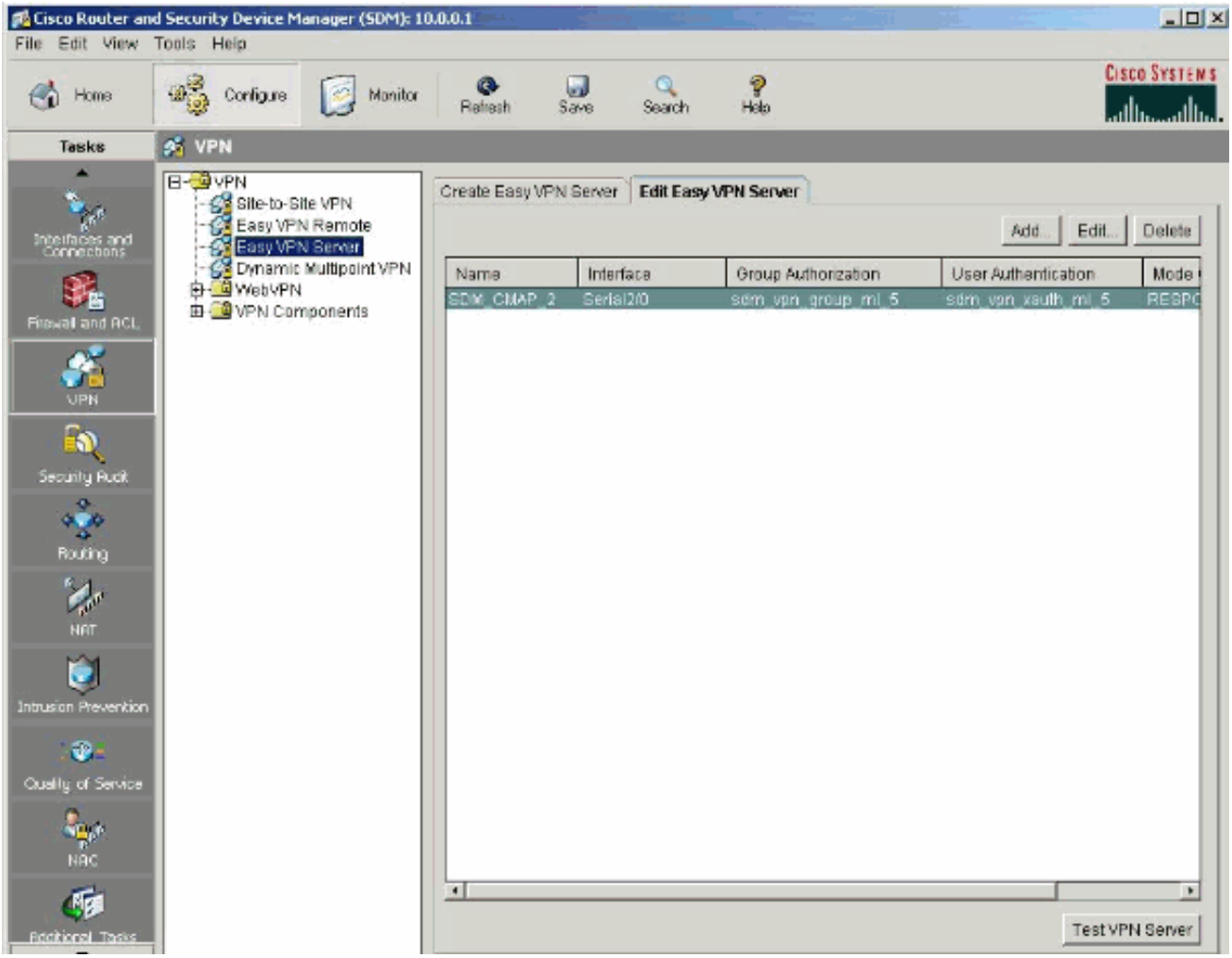
В этом окне показана сводка выполненных действий. Нажмите **Завершить**, если настройка выполнена правильно.



SDM отправляет настройки на маршрутизатор, чтобы обновить действующую конфигурацию. Нажмите **OK** для завершения.

После завершения изменения конфигурации можно изменить и модифицировать при

необходимости.



Настройка маршрутизатора (VPN-сервер)

```
Building configuration...

Current configuration : 3336 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
aaa new-model
!
!--- In order to set AAA authentication at login,
use the aaa authentication login !--- command in
global configuration mode
.
aaa authentication login default local
!--- Here, list name "sdm_vpn_xauth_ml_1" is
specified for !--- the authentication of the
clients. aaa authentication login sdm_vpn_xauth_ml_1
local aaa authorization exec default local aaa
```

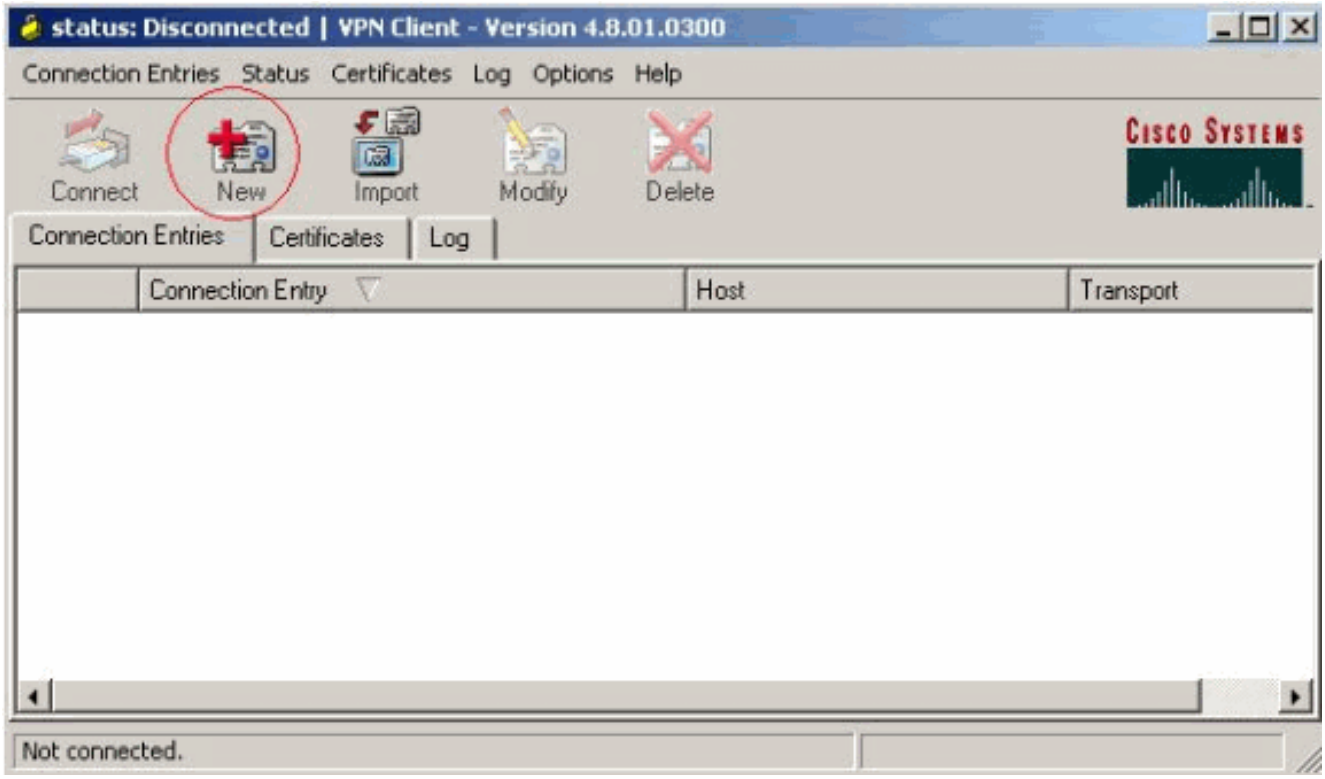
```
authorization network sdm_vpn_group_ml_1 local ! aaa
session-id common ! resource policy ! ! ! ip cef ! !
! ! !--- The RSA certificate generates after the !--
- ip http secure-server command is enabled.

crypto pki trustpoint TP-self-signed-392370502
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-
392370502
 revocation-check none
 rsakeypair TP-self-signed-392370502
!
!
crypto pki certificate chain TP-self-signed-
392370502
 certificate self-signed 01
  3082023C 308201A5 A0030201 02020101 300D0609
2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66
2D536967 6E65642D 43657274
  69666963 6174652D 33393233 37303530 32301E17
0D303530 39323130 30323135
  375A170D 32303031 30313030 30303030 5A303031
2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966
69636174 652D3339 32333730
  35303230 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100
  ED61BD43 0AD90559 2C7D7DB1 BB3147AA 784F3B46
9E63E63C 5CD61976 6BC46596
  DB1AEB44 46644B18 8A890604 489B0447 B4B5C702
98272464 FFFD5511 A4BA79EC
  239BCEA2 823F94EE 438B2E0A 5D90E9ED 8158BC8D
04F67C21 AEE1DB6F 046A0EF3
  4C8798BE 0A171421 3FD5A690 7C735751 E7C58AA3
FB4CCE4F 5930212D 90EB4A33
  02030100 01A36630 64300F06 03551D13 0101FF04
05300301 01FF3011 0603551D
  11040A30 08820652 6F757465 72301F06 03551D23
04183016 8014B278 183F02DF
  5000A124 124FEF08 8B704656 15CD301D 0603551D
0E041604 14B27818 3F02DF50
  00A12412 4FEF088B 70465615 CD300D06 092A8648
86F70D01 01040500 03818100
  C12AB266 0E85DAF6 264AC86F 27761351 E31DF628
BE7792B2 991725ED AAB3BABE
  B1F1C6CA 7E5C0D19 B9793439 E5AECC78 C5ECBE56
871EB4D3 39B60AD1 AB0B97FE
  515B4CC6 81BEE802 DC02BD1B A0D10EE9 0FD79D72
B44C0143 6E39C06B D9178590
  57D02A8F 750DA100 ABEEB1F1 B02A8B1F B746942B
892D1514 B2CC9D58 A28F08E2
  quit
!
!
!
!
!
!
!
!
!
!
!--- Creates a user account with all privileges.
```

```
username sdmsdm privilege 15 password 0 sdmsdm ! !
!--- Creates an isakmp policy 1 with parameters like
!--- 3des encryption, pre-share key authentication,
and DH group 2. crypto isakmp policy 1 encr 3des
authentication pre-share group 2 crypto isakmp
client configuration group vpn !--- Defines the pre-
shared key as sdmsdm. key sdmsdm pool SDM_POOL_1
netmask 255.255.255.0 ! !--- Defines transform set
parameters. crypto ipsec transform-set ESP-3DES-SHA
esp-3des esp-sha-hmac ! crypto dynamic-map
SDM_DYNMAP_1 1 set transform-set ESP-3DES-SHA
reverse-route ! !--- Specifies the crypto map
parameters. crypto map SDM_CMAP_1 client
authentication list sdm_vpn_xauth_ml_1 crypto map
SDM_CMAP_1 isakmp authorization list
sdm_vpn_group_ml_1 crypto map SDM_CMAP_1 client
configuration address respond crypto map SDM_CMAP_1
65535 ipsec-isakmp dynamic SDM_DYNMAP_1 ! ! ! !
interface Ethernet0/0 no ip address shutdown half-
duplex ! interface FastEthernet1/0 ip address
10.77.241.157 255.255.255.192 duplex auto speed auto
! interface Serial2/0 ip address 10.1.1.1
255.255.255.0 no fair-queue !--- Applies the crypto
map SDM_CMAP1 to the interface. crypto map
SDM_CMAP_1 ! interface Serial2/1 no ip address
shutdown ! interface Serial2/2 no ip address
shutdown ! interface Serial2/3 no ip address
shutdown !--- Creates a local pool named SDM_POOL_1
for issuing IP !--- addresses to clients. ip local
pool SDM_POOL_1 192.168.2.1 192.168.2.5 !---
Commands for enabling http and https required to
launch SDM. ip http server ip http secure-server ! !
! ! ! control-plane ! ! ! ! ! ! ! ! ! line con 0
line aux 0 line vty 0 4 password cisco ! ! end
```

Проверка

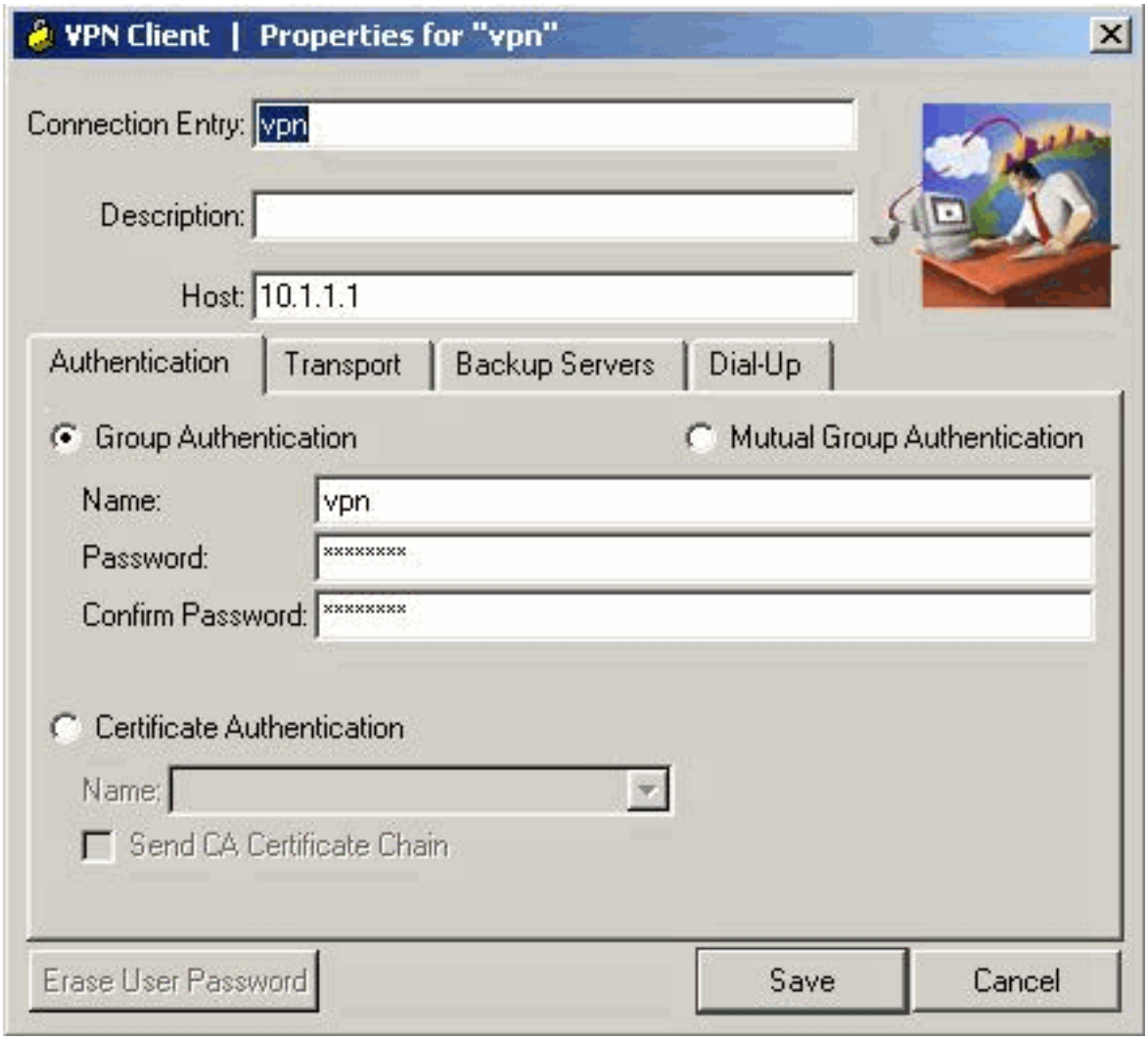
Попытайтесь подключиться к маршрутизатору Cisco с помощью Cisco VPN Client, чтобы убедиться, что маршрутизатор Cisco настроен правильно.

Выберите **Connection Entries > New**.

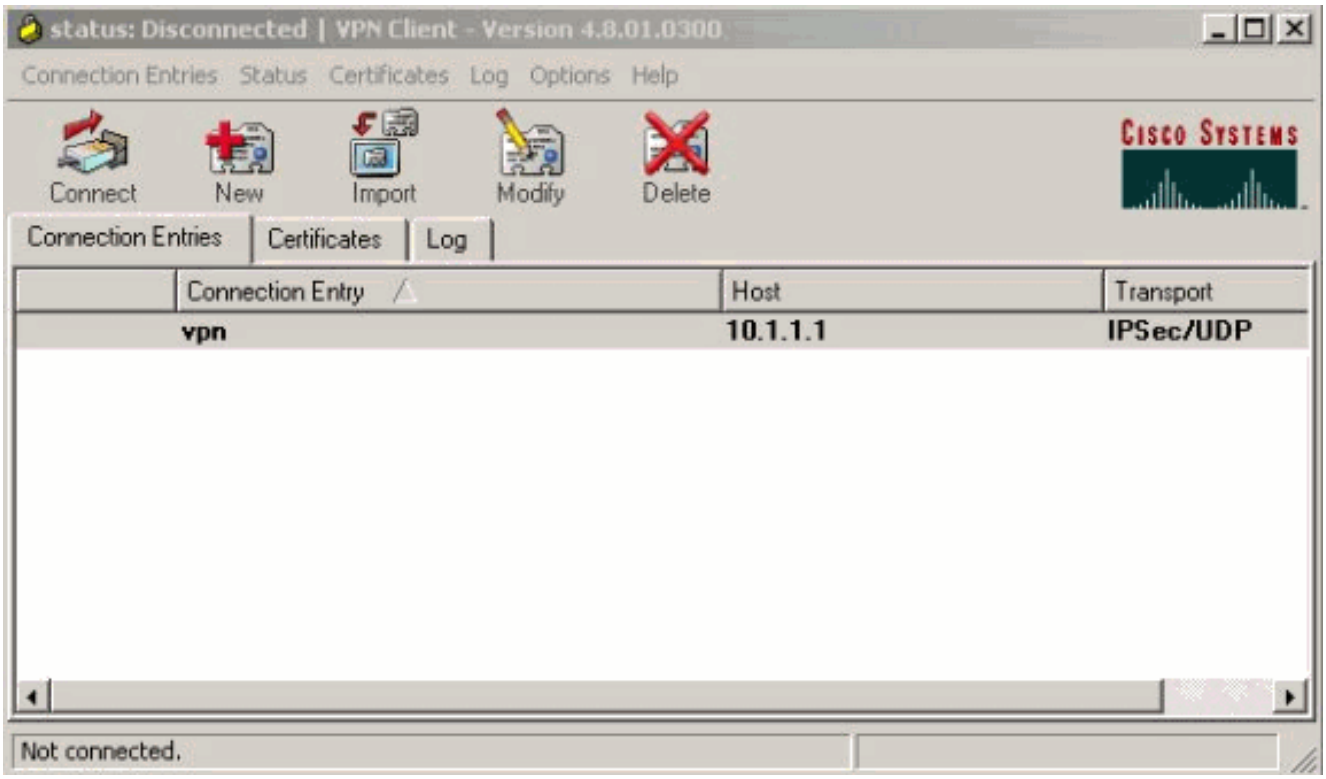


Введите данные нового подключения.

Поле Host должно содержать IP-адрес или имя узла конечной точки туннеля сервера Easy VPN (маршрутизатора Cisco). Данные групповой аутентификации должны соответствовать данным, использованным на шаге 9. После завершения ввода нажмите **Сохранить**.



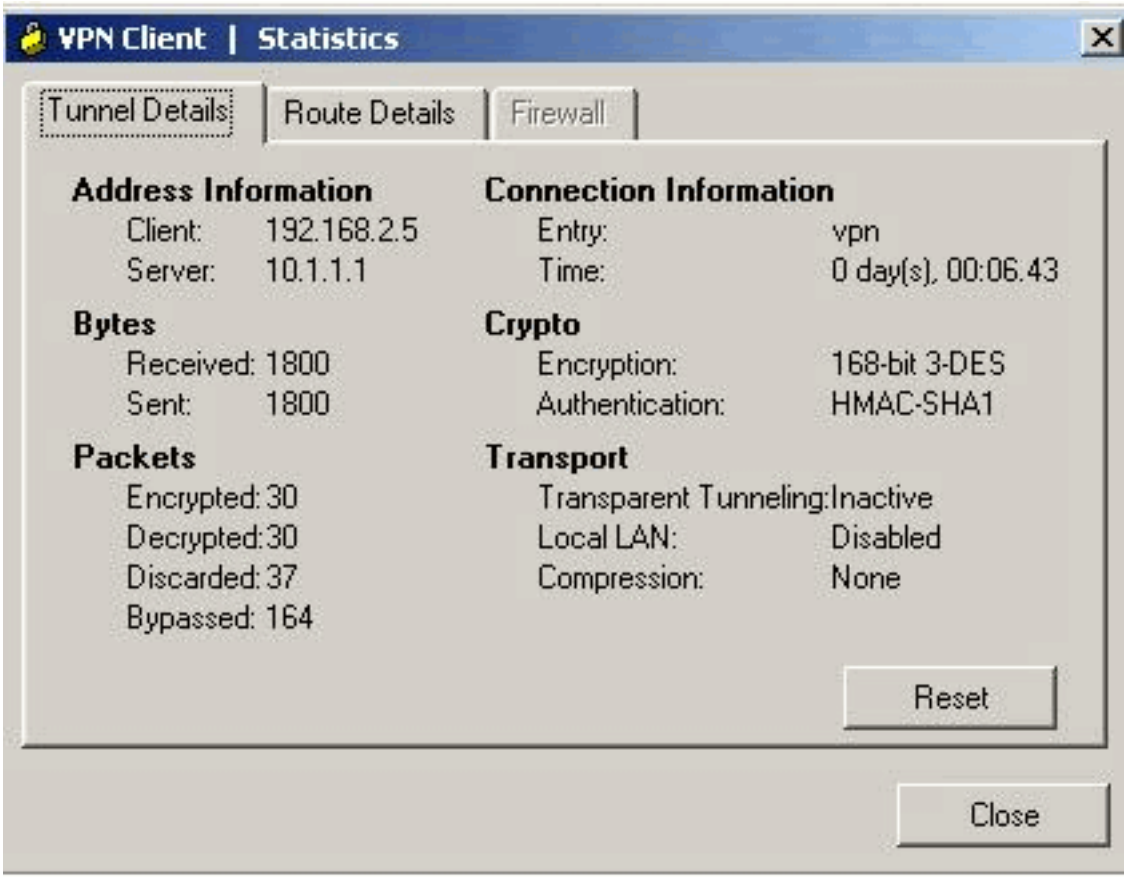
Выберите только что созданное подключение и нажмите **Соединить**.



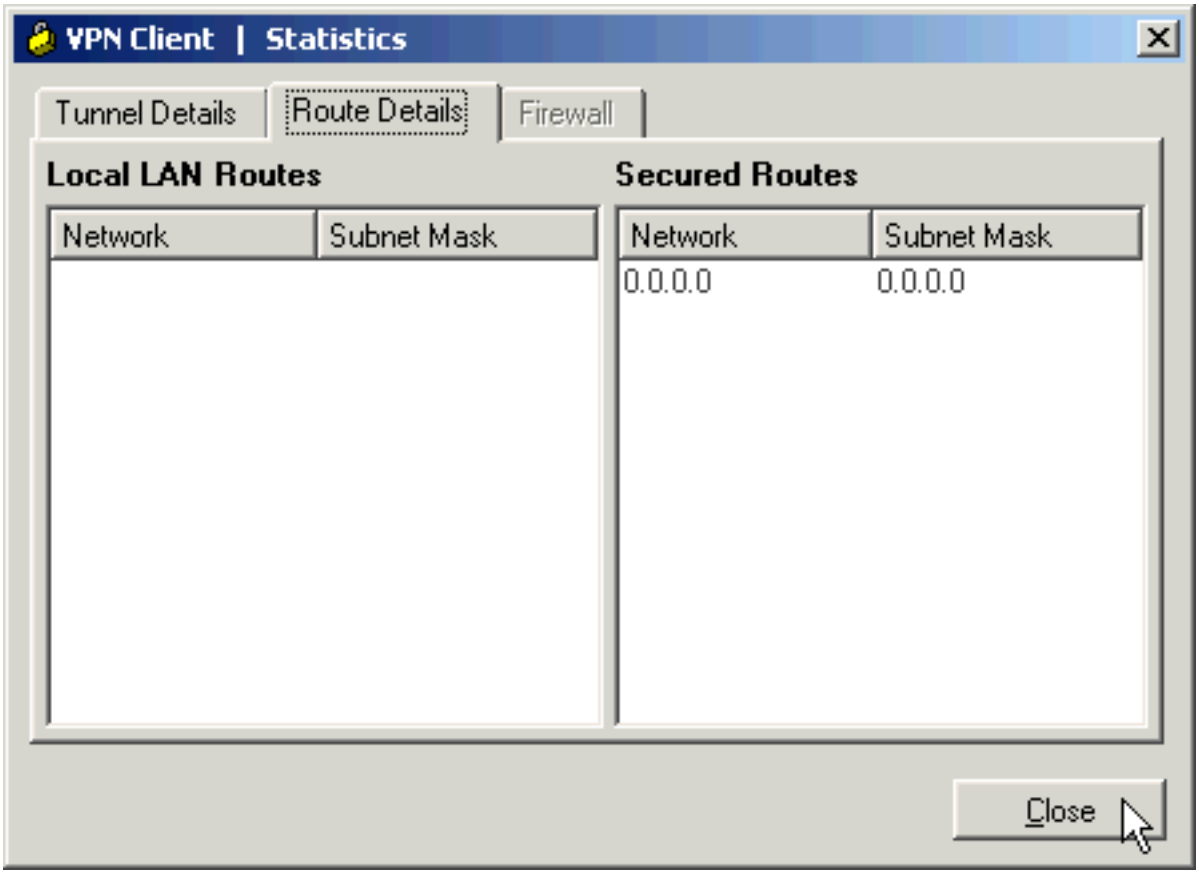
Введите имя пользователя и пароль для расширенной аутентификации (Xauth). Эти данные определяются параметрами Xauth на шаге 7.

После успешного установления соединения выберите пункт **Статистика** в меню Status ("Состояние"), чтобы проверить данные туннеля.

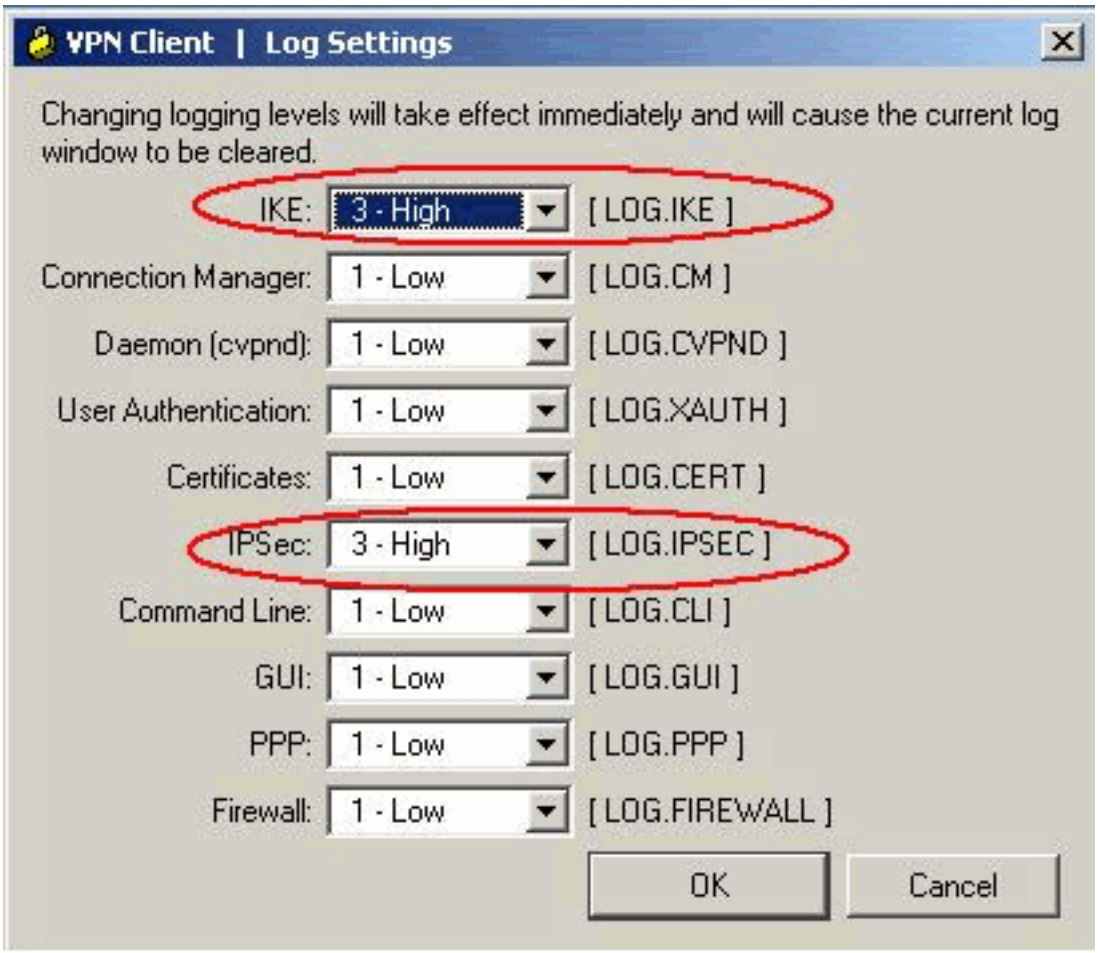
В этом окне показана информация о трафике и шифровании:



В этом окне показана информация о раздельном туннелировании, если оно настроено:



Выберите **Log > Log Settings**, чтобы включить уровни журнала в Cisco VPN Client.



Выберите **Log > Log Windows**, чтобы просмотреть записи журнала в Cisco VPN Client.

Дополнительные сведения

- Загрузка и установка программы Cisco Router and Security Device Manager
- Страница поддержки VPN Client Cisco
- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация