ASA 8. X: Маршрутизация трафика VPN SSL через туннелируемый пример конфигурации шлюза по умолчанию

Содержание

Введение

В этом документе описывается способ настройки устройства адаптивной защиты (ASA) для маршрутизации трафика VPN SSL через туннелируемый шлюз по умолчанию (TDG). Когда вы создаете маршрут по умолчанию с туннелируемой опцией, всем трафиком из туннеля, завершающегося на ASA, который не может маршрутизироваться с помощью изученный, или статические маршруты передается этому маршруту. Для трафика, появляющегося из туннеля, этот маршрут отвергает любые другие настроенные или изученные маршруты по умолчанию.

Предварительные условия

Требования

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

- ASA, который работает на версии 8. x
- Cisco SSL VPN Client (SVC) 1. x**Примечание:** Загрузите пакет VPN-клиента SSL (SVC) (sslclient-win*.pkg) от Загрузки Программного обеспечения Cisco (только зарегистрированные клиенты). Скопируйте SVC к флэш-памяти на ASA. SVC должен быть загружен к компьютерам удаленного пользователя для установления VPN-

подключения на базе SSL с ASA.

Используемые компоненты

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

- ASA серии 5500 Cisco, который работает под управлением ПО версии 8. x
- Версия Cisco SSL VPN Client для Windows 1.1.4.179
- ПК, который выполняет Windows 2000 Professional или Windows XP
- Cisco Adaptive Security Device Manager (ASDM) версия 6.1 (5)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

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

Общие сведения

Клиент SSL VPN (SVC) является технологией туннелирования VPN, которая приносит удаленным пользователям пользу VPN-клиента IPSec без потребности в администраторах сети, чтобы установить и настроить VPN-клиентов IPSec на удаленных компьютерах. SVC использует шифрование SSL, которое уже присутствует на удаленном компьютере, а также входе в систему WebVPN и аутентификации Устройства безопасности.

В текущем сценарии существует VPN-клиент SSL (SVC), соединяющийся с внутренними ресурсами позади ASA через VPN-туннель SSL. Разделение туннеля не включено. Когда VPN-клиент SSL (SVC) будет связан с ASA, все данные будут туннелированы. Помимо доступа к внутренним ресурсам, основной критерий должен направить этот туннельный трафик через По умолчанию туннелировал шлюз (DTG).

Можно определить отдельный маршрут по умолчанию для туннельного трафика наряду со стандартным маршрутом по умолчанию. Незашифрованный трафик, полученный ASA, для которого нет никаких помех или полученного маршрута, маршрутизируется через стандартный маршрут по умолчанию. Зашифрованный поток данных, полученный ASA, для которого нет никаких помех или полученного маршрута, передадут к DTG, определенному через туннелируемый маршрут по умолчанию.

Для определения туннелируемого маршрута по умолчанию используйте эту команду:

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

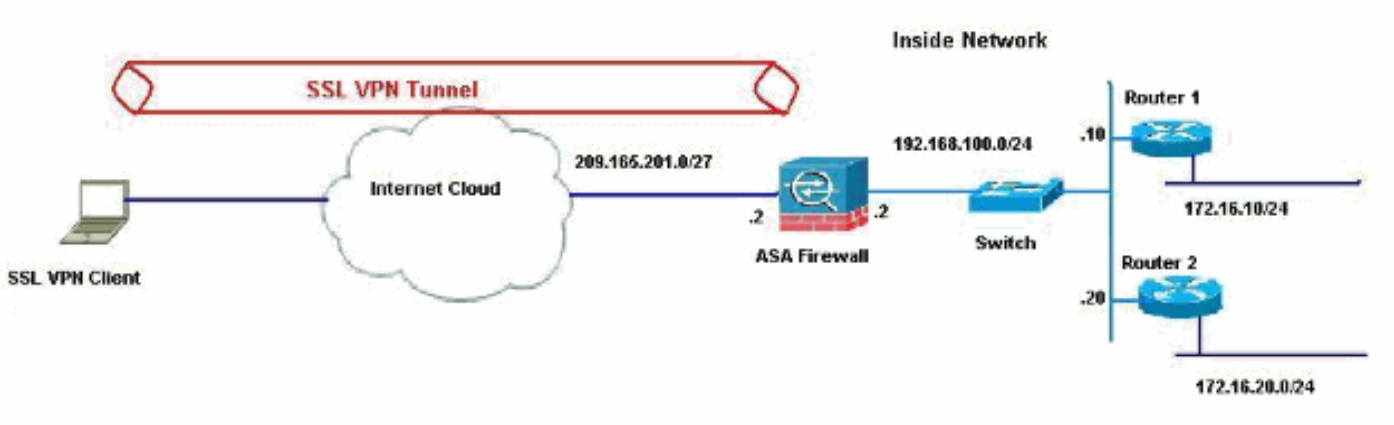
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



В данном примере VPN-клиент SSL (SVC) обращается к внутренней сети ASA через туннель. Трафик, предназначенный для назначений кроме внутренней сети, также туннелирован, поскольку нет никакого разделения туннеля, настроенного, и не маршрутизируется через TDG (192.168.100.20).

После того, как пакеты маршрутизируются к TDG, который является маршрутизатором 2 в этом случае, это выполняет переадресацию для маршрутизации тех пакетов вперед к Интернету. Для получения дополнительной информации о настройке маршрутизатора как интернет-шлюз обратитесь к тому, Как Настроить маршрутизатор Cisco Позади Кабельного модема стороннего производителя.

Конфигурация ASA с помощью ASDM 6.1 (5)

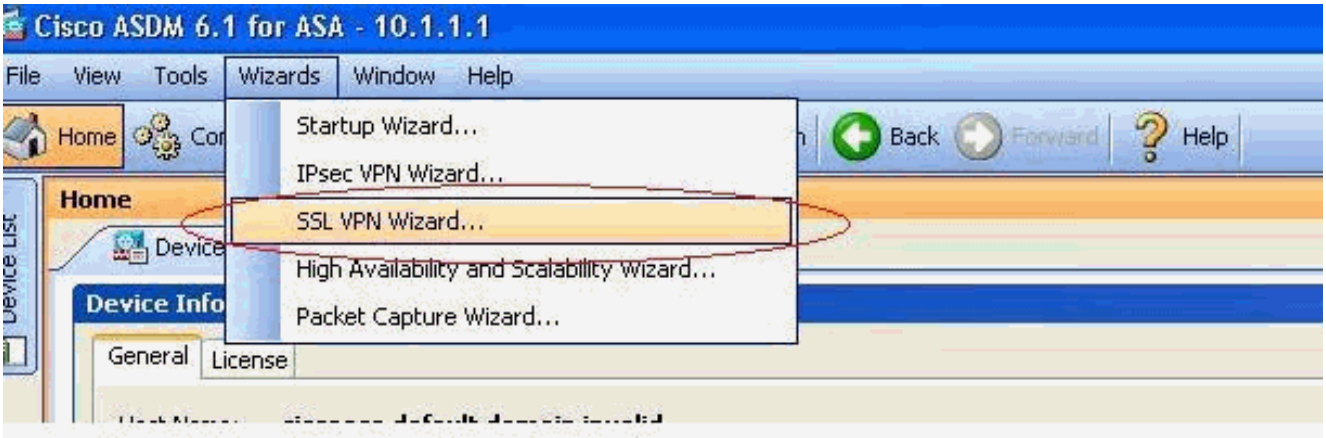
Этот документ принимает базовые конфигурации, такие как конфигурация интерфейса, завершен и работает должным образом.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM для получения информации о том, как позволить ASA быть настроенным ASDM.

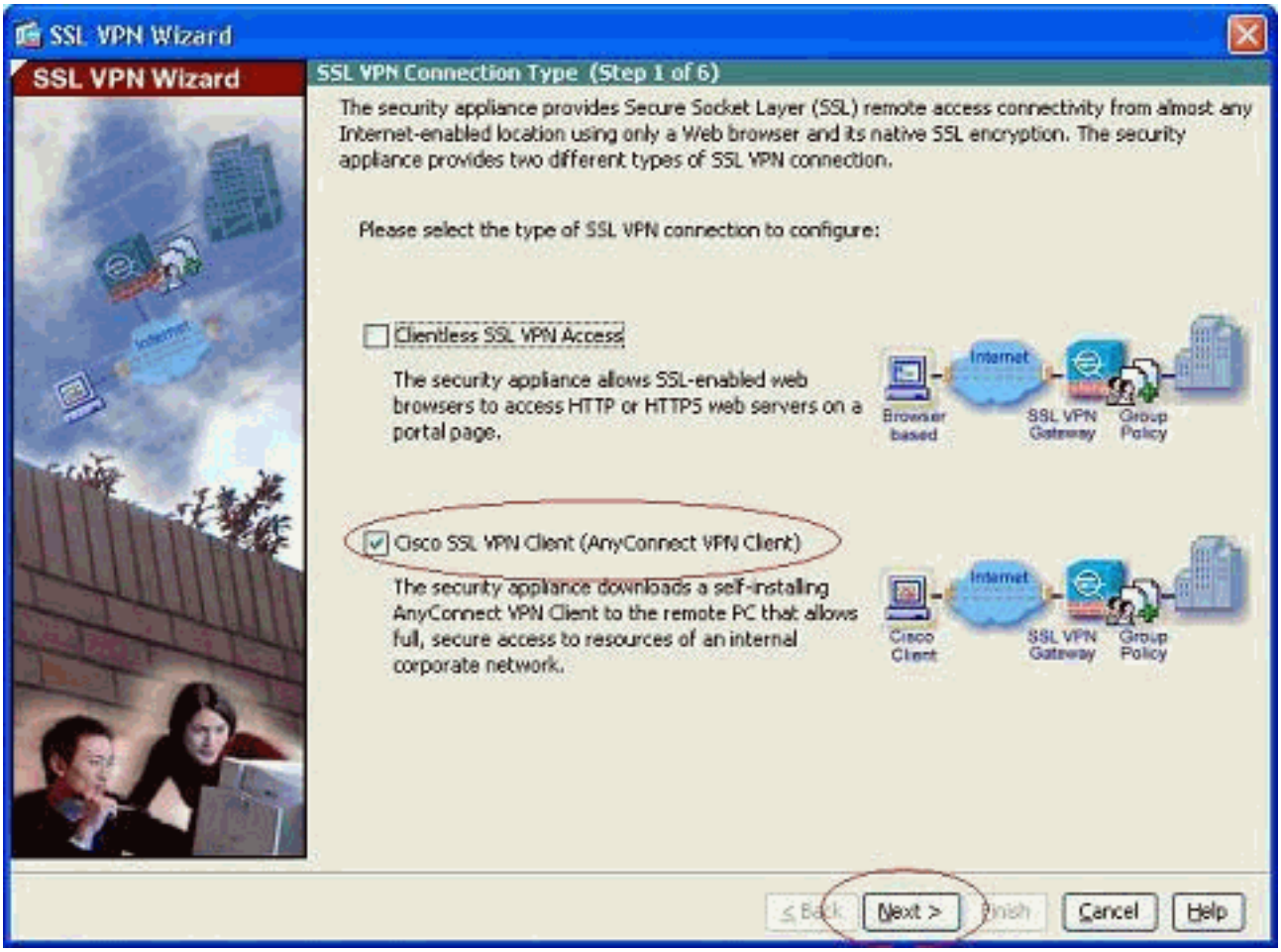
Примечание: Нельзя включать WebVPN и ASDM на одном и том же интерфейсе ASA, если не изменены номера портов. Для получения дополнительных сведений обратитесь к документу Включение ASDM и WebVPN на одном и том же интерфейсе ASA.

Выполните эти шаги для настройки VPN SSL при помощи Мастера VPN SSL.

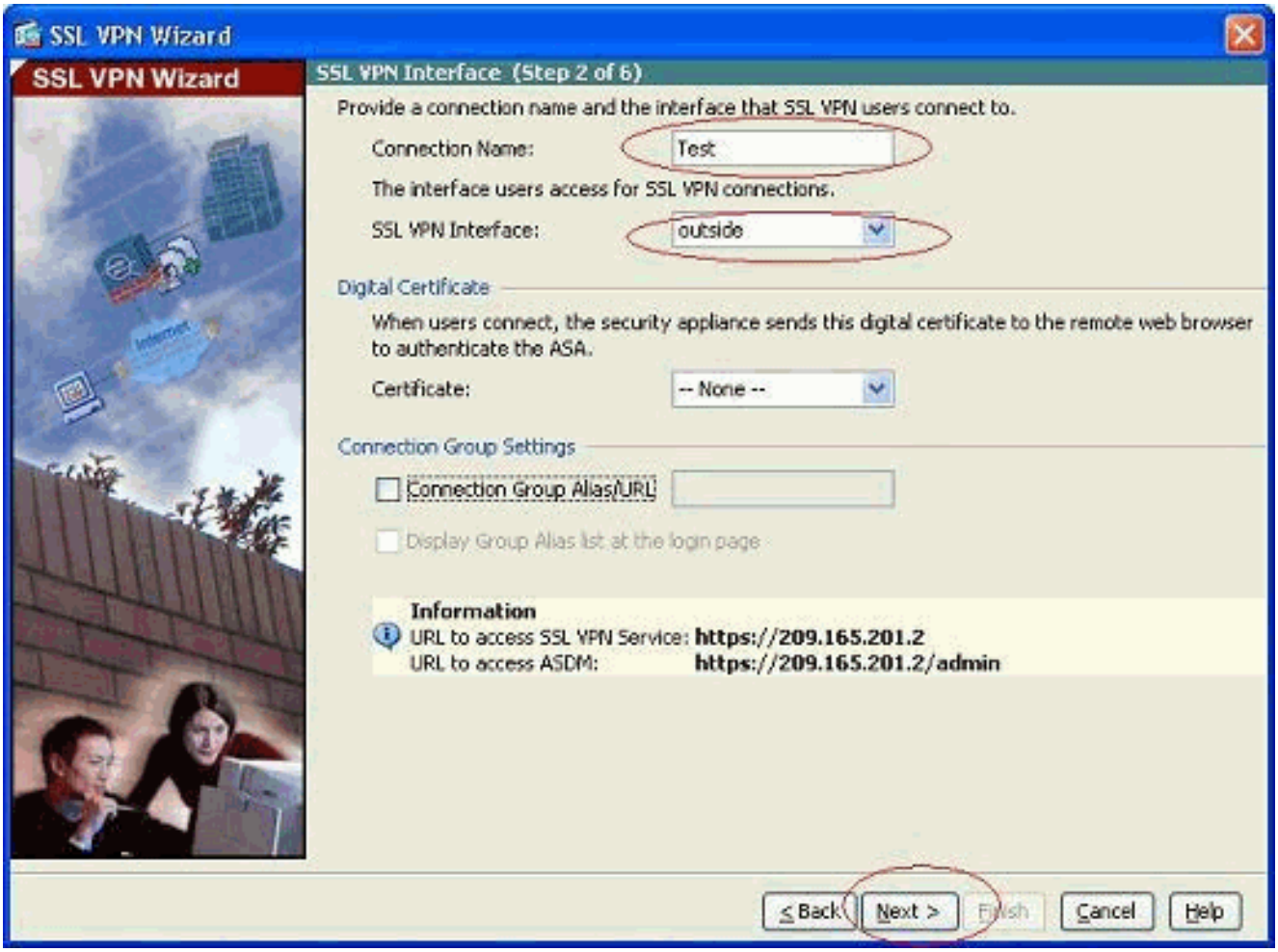
1. Из меню Wizards выберите **SSL VPN Wizard**.



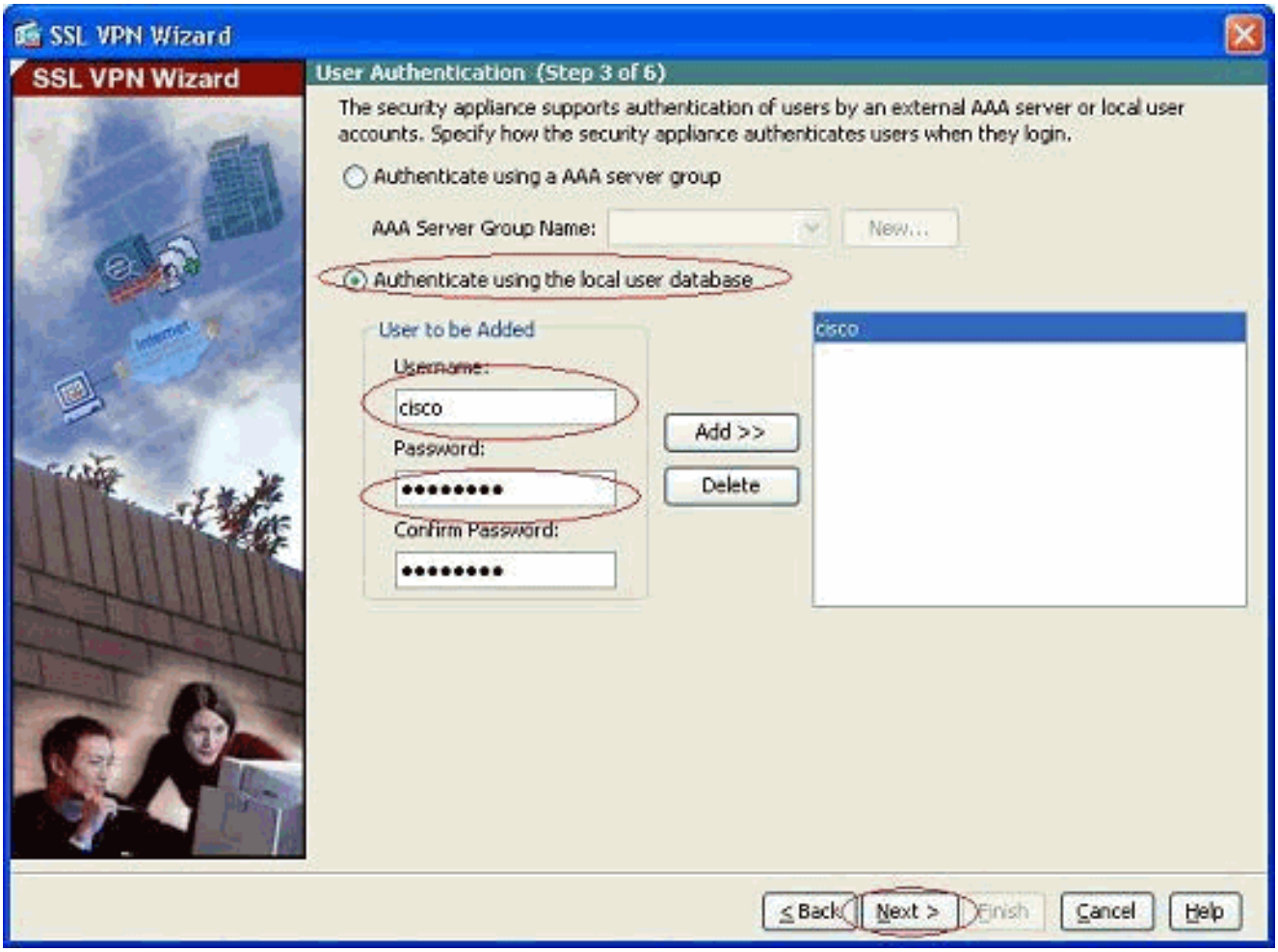
2. Нажмите флажок **Cisco SSL VPN Client** и нажмите **Next**.



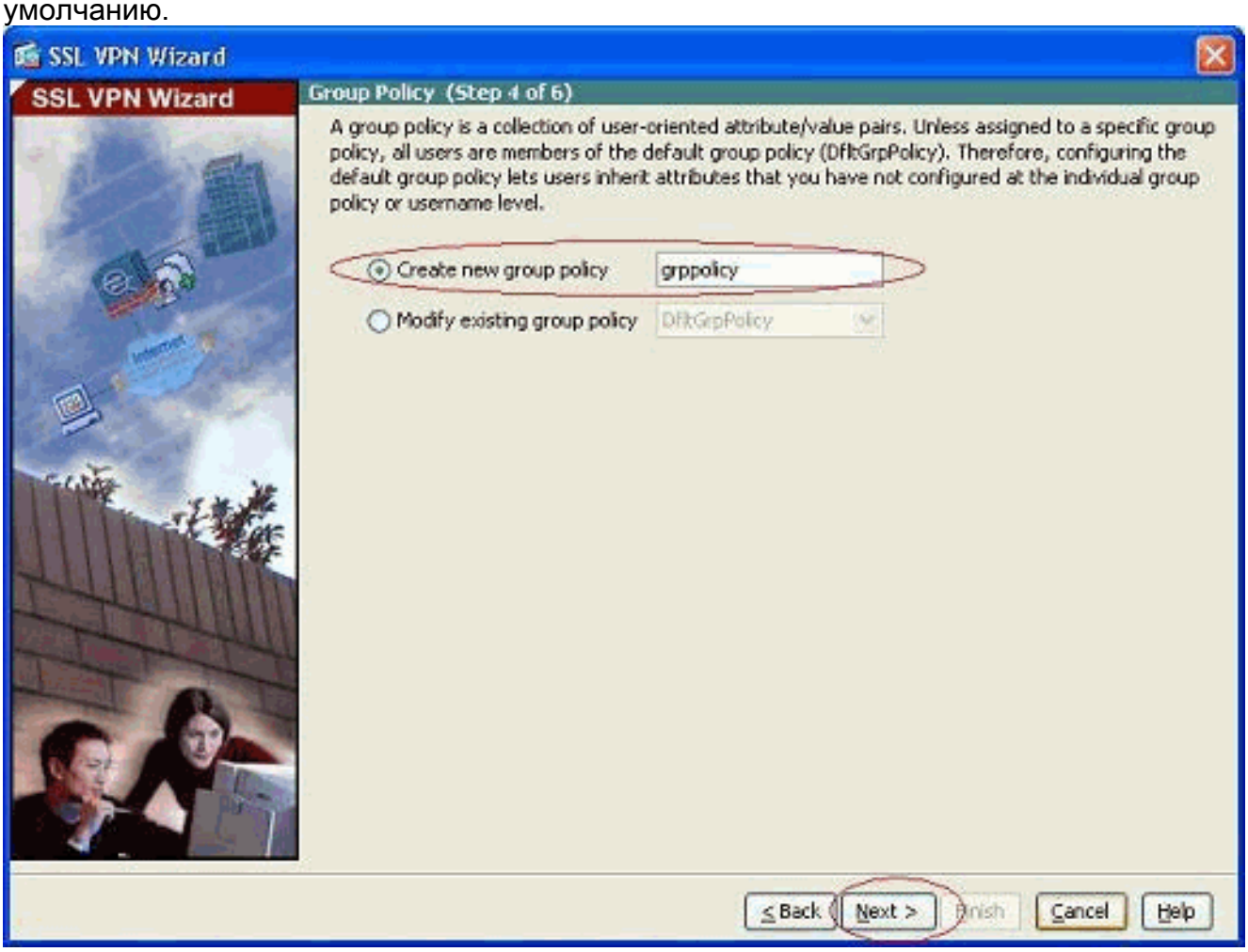
3. Введите имя для соединения в поле Connection Name, и затем выберите интерфейс, который используется пользователем для доступа к VPN SSL от выпадающего списка Интерфейса VPN
SSL.



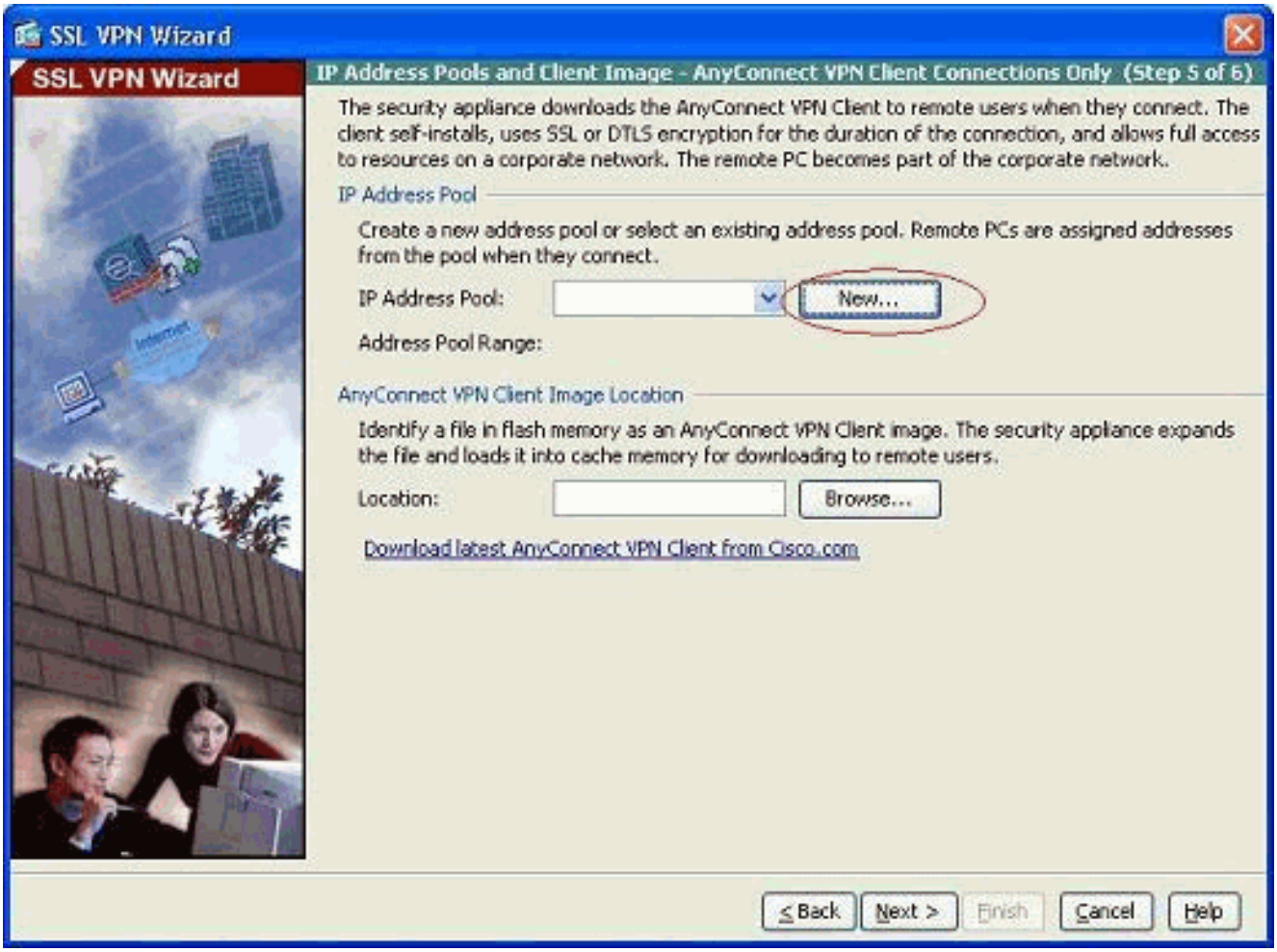
4. **Нажмите кнопку Next.**
5. Выберите режим аутентификации и нажмите **Next**. (Данный пример использует локальную проверку
подлинности.)



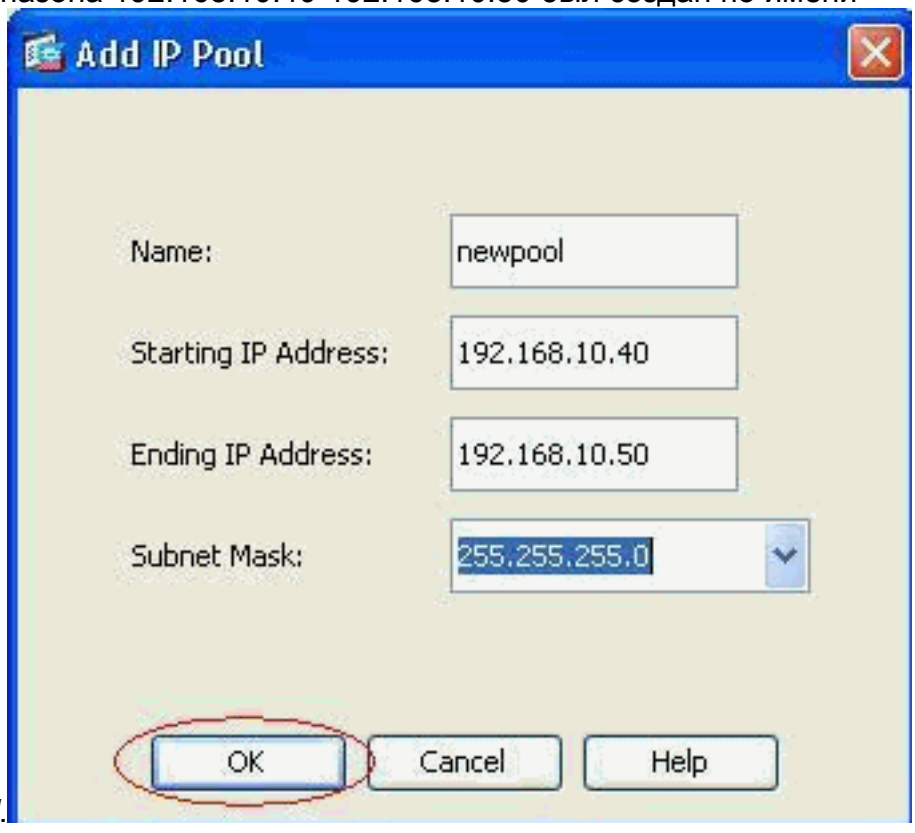
6. Создайте новую групповую политику кроме существующей политики группы по умолчанию.



7. Создайте новый пул адресов, которые будут назначены на PC VPN-клиента SSL (SVC), как только они
связаны.

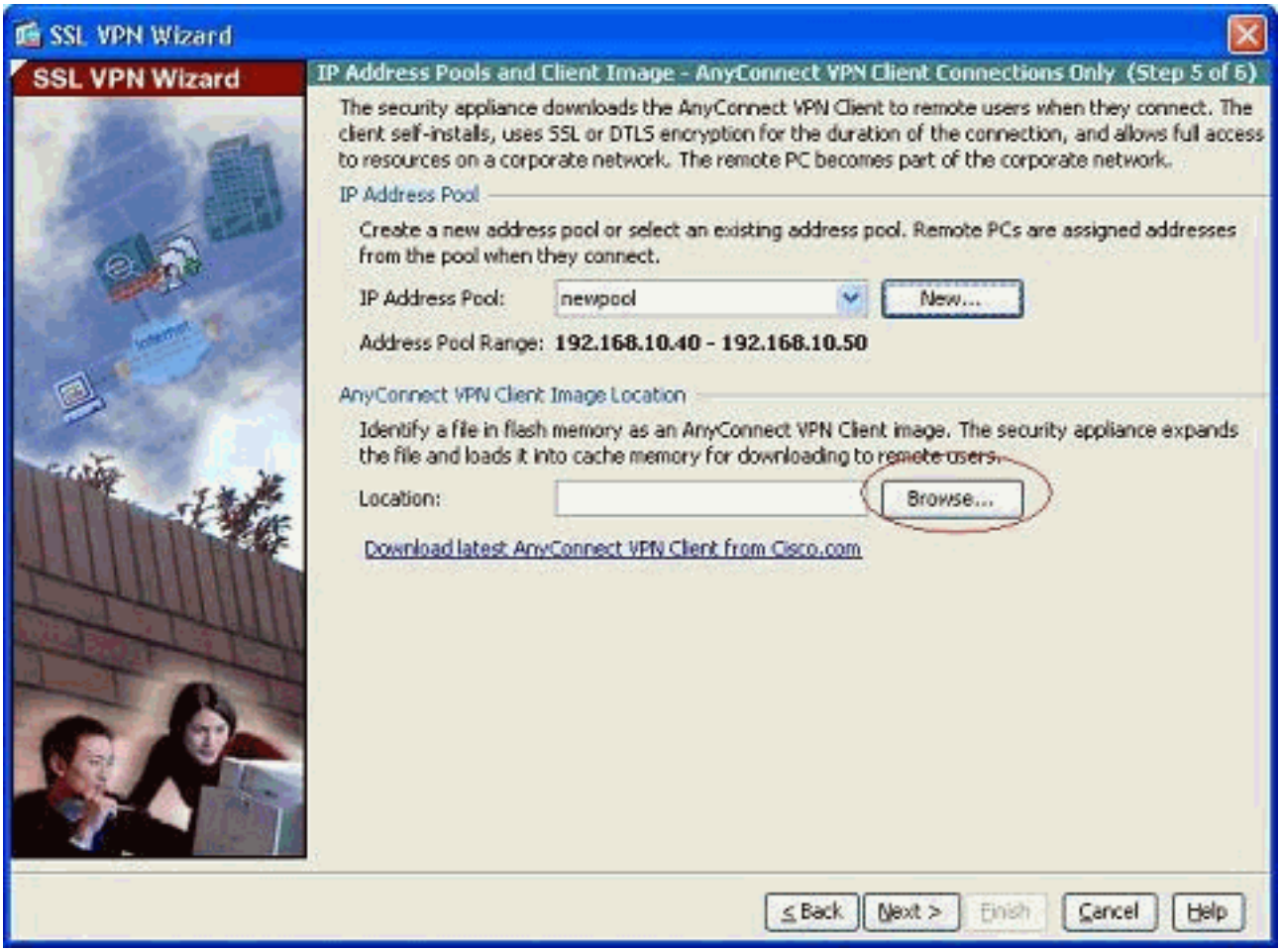


Пул диапазона 192.168.10.40-192.168.10.50 был создан по имени
newpool.

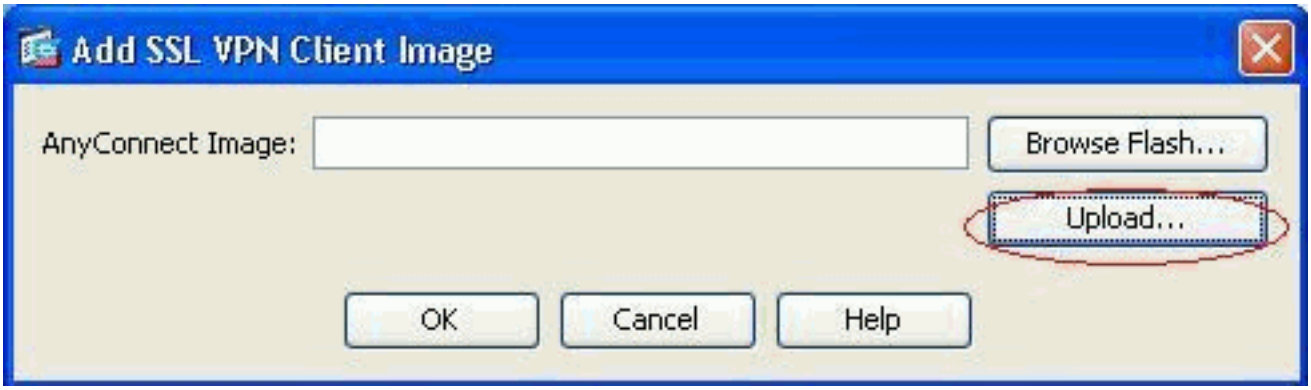


8. Нажмите **Browse**, чтобы выбрать и загрузить образ VPN-клиента SSL (SVC) к флэш-

памяти
ASA.

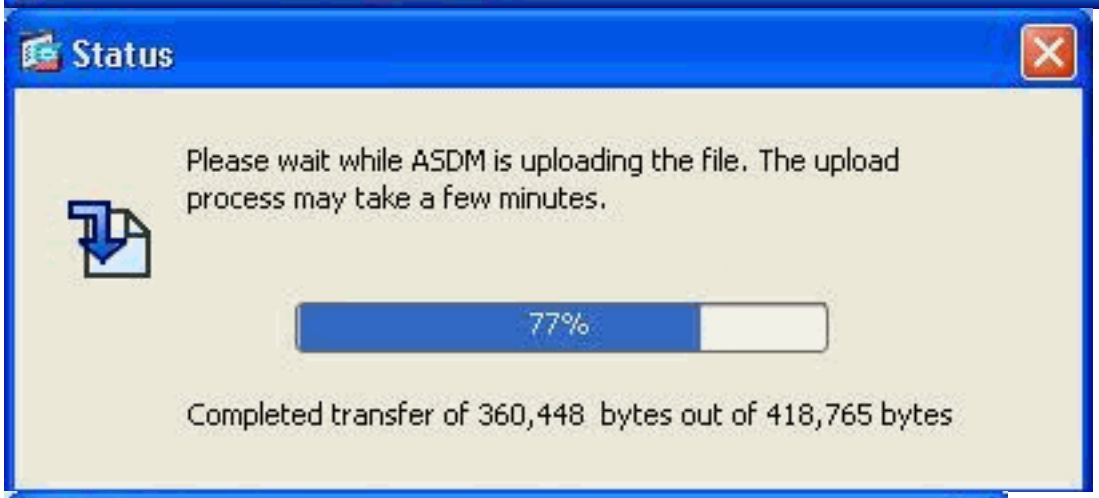


9. Нажмите **Upload** для установки пути к файлу из локального каталога машины.

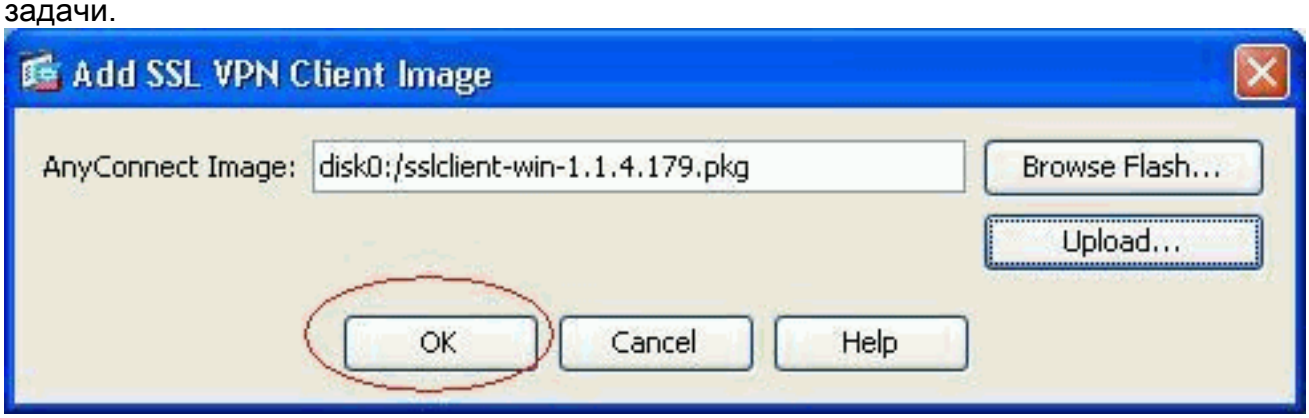


10. Нажмите **Browse Local Files** для выбора каталога, где существует sslclient.pkg файл.

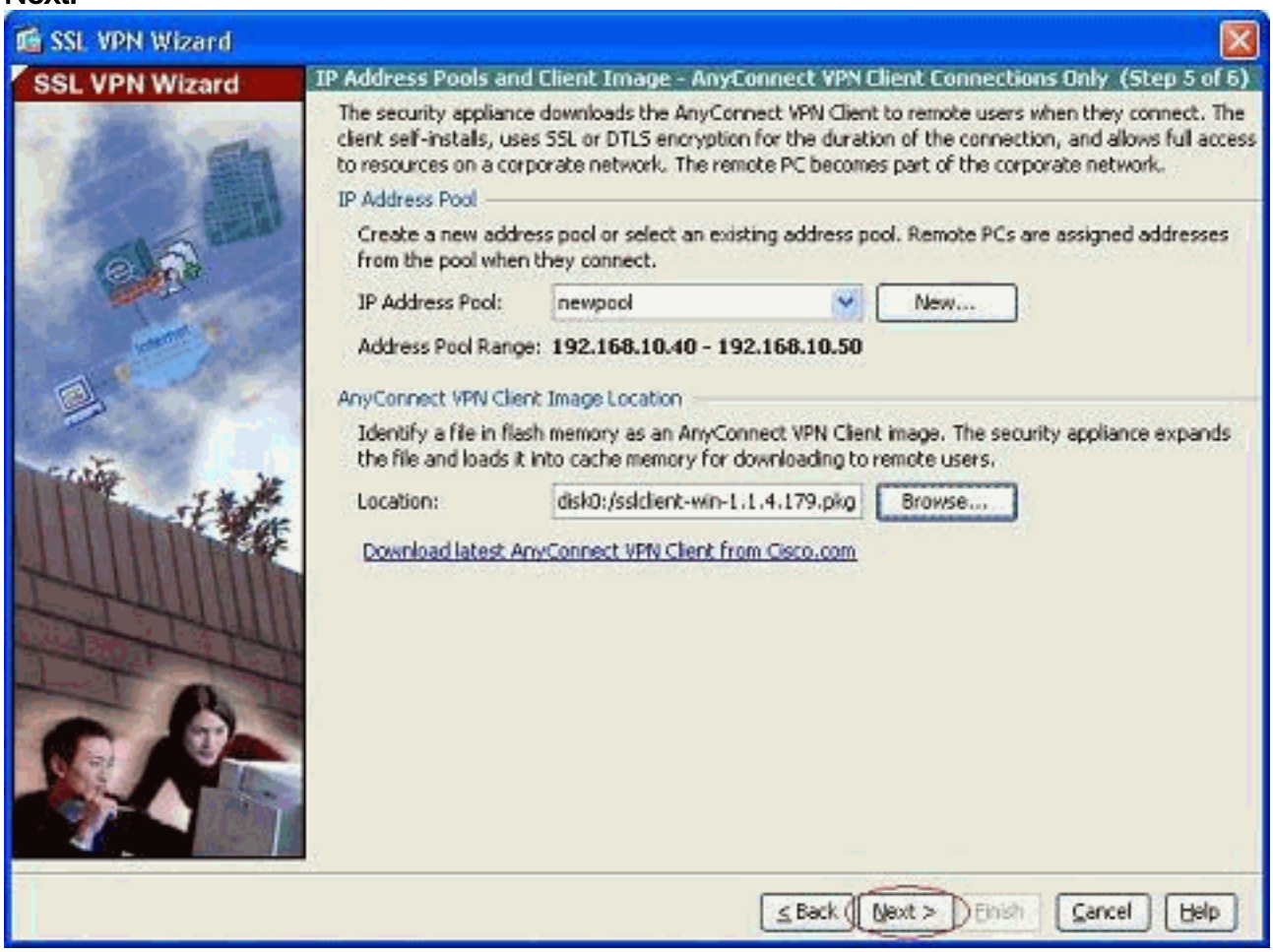
11. Нажмите **Upload File** для загрузки выбранного файла к флэш-памяти ASA.



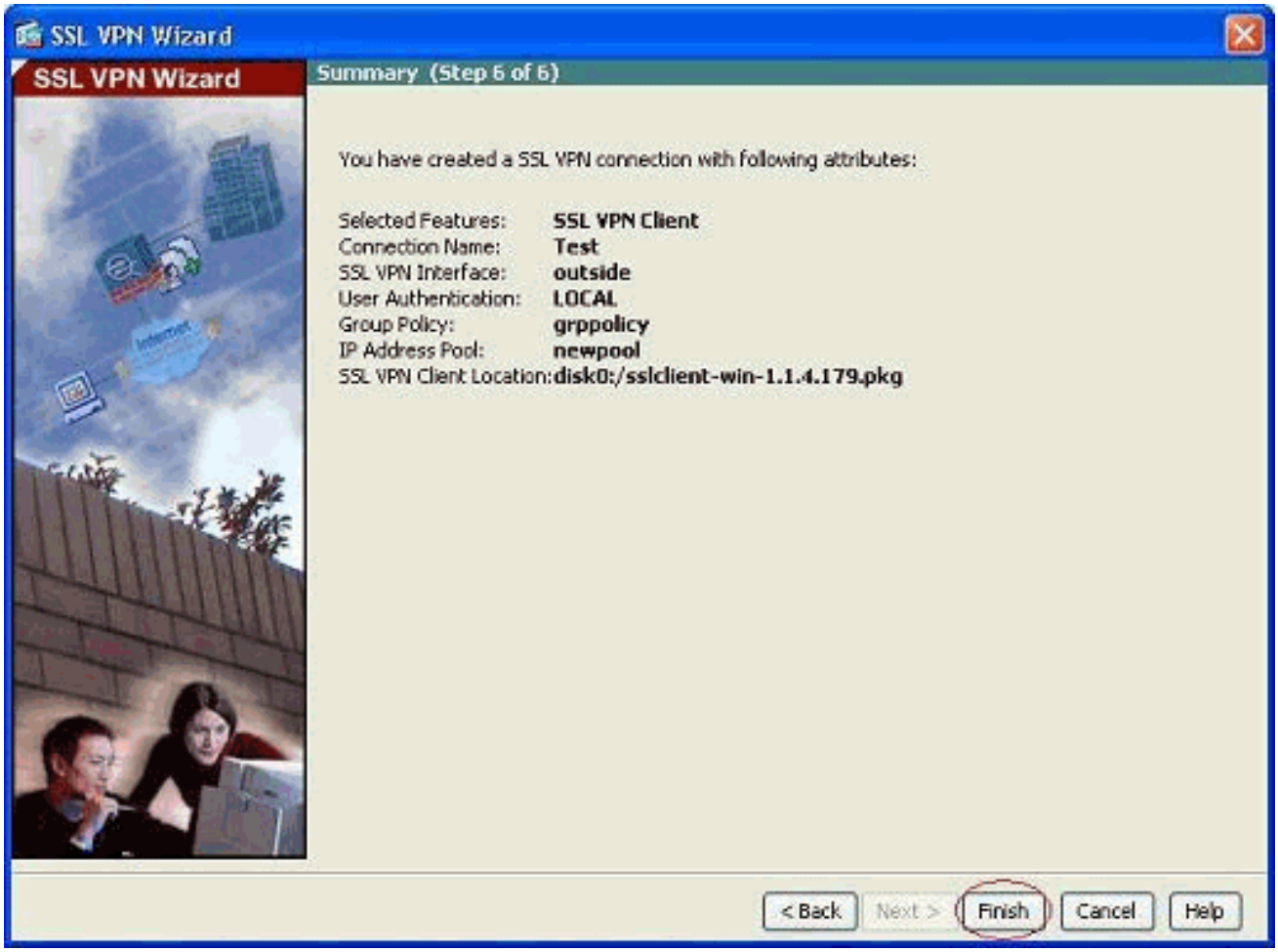
12. Как только файл загружен на флэш-памяти ASA, нажмите **OK** для выполнения той задачи.



13. Теперь это показывает последний anyconnect pkg файл, загруженный на флэш-памяти ASA. **Нажмите кнопку Next.**



14. Сводку конфигурации VPN-клиента SSL (SVC) показывают. Нажмите **Finish** для завершения мастера.



Конфигурация, показанная в ASDM в основном, принадлежит Настройке при помощи мастера VPN-клиента SSL (SVC).

В CLI можно наблюдать некоторую дополнительную настройку. Завершенную конфигурацию интерфейса командой строки показывают ниже, и были выделены важные команды.

cisco ASA

```
ciscoasa#show running-config : Saved : ASA Version
8.0(4) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.2
255.255.255.0 ! interface Ethernet0/2 nameif manage
security-level 0 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Ethernet0/4 shutdown no
nameif no security-level no ip address ! interface
Ethernet0/5 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list nonat extended permit ip
192.168.100.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0 !--- ACL to
define the traffic to be exempted from NAT. no pager
logging enable logging asdm informational mtu outside
1500 mtu inside 1500 mtu manage 1500 !--- Creating IP
address block to be assigned for the VPN clients ip
local pool newpool 192.168.10.40-192.168.10.50 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin no asdm
history enable arp timeout 14400 global (outside) 1
```

```
interface nat (inside) 0 access-list nonat !--- The
traffic permitted in "nonat" ACL is exempted from NAT.
nat (inside) 1 192.168.100.0 255.255.255.0 route outside
0.0.0.0 0.0.0.0 209.165.201.1 1 !--- Default route is
configured through "inside" interface for normal
traffic. route inside 0.0.0.0 0.0.0.0 192.168.100.20
tunneled !--- Tunneled Default route is configured
through "inside" interface for encrypted traffic !
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable !--- Configuring the ASA as HTTP server.
http 10.1.1.0 255.255.255.0 manage !--- Configuring the
network to be allowed for ASDM access. ! !--- Output is
suppressed ! telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global ! !-
-- Output suppressed ! webvpn enable outside !--- Enable
WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1 !--- Assign the
AnyConnect SSL VPN Client image to be used svc enable !-
-- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal !--- Create an
internal group policy "grppolicy" group-policy grppolicy
attributes VPN-tunnel-protocol svc !--- Specify SSL as a
permitted VPN tunneling protocol ! username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 15 !---
Create a user account "cisco" tunnel-group Test type
remote-access !--- Create a tunnel group "Test" with
type as remote access tunnel-group Test general-
attributes address-pool newpool !--- Associate the
address pool vpnpool created default-group-policy
grppolicy !--- Associate the group policy "clientgroup"
created prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

Проверка

Команды, данные в этом разделе, могут использоваться для проверки этой конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

- show webvpn svc — отображает образы SVC, записанные во флэш-памяти ASA.
- show vpn-sessiondb svc — отображает информацию о текущих SSL-подключениях.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Поддержка адаптивных устройств безопасности серии 5500 Cisco
- Пример конфигурации PIX/ASA и клиента VPN для каскадной сети VPN с открытым выходом в Интернет
- Пример настройки SSL клиента VPN (SVC) на ASA с ASDM
- Cisco Systems – техническая поддержка и документация