Пример настройки PIX/ASA в качестве удаленного VPN-сервера с расширенной аутентификацией при использовании CLI и ASDM

Содержание

Введение

Данный документ описывает настройку адаптивных устройств обеспечения безопасности (ASA) Cisco серии 5500 для работы в качестве удаленного VPN-сервера с использованием адаптивного менеджера устройств обеспечения безопасности (ASDM) или CLI. Программа ASDM предоставляет возможность качественного управления и контроля за безопасностью с помощью интуитивно понятного и простого в использовании интерфейса управления на базе веб-технологий. По завершении конфигурации ASA Cisco, можно осуществить проверку при использовании VPN-клиента Cisco.

См. Пример настройки аутентификации PIX/ASA 7.x и VPN-клиента 4.x Cisco в Windows 2003 IAS RADIUS (в Active Directory) для настройки удаленного доступа для соединений с VPN между VPN-клиентом Cisco (4.x для Windows) и PIX Security Appliance 7.x серии 500. Пользователь удаленного VPN-клиента проходит проверку подлинности в Active Directory с помощью RADIUS-сервера службы проверки подлинности в Интернете (IAS) в Microsoft Windows 2003.

См. Пример настройки аутентификации PIX/ASA 7.x и VPN-клиента 4.x Cisco для Cisco Secure ACS для настройки удаленного доступа для соединений с VPN между VPN-клиентом Cisco (4.x для Windows) и PIX Security Appliance 7.x серии 500 с использованием сервера управления доступом Cisco Secure (ACS версии 3.2) для расширенной аутентификации (Xauth).

Предварительные условия

Требования

В данном документе предполагается, что ASA полностью функционален и настроен, чтобы разрешать ASDM Cisco или CLI выполнять изменения в конфигурации.

Примечание. Чтобы позволить ASDM или Secure Shell (SSH) удаленно настроить устройство, см. раздел Разрешение доступа HTTPS для ASDM или PIX/ASA 7.x пример конфигурации SSH на внешнем и внутреннем интерфейсе.

Используемые компоненты

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

- Программное обеспечение адаптивного менеджера устройств обеспечения безопасности Cisco версии 7.x и более поздних
- Адаптивный менеджер устройств обеспечения безопасности версии 5.x и более поздних
- VPN-клиент Cisco версии 4.x и более поздних

Данные для документа были получены в специально созданных лабораторных условиях. Все устройства, используемые в данном документе, были запущены с чистой (заданной по умолчанию) конфигурацией. Если сеть работает в реальных условиях, убедитесь, что вы понимаете потенциальное воздействие каждой команды.

Соответствующие продукты

Данную конфигурацию также можно использовать с Cisco PIX Security Appliance версии 7.x и более поздних

Условные обозначения

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

Базовые сведения

Конфигурация удаленного доступа предоставляет безопасный удаленный доступ для VPN-клиентов Cisco, например, для мобильных пользователей. Удаленный доступ VPN предоставляет удаленным пользователям безопасный доступ к централизованным сетевым ресурсам. VPN-клиент Cisco выполняет протокол IPSec, а также специально разработан для работы с устройством обеспечения безопасности. Однако устройство обеспечения безопасности может устанавливать соединения IPSec со многими клиентами совместимыми с протоколом. Дополнительные сведения о протоколе IPSec, см. Руководство по настройке ASA.

Группы и пользователи являются основными понятиями в управлении безопасностью VPN и в конфигурации устройств обеспечения безопасности. Они указывают атрибуты, которые определяют доступ и использование VPN пользователям. Группа – это собрание

пользователей, которое считается как единый объект. Пользователи получают атрибуты от групповой политики. Туннельные группы определяют групповую политику для конкретных соединений. Если пользователям не назначить определенную групповую политику, то для соединений будет применяться групповая политика по умолчанию.

Туннельная группа состоит из набора записей, которые определяют политику туннельного подключения. Данные записи определяют серверы, для которых туннельные пользователи проходят проверку подлинности, а также сервера учетной информации, если такие имеются, на которые отсылаются сведения о подключениях. Они также определяют стандартную групповую политику подключений, и содержат параметры подключений, зависящие от протоколов. Туннельные группы включают небольшое число атрибутов, которые описывают создание самого туннеля. Туннельные группы включают в себя указатель на групповую политику, который определяет атрибуты, ориентированные на пользователя.

Примечание. В примере данного документа, учетные записи локальных пользователей используются для аутентификации. Если необходимо использовать другие службы, например LDAP и RADIUS, см. Настройка внешнего сервера RADIUS для аутентификации и авторизации.

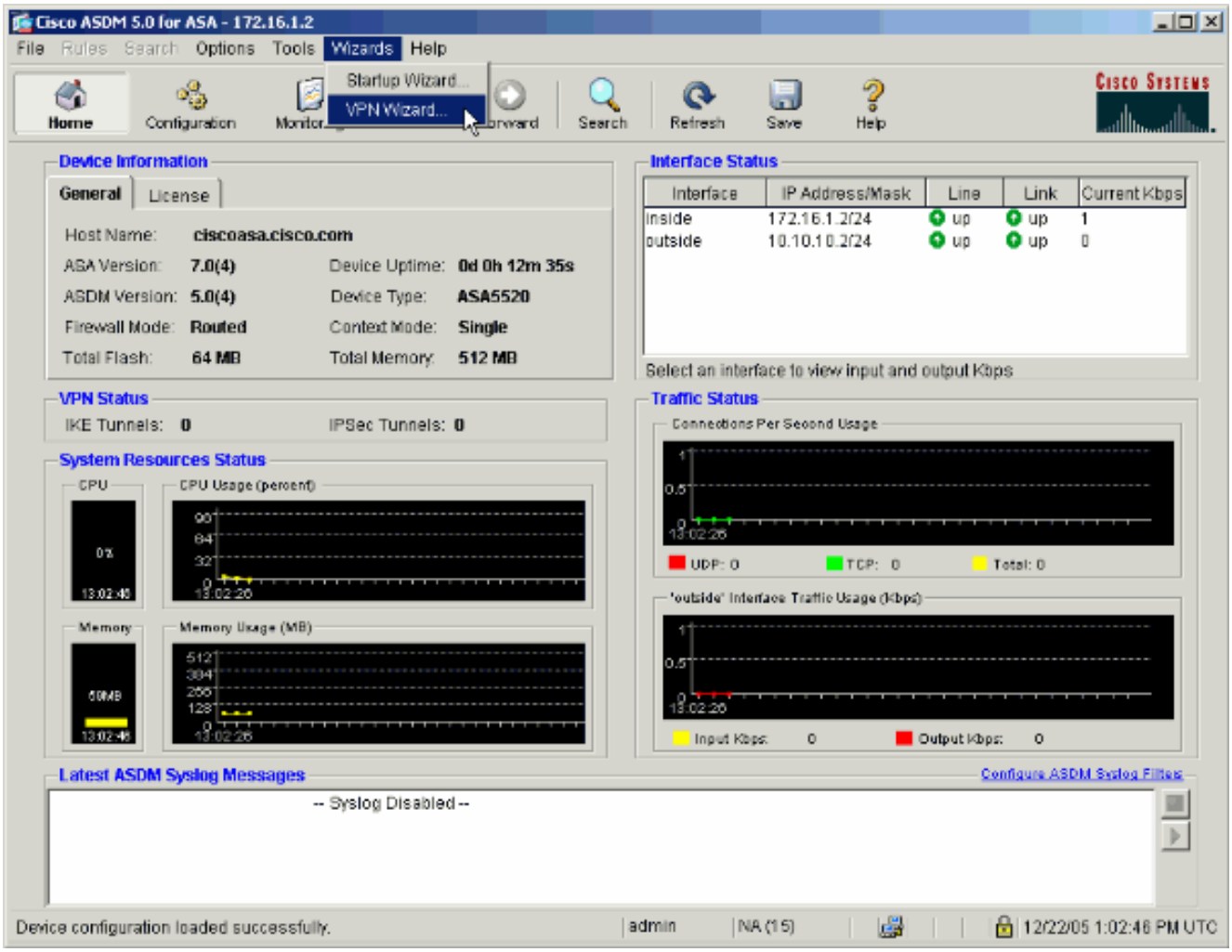
Протокол ассоциаций безопасности и управления ключами в Интернет (ISAKMP), также имеет название IKE, является протоколом согласования, который хранит согласования о построении ассоциации безопасности IPSec. Каждый протокол согласования ISAKMP разделен на два раздела, фаза 1 и фаза 2. Фаза 1 создает первый туннель, который обеспечивает защиту дальнейших сообщений согласования ISAKMP. Фаза 2 создает туннель, который обеспечивает защиту данных, перемещаемых через безопасное соединение. Дополнительные сведения о ISAKMP, см. Ключевые слова политики ISAKMP для команд CLI.

Конфигурации

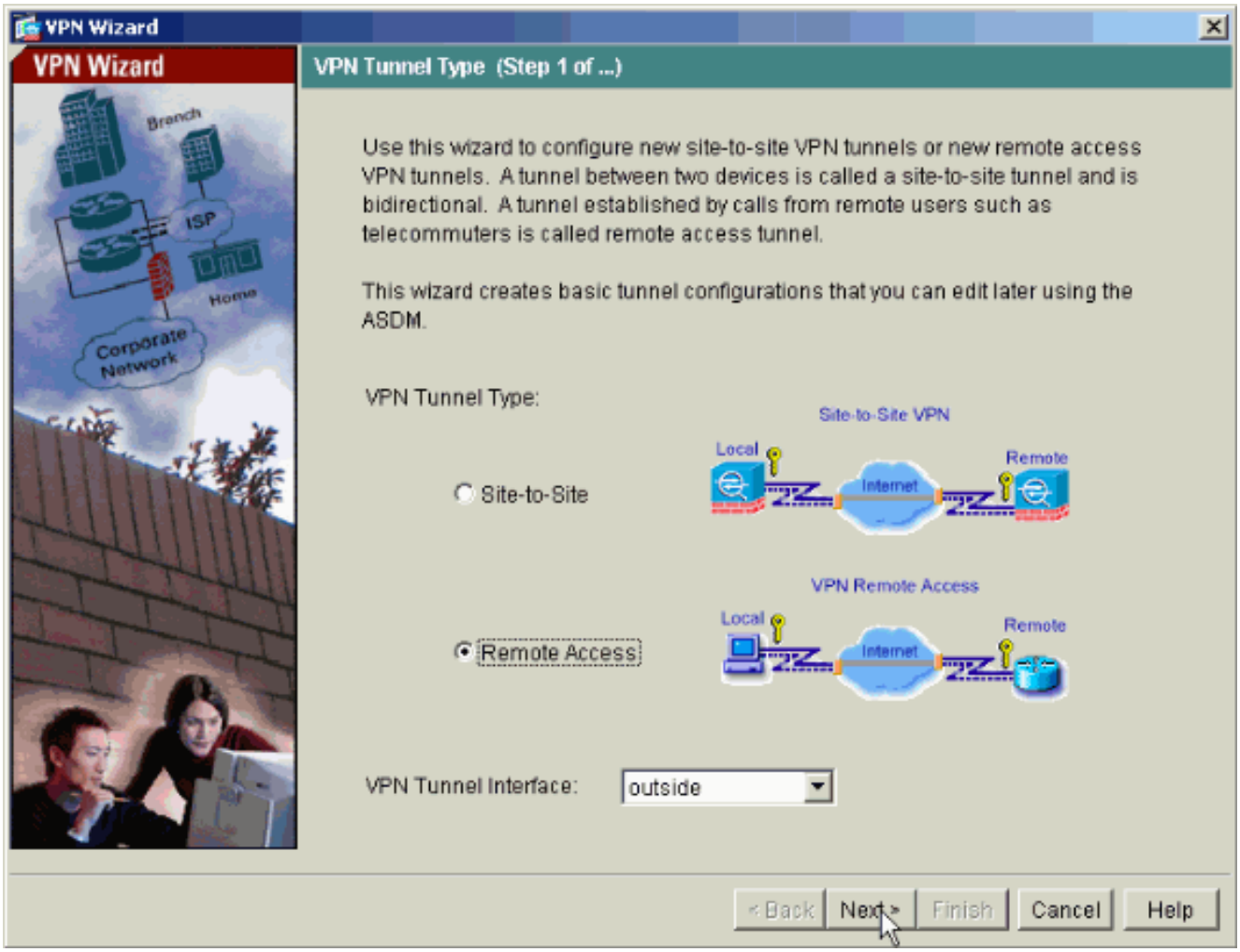
Настройка ASA/PIX в качестве удаленного VPN-сервера с помощью ASDM

Чтобы настроить ASA Cisco в качестве удаленного VPN-сервера с использованием ASDM, необходимо выполнить следующие действия:

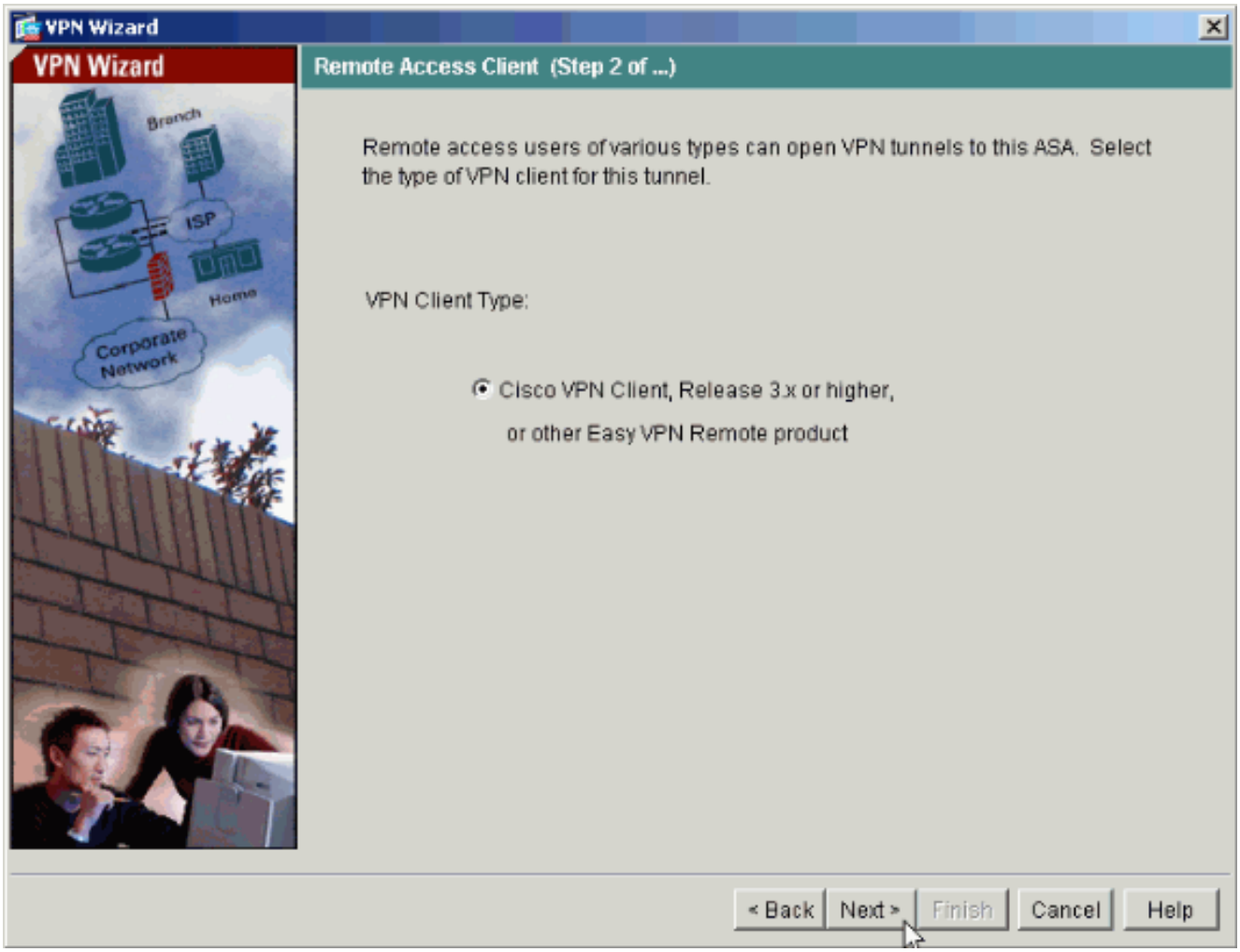
1. Выберите **Wizards > VPN Wizard** в окне "Home".



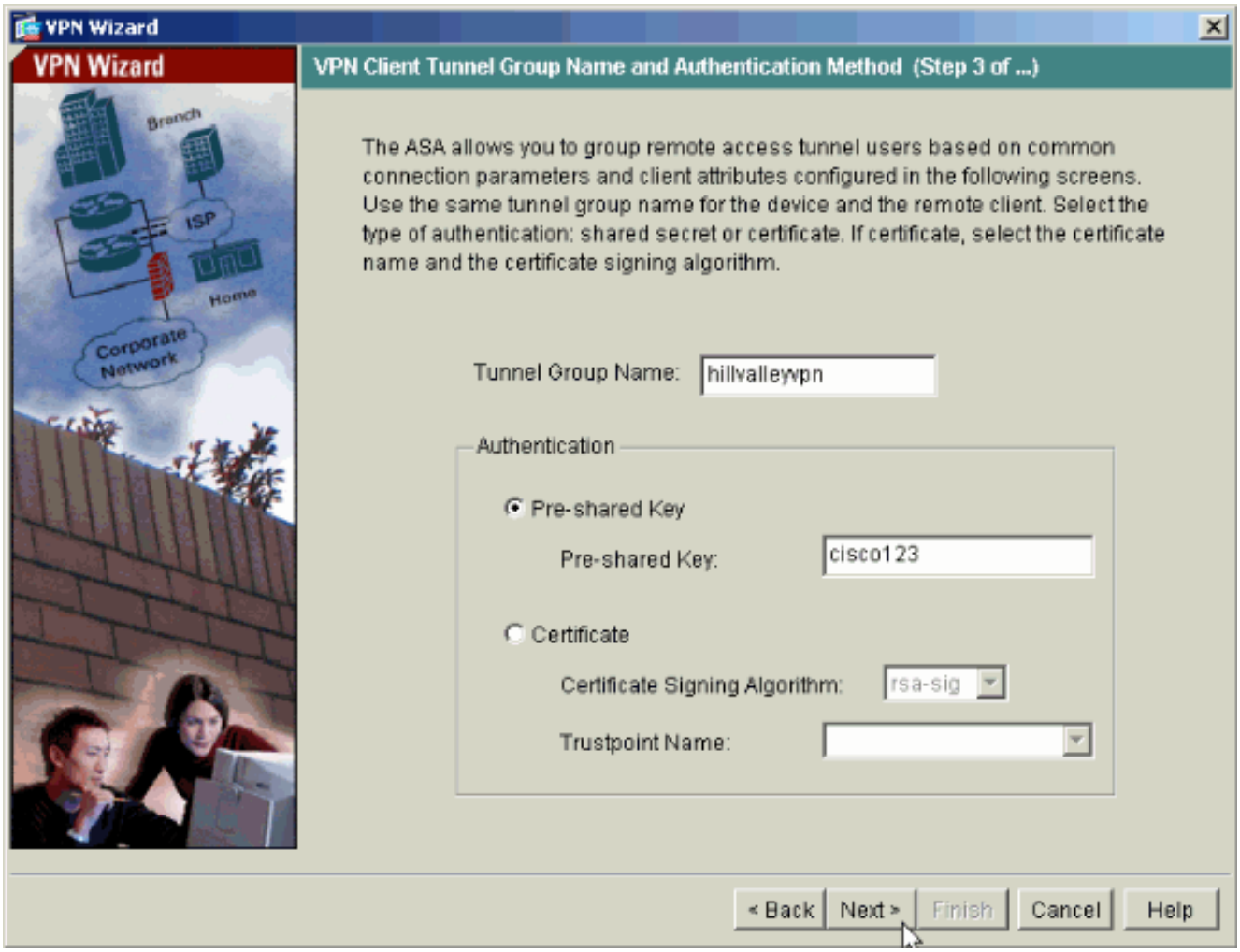
2. В **Remote Access** выберите тип VPN-туннеля и убедитесь, что интерфейс туннеля VPN установлен, как
требуется.



3. Единственный доступный тип VPN-клиент уже выбран. Нажмите **Next**.

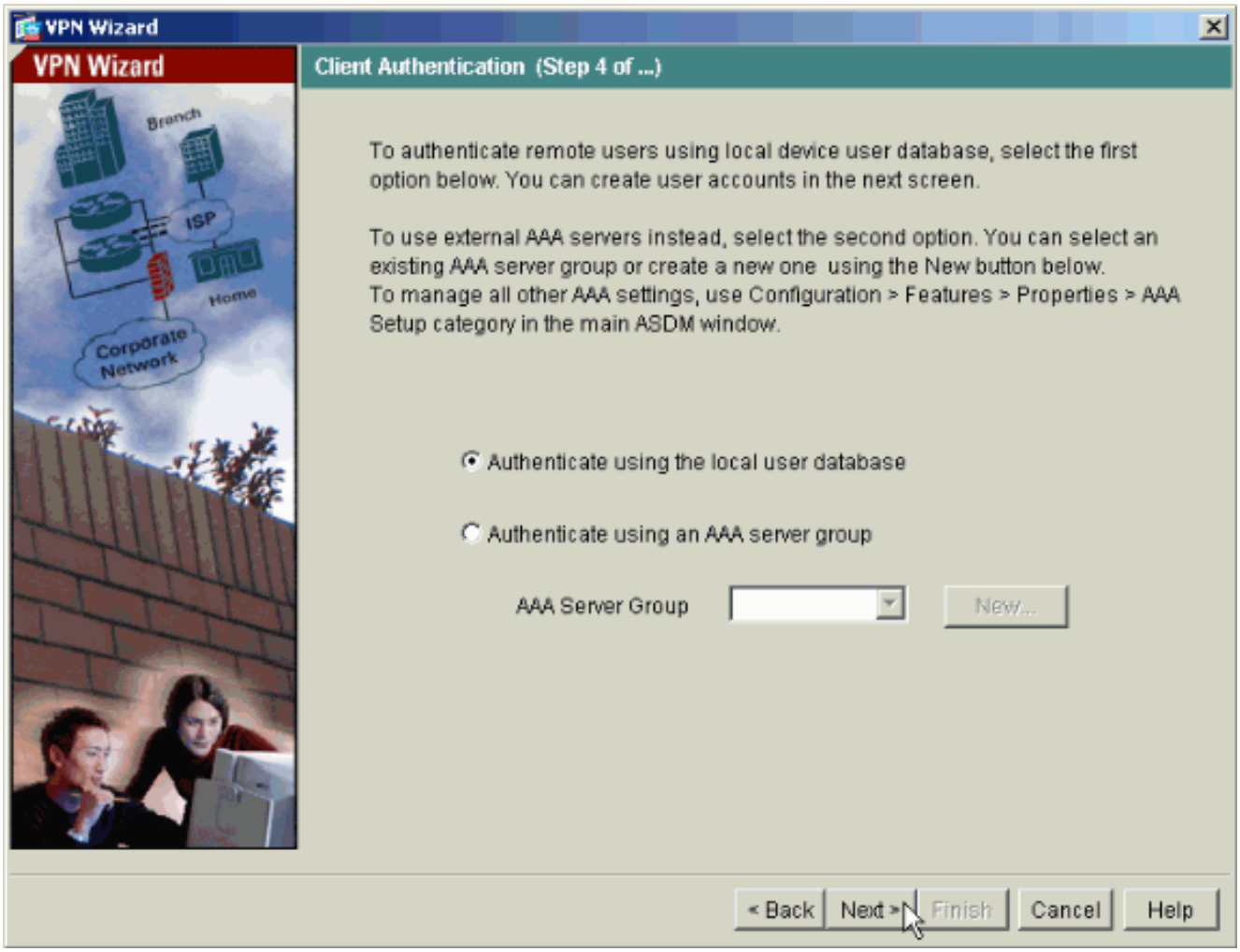


4. Введите имя для туннельной группы. Предоставьте необходимые для использования сведения об аутентификации.В данном документе выбран **Pre-shared Key**.

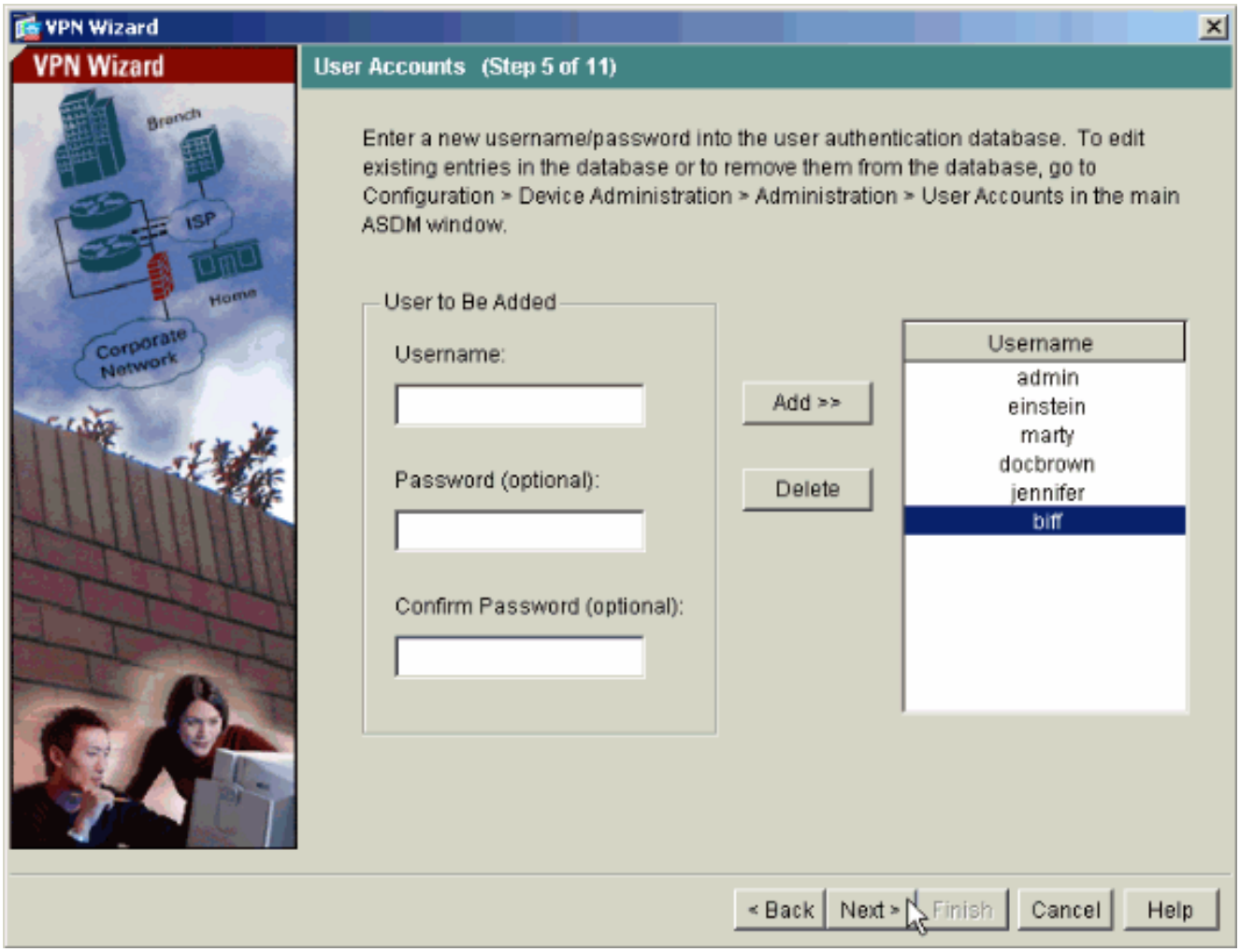


Примечание. На ASDM нет способа скрыть или зашифровать предварительно согласованный ключ. Причина в том, что ASDM должен использоваться только людьми, которые настраивали ASA или теми, кто помогает клиентам с данной конфигурацией.

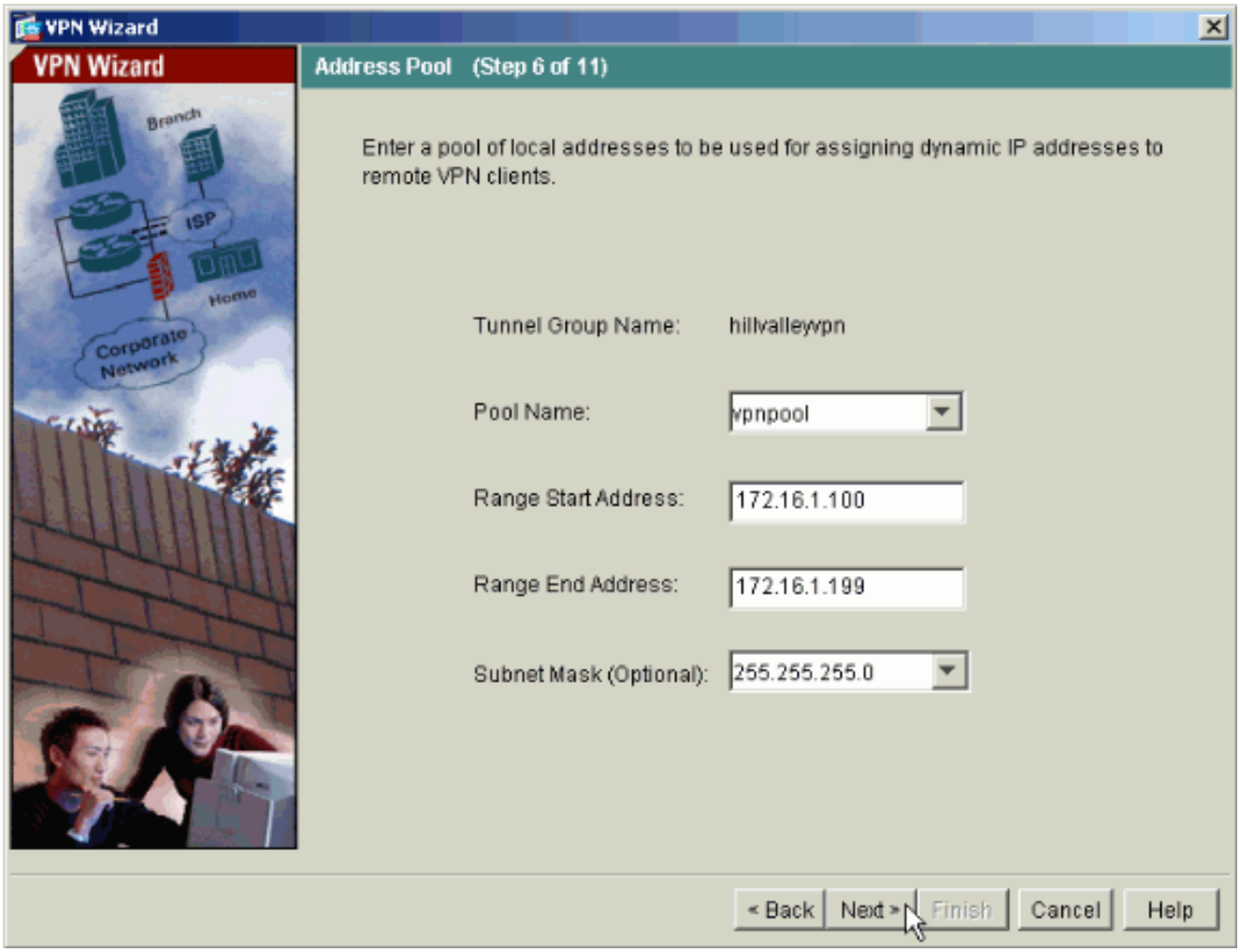
5. Выберите, где будет происходить аутентификация удаленных пользователей, либо на локальной базе данных пользователей, либо на внешней группе сервера AAA.**Примечание.** Добавление пользователей к локальной базе данных пользователей происходит в шаге 6.**Примечание.** Дополнительные сведения о настройке внешней группы сервера AAA с помощью ASDM, см. Пример настройки PIX/ASA 7.x авторизация и аутентификация групп серверов для пользователей VPN с помощью ASDM.



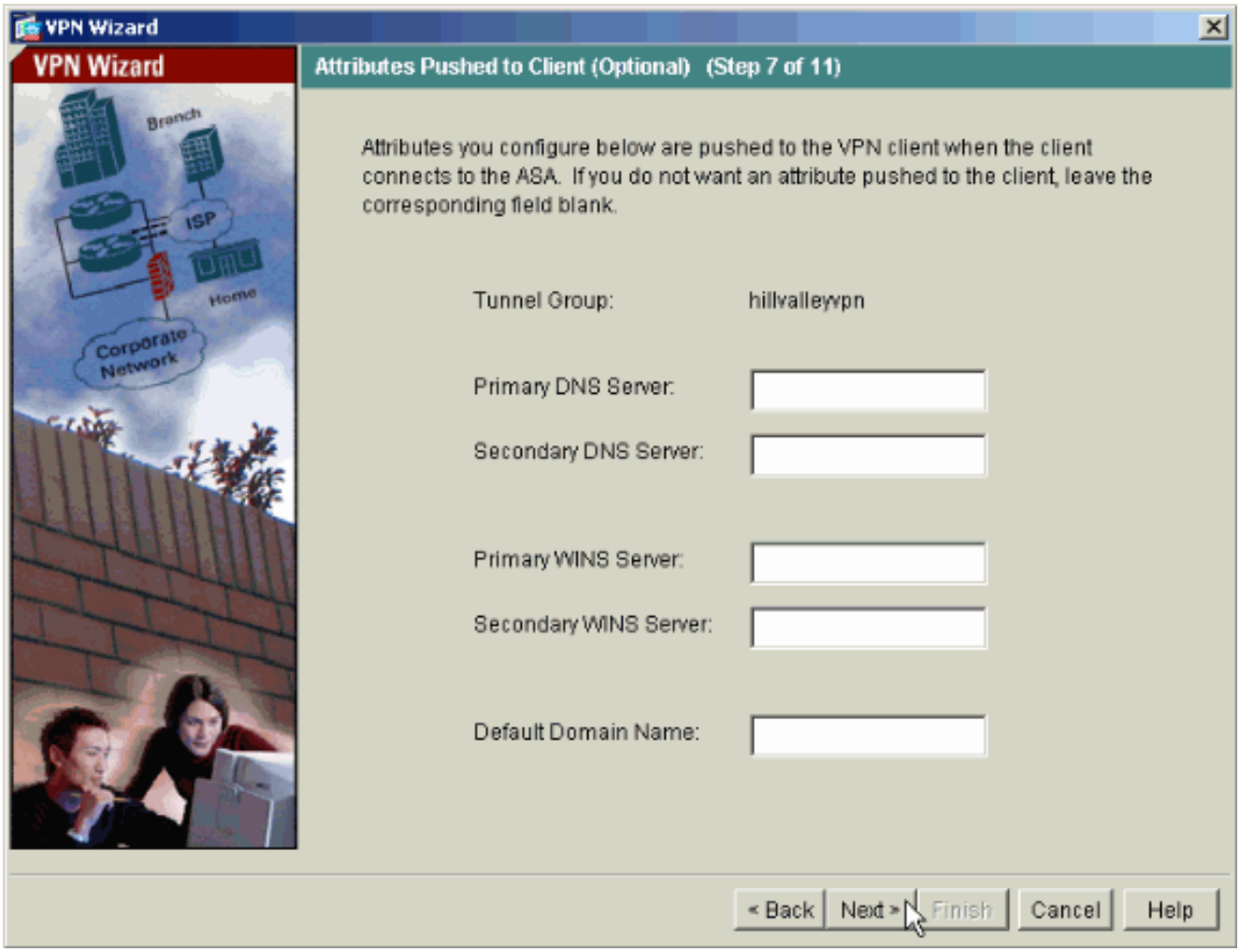
6. При необходимости добавьте пользователей к локальной базе данных.**Примечание.** Не удаляйте существующих пользователей из данного окна. Выберите **Configuration > Device Administration > Administration > User Accounts in the main ASDM window**, чтобы отредактировать существующие в базе данных записи или удалить их из базы данных.



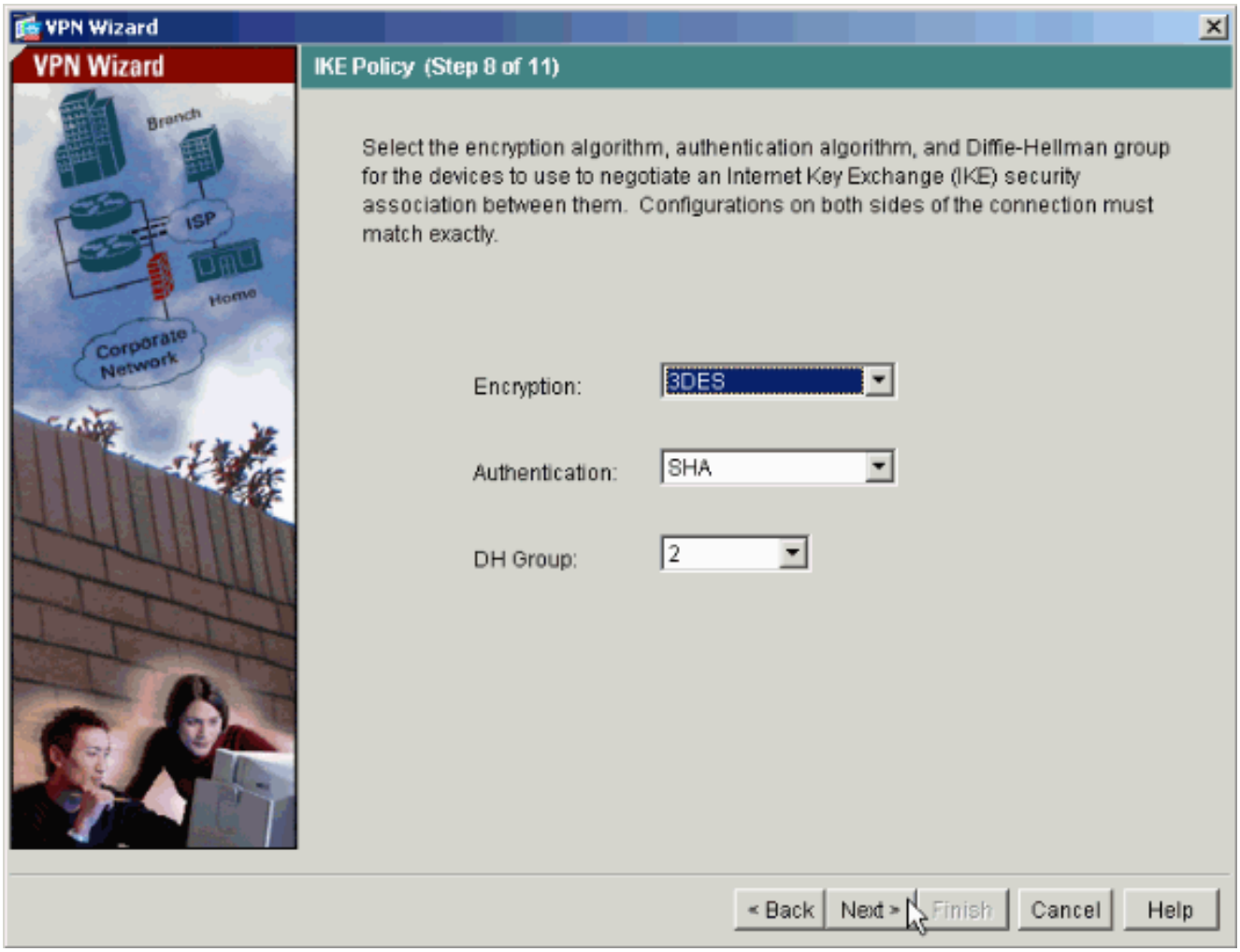
7. Определите пул локальных адресов, который будет динамически назначен удаленным VPN-клиентам при
подключении.



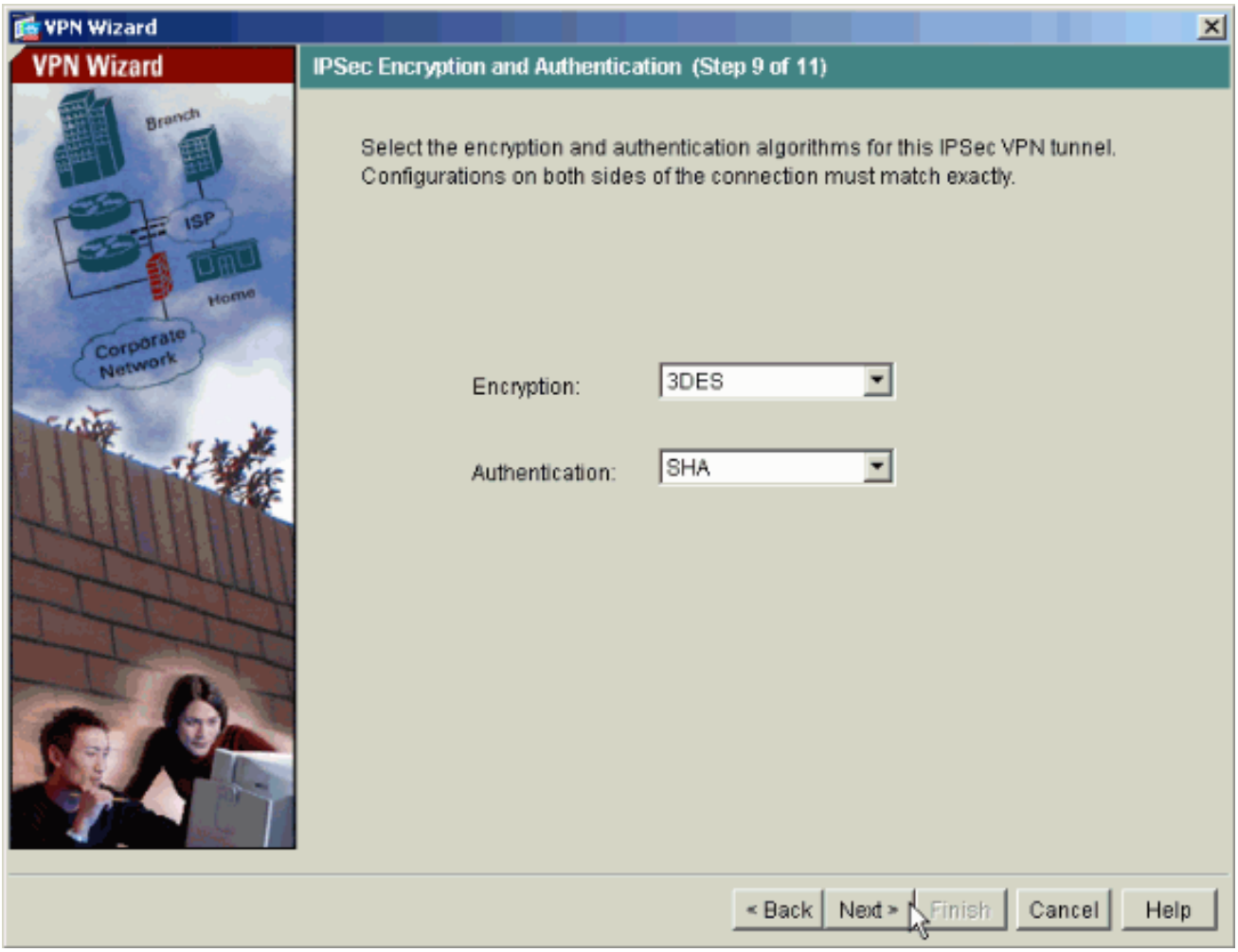
8. *Необязательно:* Укажите сведения серверов DNS и WINS, а также имя домена по умолчанию. Эти сведения будут переданы удаленным VPN-клиентам.



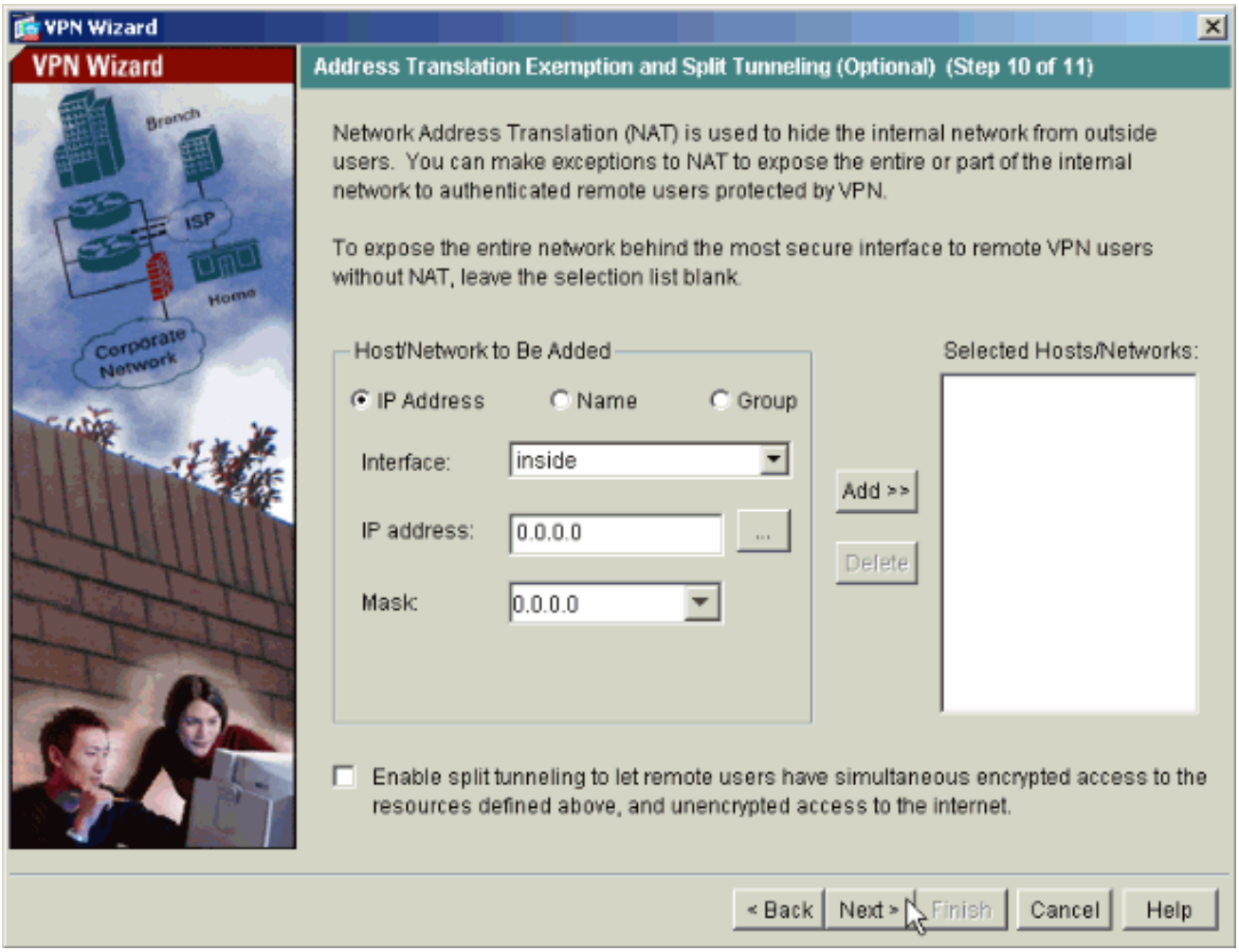
9. Укажите параметры для IKE, который также известен как IKE фаза1.Конфигурации на обоих концах туннеля должны совпадать. Однако VPN-клиент Cisco автоматически выбирает подходящую для него конфигурацию. Таким образом, конфигурация IKE на PC-клиенте
необязательна.



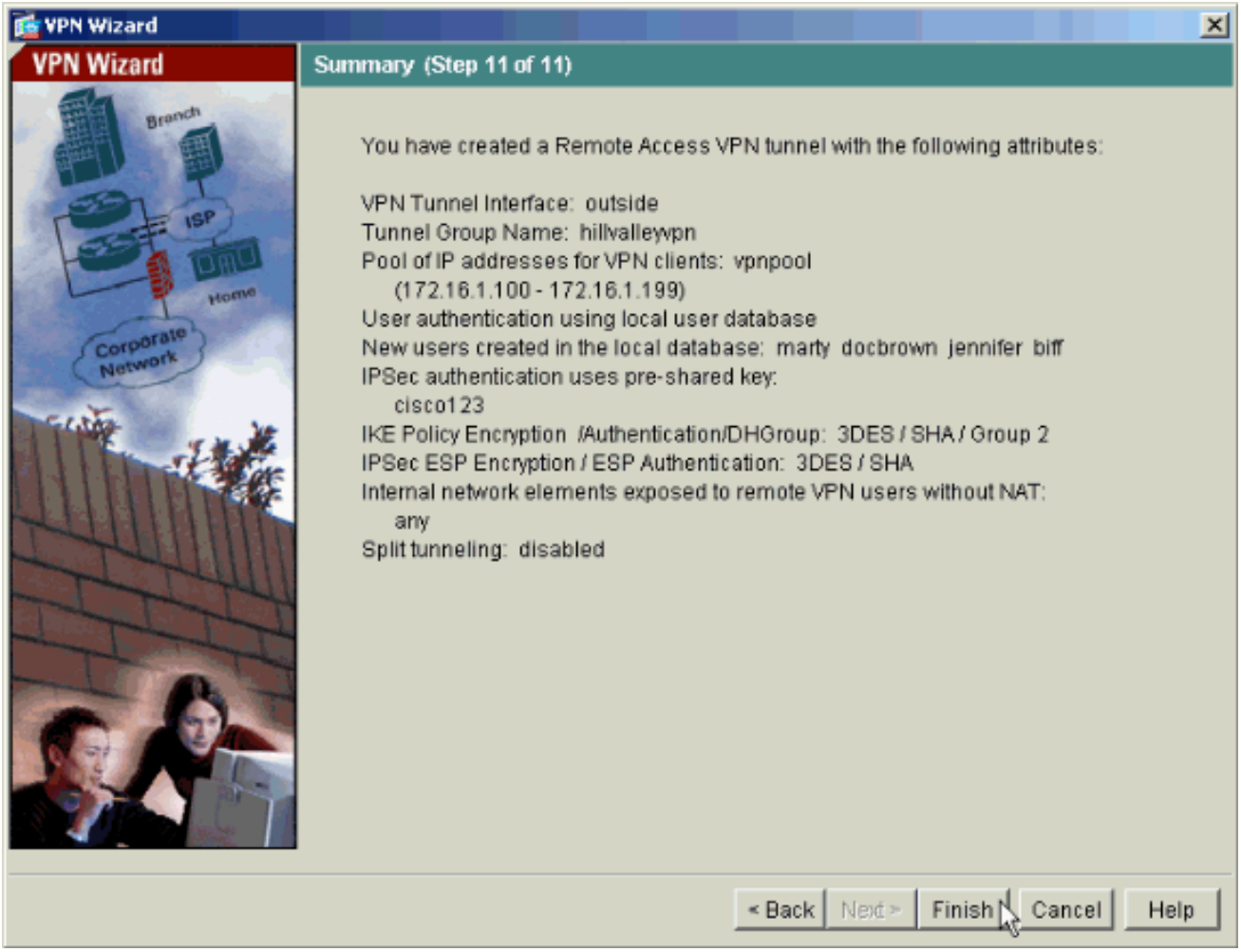
10. Укажите параметры для IPSec, который также известен как IKE фаза 2.Конфигурации на обоих концах туннеля должны совпадать. Однако VPN-клиент Cisco автоматически выбирает подходящую для него конфигурацию. Таким образом, конфигурация IKE на PC-клиенте
необязательна.



11. Укажите, какие из внутренних узлов или сетей (если таковые имеются) должны быть доступны удаленным пользователям VPN.Если данный список оставить пустым, это позволит удаленным пользователям VPN получить доступ ко всей внутренней сети ASA.В данном окне можно также включить раздельное туннелирование. Раздельное туннелирование шифрует трафик в указанные раннее ресурсы данной процедуры и предоставляет нешифрованный доступ к Интернет в полной мере без туннелирования этого трафика. Если раздельное туннелирование *не* включено, весь трафик удаленных VPN-пользователей направлен к ASA. Полоса пропускания и процессор могут работать слишком интенсивно в соответствии с конфигурацией.



12. Данное окно показывает сводку по совершенным действиям. Если конфигурация в порядке, нажмите
Finish.



Настройка ASA/PIX в качестве удаленного VPN-сервера с помощью CLI

Чтобы настроить удаленный VPN-сервер доступа из командной строки, выполните следующие действия. Дополнительные сведения по каждой использованной команды, см. Настройка удаленного доступа VPN или Справочник команд адаптивных устройств обеспечения безопасности Cisco ASA серии 5500.

1. Введите команду **ip local pool** в режиме глобальной конфигурации, чтобы настроить пулы IP-адресов, которые будут использоваться VPN-туннелями удаленного доступа. Чтобы удалить пулы адресов, введите данную команду с параметром "no".Устройство обеспечения безопасности использует пулы адресов, основанные на туннельной группе данного подключения. Если настроить более чем один адресный пул для туннельной группы, устройство обеспечения безопасности будет использовать их в том порядке, в котором они настроены. Подайте данную команду, чтобы создать пул для локальных адресов, который может быть использован для назначения динамических адресов VPN-клиентам удаленного доступа:`ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`
2. Подайте следующую команду:`ASA-AIP-CLI(config)#username marty password 12345678`
3. Подайте следующую команду:`ASA-AIP-CLI(config)#tunnel-group hillvalleyvpn general-attributes`
4. Подайте следующую команду, чтобы обозначить локальную базу данных пользователей для аутентификации.`ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL`
`ASA-AIP-CLI(config-tunnel-general)#authentication-server-group LOCAL`
5. Подайте данную команду, находясь в режиме общих атрибутов туннельной группы

hillvalleyvpn, чтобы назначить vpnpool созданный в шаге 1 для группы hillvalleyvpn.ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

6. Подайте следующую команду:ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**
7. Подайте следующую команду:ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**
8. Подайте следующую команду:ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**
9. Подайте следующие команды, чтобы настроить определенный туннель:ASA-AIP-CLI(config)#**isakmp policy 1 authentication pre-share**ASA-AIP-CLI(config)#**isakmp policy 1 encryption 3des**ASA-AIP-CLI(config)#**isakmp policy 1 hash sha**ASA-AIP-CLI(config)#**isakmp policy 1 group 2**ASA-AIP-CLI(config)#**isakmp policy 1 lifetime 43200**ASA-AIP-CLI(config)#**isakmp enable outside**ASA-AIP-CLI(config)#**crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA-AIP-CLI(config)#**crypto dynamic-map Outside_dyn_map 10 set reverse-route**ASA-AIP-CLI(config)#**crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**ASA-AIP-CLI(config)#**crypto map Outside_map 10 ipsec-isakmp dynamic Outside_dyn_map**ASA-AIP-CLI(config)#**crypto map outside_map interface outside**ASA-AIP-CLI(config)#**crypto isakmp nat-traversal**
10. *Необязательно:* Подайте следующую команду, если требуется совершить подключение в обход списка доступа, который применяется к интерфейсу:ASA-AIP-CLI(config)#**sysopt connection permit-ipsec**

    Примечание. Данная команда работает на образах версии 7.x до версии 7.2(2). Если используется образ версии 7.2(2), подайте следующую команду ASA-AIP-CLI(config)#sysopt connection permit-vpn.
11. Подайте следующую команду:ASA-AIP-CLI(config)#**group-policy hillvalleyvpn interna**
12. Подайте следующие команды, чтобы настроить клиентское соединение:ASA-AIP-CLI(config)#**group-policy hillvalleyvpn attributes**ASA-AIP-CLI(config)#(config-group-policy)#**dns-server value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**

Запуск конфигурации на устройстве ASA

```
ASA-AIP-CLI(config)#show running-config
ASA Version 7.2(2)
!
hostname ASAwAIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
```

```
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp.com
pager lines 24
mtu Outside 1500
mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
group-policy hillvalleyvpn1 internal
group-policy hillvalleyvpn1 attributes
 dns-server value 172.16.1.11
 vpn-tunnel-protocol IPSec
 default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto dynamic-map Outside_dyn_map 10 set transform-set
ESP-3DES-SHA
crypto dynamic-map outside_dyn_map 10 set security-
association lifetime seconds 288000
crypto map Outside_map 10 ipsec-isakmp dynamic
Outside_dyn_map
crypto map Outside_map interface Outside
crypto isakmp enable Outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group hillvalleyvpn type ipsec-ra
tunnel-group hillvalleyvpn general-attributes
 address-pool vpnpool
```

```
tunnel-group hillvalleyvpn ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
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
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192
: end
ASA-AIP-CLI(config)#
```

Конфигурация хранения паролей VPN-клиента Cisco

Если VPN-клиентов Cisco несколько, становится трудно запомнить все имена пользователя и пароли VPN-клиента. Чтобы хранить пароли VPN-клиента на компьютере, настройте ASA/PIX и VPN-клиент, как описано в данном разделе.

ASA/PIX

В режиме глобальной конфигурации используйте команду **group-policy attributes**:

```
group-policy VPNusers attributes
  password-storage enable
```

VPN-клиент Cisco

Отредактируйте файл **.pcf file** и измените эти параметры:

```
SaveUserPassword=1
UserPassword= <type your password>
```

Отключение расширенной аутентификации

В режиме туннельной группы, введите эту команду, чтобы отключить расширенную аутентификацию, включенную по умолчанию, на PIX/ASA 7.x:

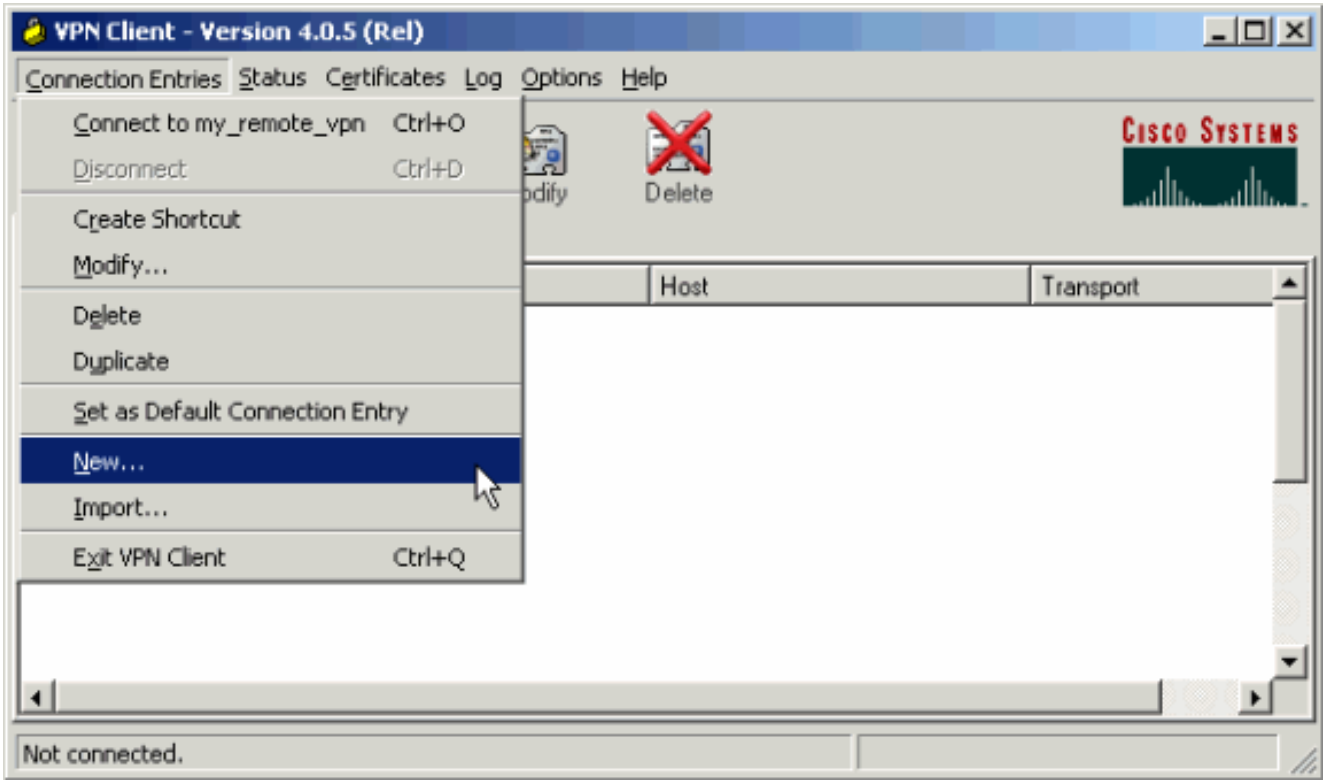
```
asa(config)#tunnel-group client ipsec-attributes
asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

После отключения расширенной аутентификации, VPN-клиенты не отображают всплывающее окно с именем пользователя и паролем для аутентификации (Xauth). Таким образом, ASA/PIX не требуется конфигурация имени пользователя и пароля для аутентификации VPN-клиентов.

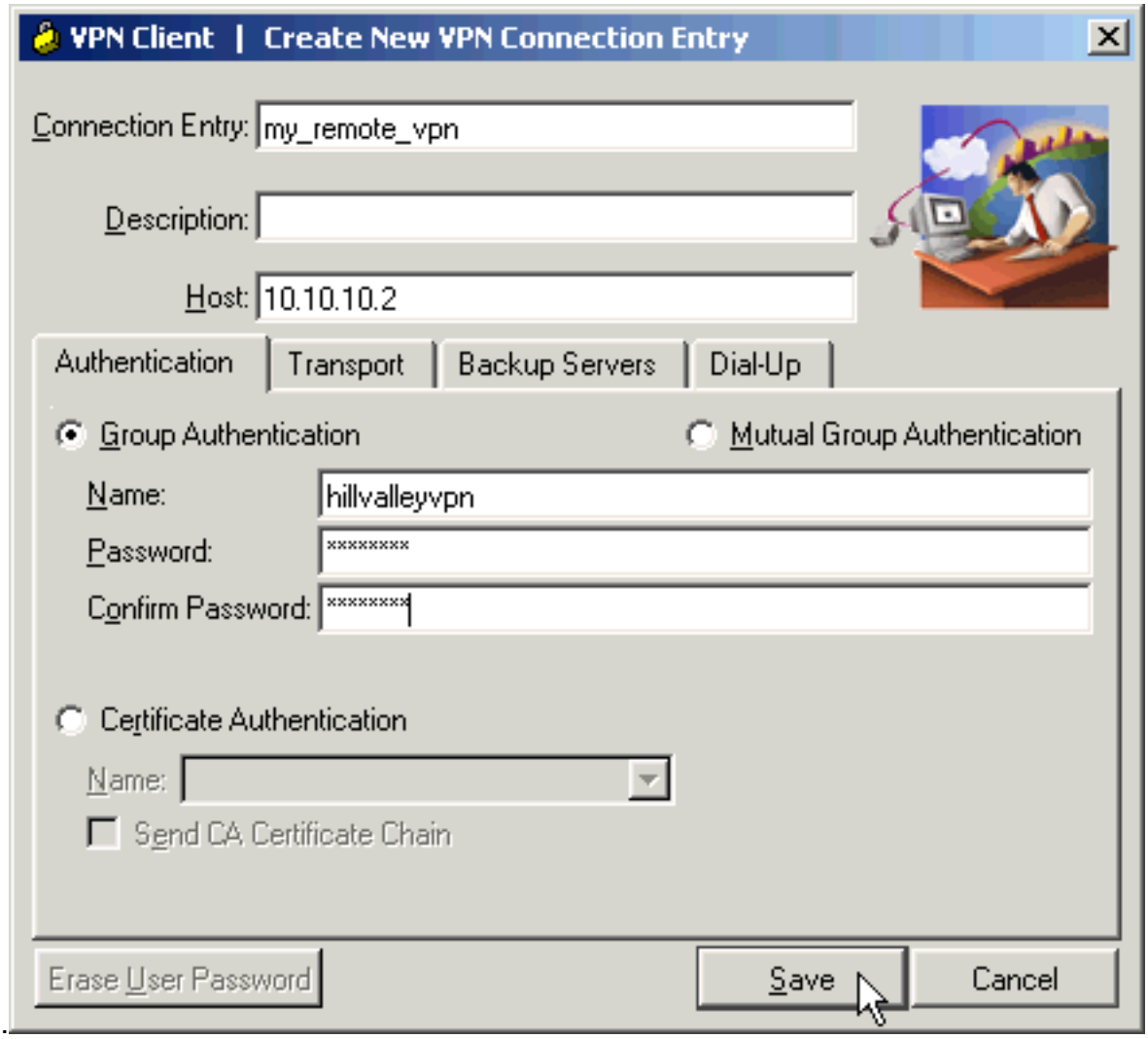
Проверка

Попытайтесь подключиться к ASA Cisco с использованием VPN-клиента Cisco, чтобы проверить правильность настройки ASA.

1. Выберите **Connection Entries > New**.

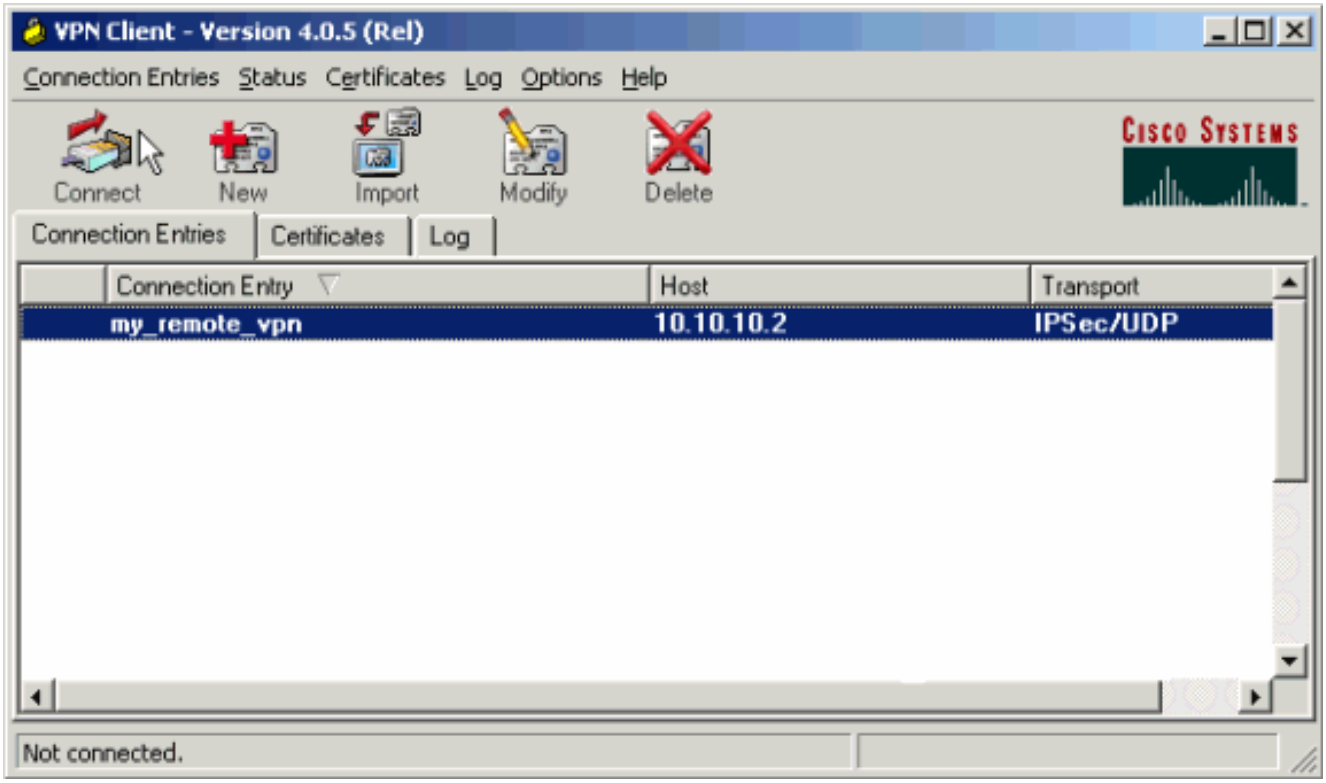


2. Введите сведения о новом подключении.Поле "Host" должно содержать IP-адрес или имя узла изначально настроенного ASA Cisco. Сведения об аутентификации группы должны соответствовать тем, которые были использованы в шаге 4. По окончании нажмите



Save.

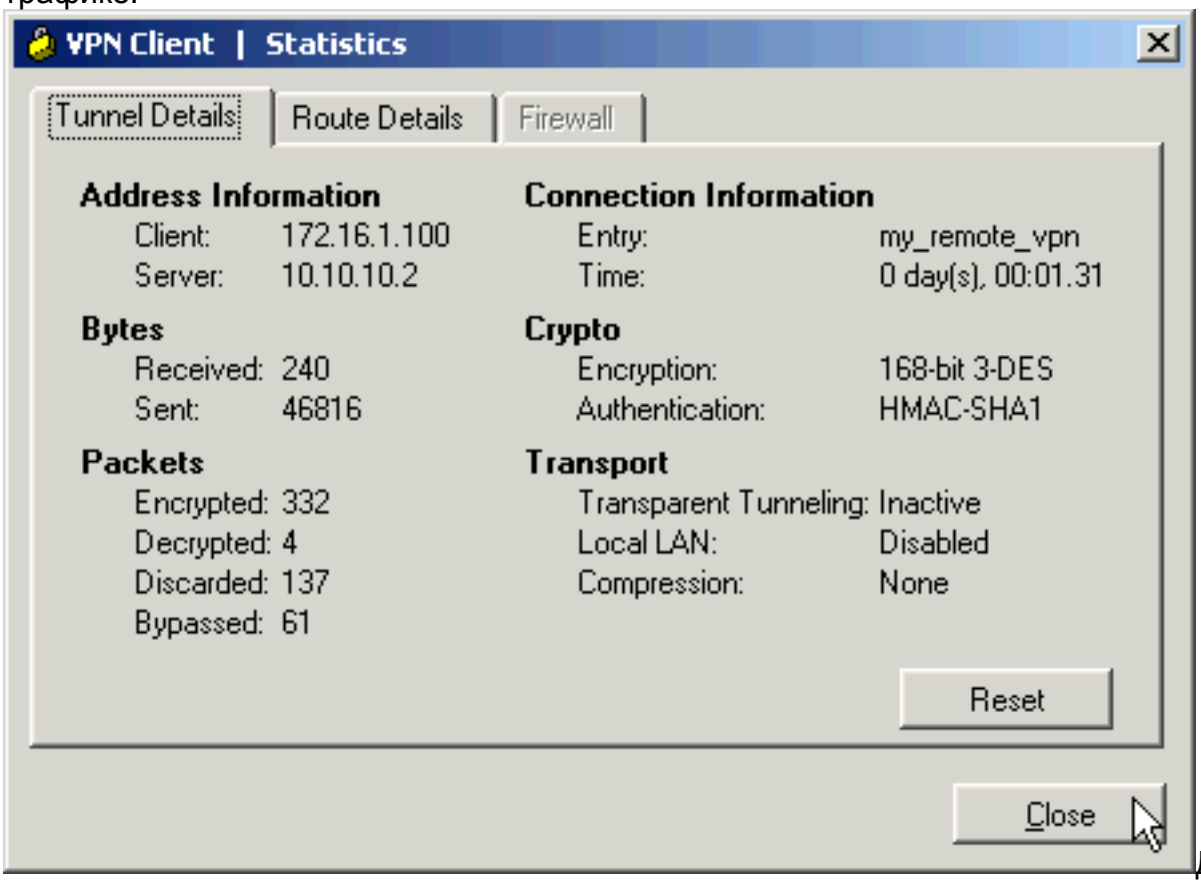
3. Выберите созданное только что новое подключение и нажмите **Connect**.



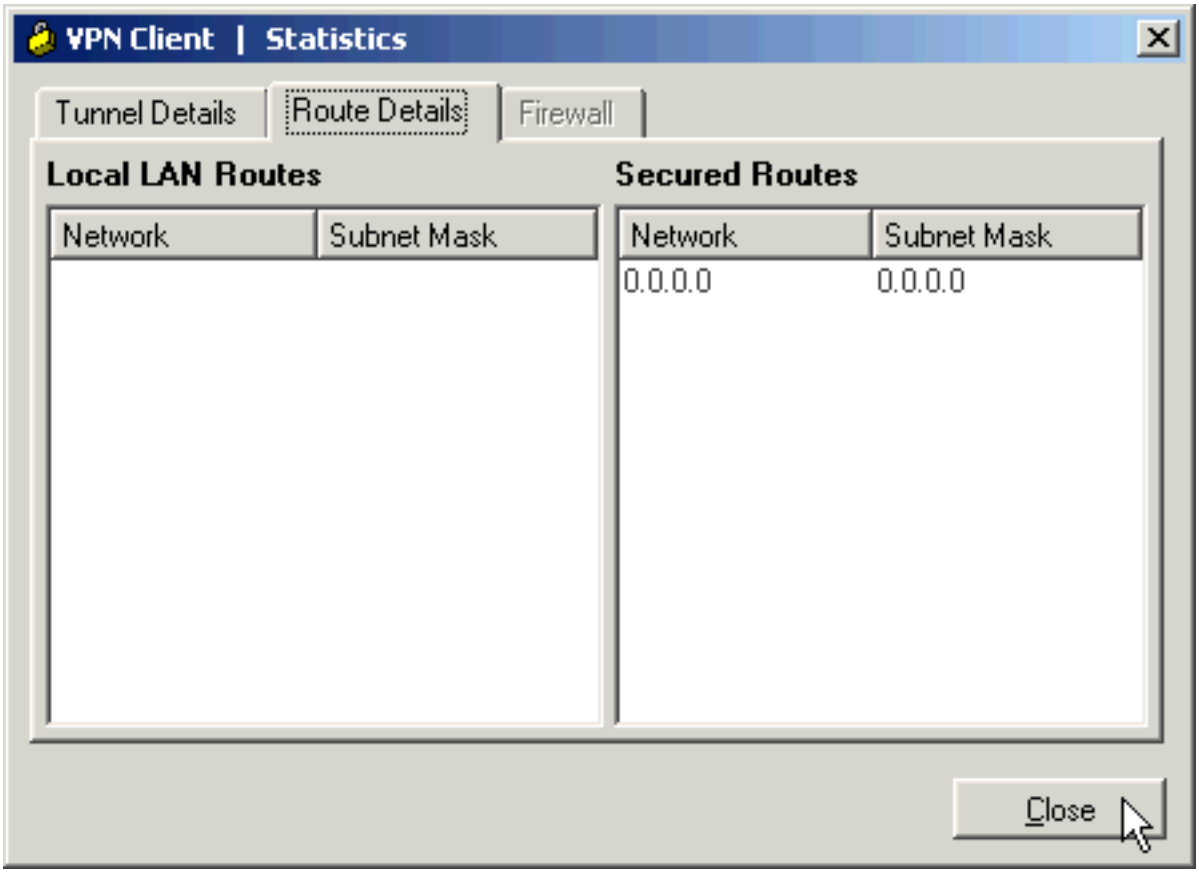
4. Введите имя пользователя и пароль для расширенной аутентификации. Данные сведения должны соответствовать тем, которые были указаны в [шаге 5 и]

6.

5. После успешного установления подключения выберите **Statistics** в меню Status, чтобы проверить сведения о туннели.Данное окно отображает зашифрованные сведения и сведения о трафике:



Данное окно отображает сведения о раздельном туннелировании:



Устранение неполадок

Данный раздел предназначен для устранения неполадок конфигурации.

Неверное шифрование ACL

ASDM 5.0(2) создает и применяет зашифрованный список управления доступом (ACL), который может вызвать проблемы на VPN-клиентах, использующих раздельное туннелирование, а также на аппаратной части клиентского оборудования в режиме расширения сети. Используйте ASDM версии 5.0(4.3) или более поздних, чтобы избежать этих проблем. Пользователи могут получить дополнительную информацию, ознакомившись со сведениями об ошибке CSCsc10806 (только для зарегистрированных пользователей).

Дополнительные сведения

- Адаптивные устройства безопасности Cisco ASA серии 5500
- Наиболее распространенные решения проблем с L2L и IPsec VPN удаленного доступа
- Предупреждающие сообщения, поиск и устранение неполадок в адаптивных устройствах обеспечения безопасности Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация