Пример конфигурации PIX/ASA как удаленного сервера VPN с расширенной проверкой подлинности, использующего CLI ASDM

Содержание

Введение

В этом документе описан способ настройки устройства адаптивной защиты (ASA) Cisco серии 5500 для работы в качестве удаленного сервера VPN с использованием диспетчера устройств адаптивной защиты (ASDM) или командной строки. Программа ASDM предоставляет возможность качественного управления и контроля за безопасностью с помощью интуитивно понятного и простого в использовании web-интерфейса управления. Готовую конфигурацию Cisco ASA можно проверить, используя VPN-клиент Cisco.

См. PIX/ASA 7.x и Cisco VPN Client 4.x с Windows 2003 IAS RADIUS (Против Active Directory) Пример Конфигурации аутентификации для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7. x. Пользователь удаленного клиента VPN аутентифицируется против Active Directory с помощью сервера RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года.

См. PIX/ASA 7.x и Cisco VPN Client 4.x для Примера Конфигурации аутентификации Cisco

Secure ACS для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7.x использование сервера Cisco Secure Access Control Server (Версия ACS 3.2) для расширенной проверки подлинности (XAUTH).

Предварительные условия

Требования

В этом документе предполагается, что устройство адаптивной защиты полностью исправно и в нем разрешено изменение конфигурации с помощью Cisco ASDM или интерфейса командной строки.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM или PIX/ASA 7. x: Пример настройки SSH на внутреннем и внешнем интерфейсах для удаленной настройки устройства по протоколам ASDM или Secure Shell (SSH).

Используемые компоненты

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

- ПО устройств адаптивной защиты Cisco версии 7.x и более поздних версий
- Менеджер устройств адаптивной безопасности (ASDM) Версайон 5.x и позже
- Cisco VPN Client версии 4.x или выше

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.

Родственные продукты

Эти настройки также могут быть использованы в устройствах защиты Cisco PIX, начиная с версий 7.x.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Конфигурации удаленного доступа предоставляют безопасный удаленный доступ для клиентов Cisco VPN, таких как мобильные пользователи. VPN для удаленного доступа позволяет удаленным пользователям надежно обратиться к ресурсам централизованной сети. Cisco VPN Client соответствует Протоколу IPSec и специально предназначен для работы с устройством безопасности. Однако устройство безопасности может установить IP - безопасные соединения со многими совместимыми протоколом клиентами. См. Руководства по конфигурации ASA для получения дополнительной информации о IPSec.

Группы и пользователи являются базовыми понятиями в управлении безопасности VPN и в конфигурации устройства безопасности. Они задают атрибуты, которые решают, что пользователи обращаются к и использование VPN. Группа является набором пользователей, рассматриваемым как единый объект. Пользователи получают свои атрибуты от групповых политик. Туннельные группы определяют групповую политику для определенные соединения. Если вы не назначаете политику конкретной группы на пользователи, политика группы по умолчанию для соединения применяется.

Туннельная группа состоит из ряда записей, который определяет политику туннельного соединения. Эти записи определяют серверы, на которых серверы, к который туннельные пользователи аутентифицируются, а также учетные серверы, если таковые имеются, которому информация о соединениях передается. Они также identifiy политика группы по умолчанию для соединений, и они содержат определяемые протоколом параметры подключения. Туннельные группы включают небольшое количество атрибутов, который принадлежит созданию самого туннеля. Туннельные группы включают указатель на групповую политику, которая определяет ориентированные пользователями атрибуты.

Примечание: В примере конфигурации в этом документе учетные записи локального пользователя используются для аутентификации. Если требуется использовать другой сервис, такой как LDAP и RADIUS, обратитесь к Настройке Внешний сервер RADIUS для Авторизации и Аутентификации.

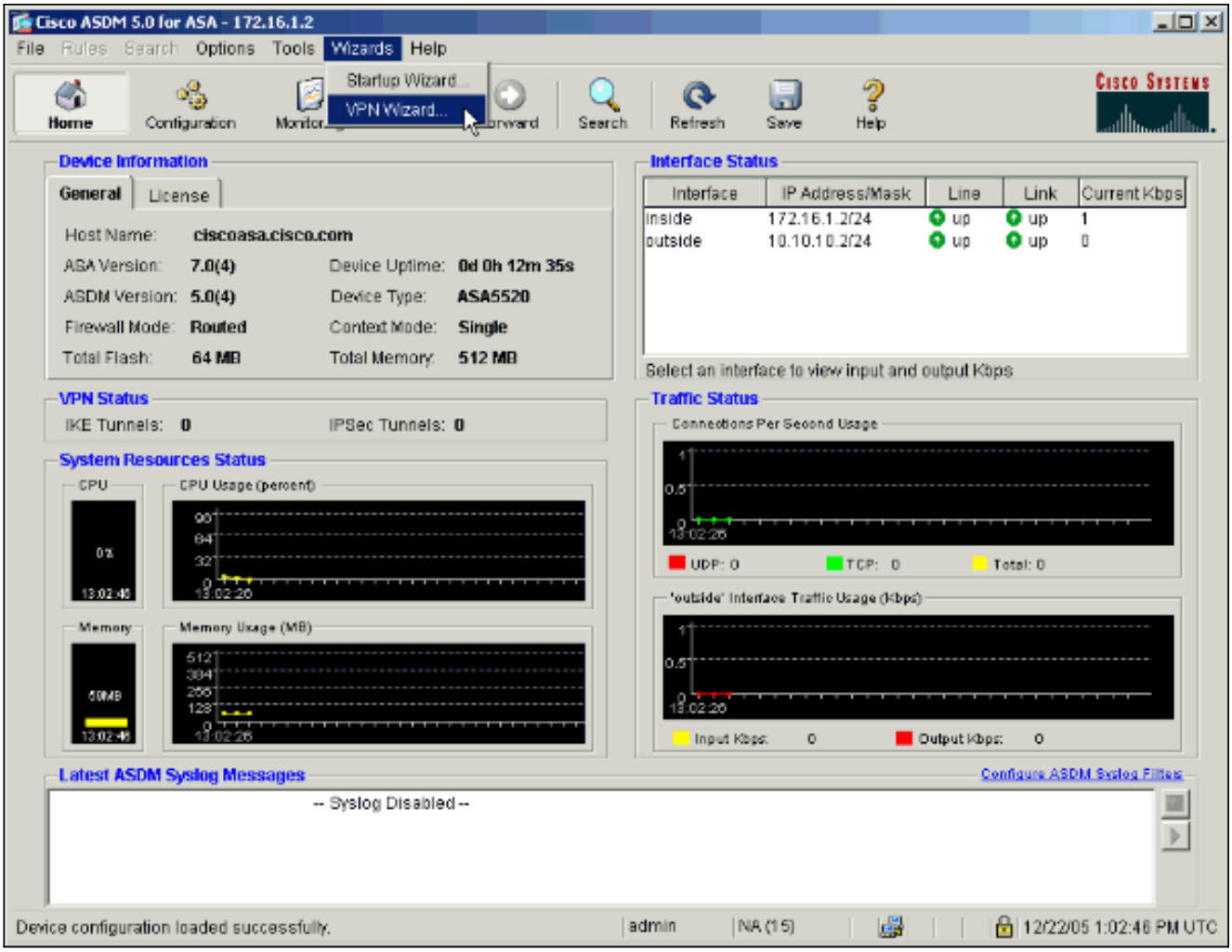
Протокол ISAKMP, также названный IKE, является протоколом согласования, о котором договариваются хосты, как создать Сопоставление безопасности IPSec. Каждое согласование ISAKMP разделено на два раздела, Phase1 и Phase2. Phase1 создает первый туннель для защиты более поздних сообщений согласования ISAKMP. Phase2 создает туннель, который защищает данные, которые перемещаются через безопасное соединение. См. Ключевые слова ПОЛИТИКИ ISAKMP для команд CLI для получения дополнительной информации о ISAKMP.

Конфигурации

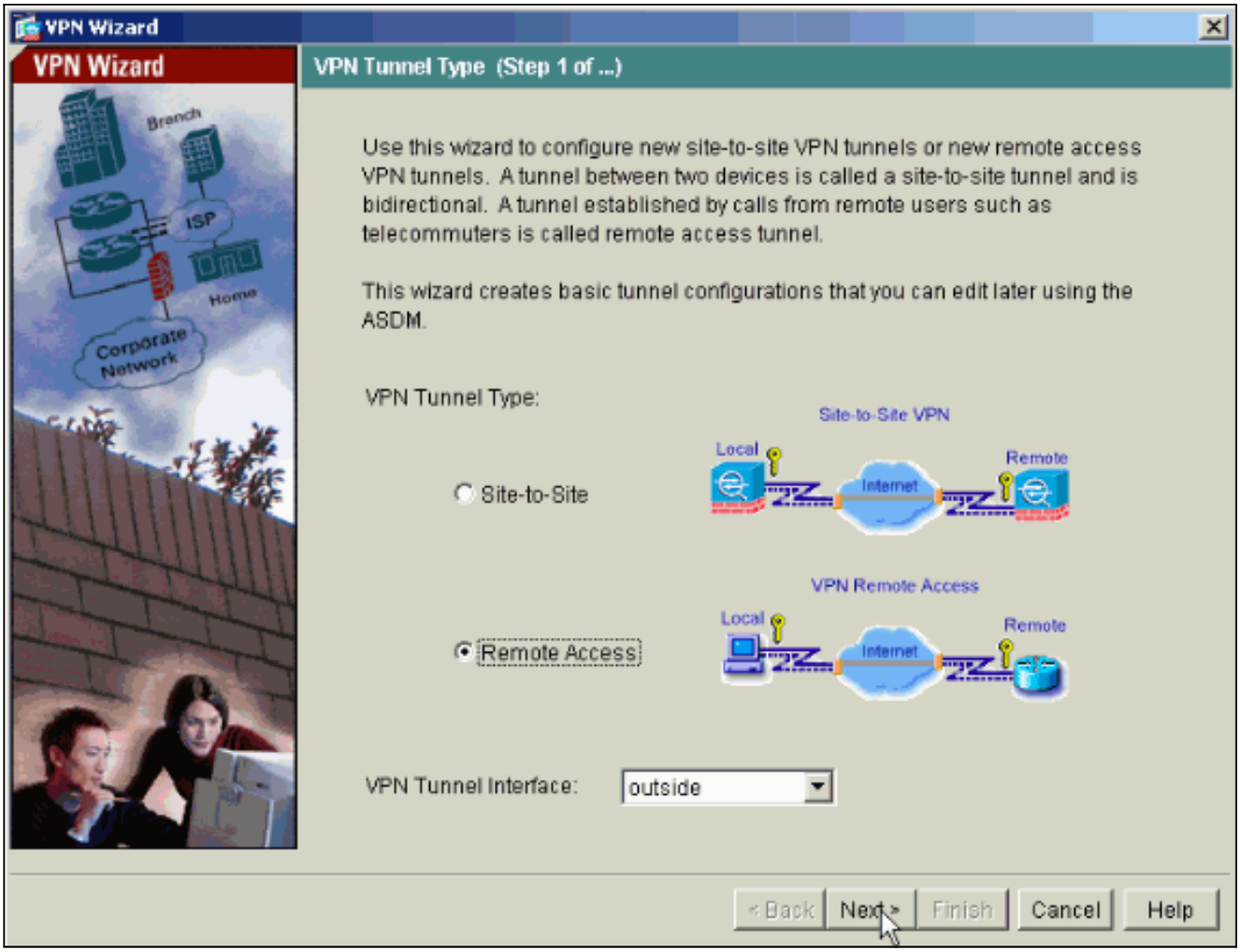
Настройте ASA/PIX как Удаленный VPN-сервер с помощью ASDM

Выполните эти шаги для настройки Cisco ASA как удаленного VPN-сервера с помощью ASDM:

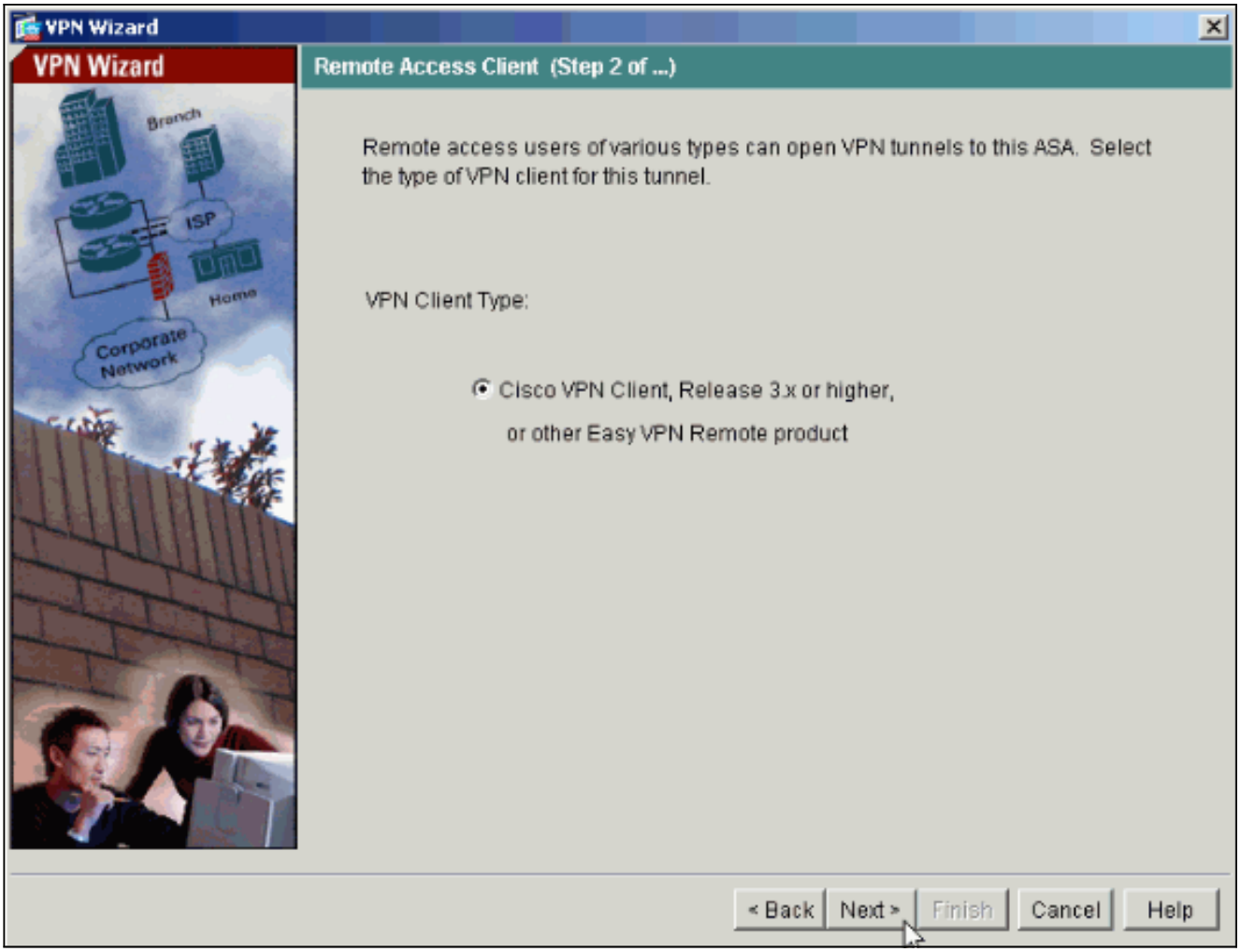
1. Выберите **Wizards> VPN Wizard** из окна Home.



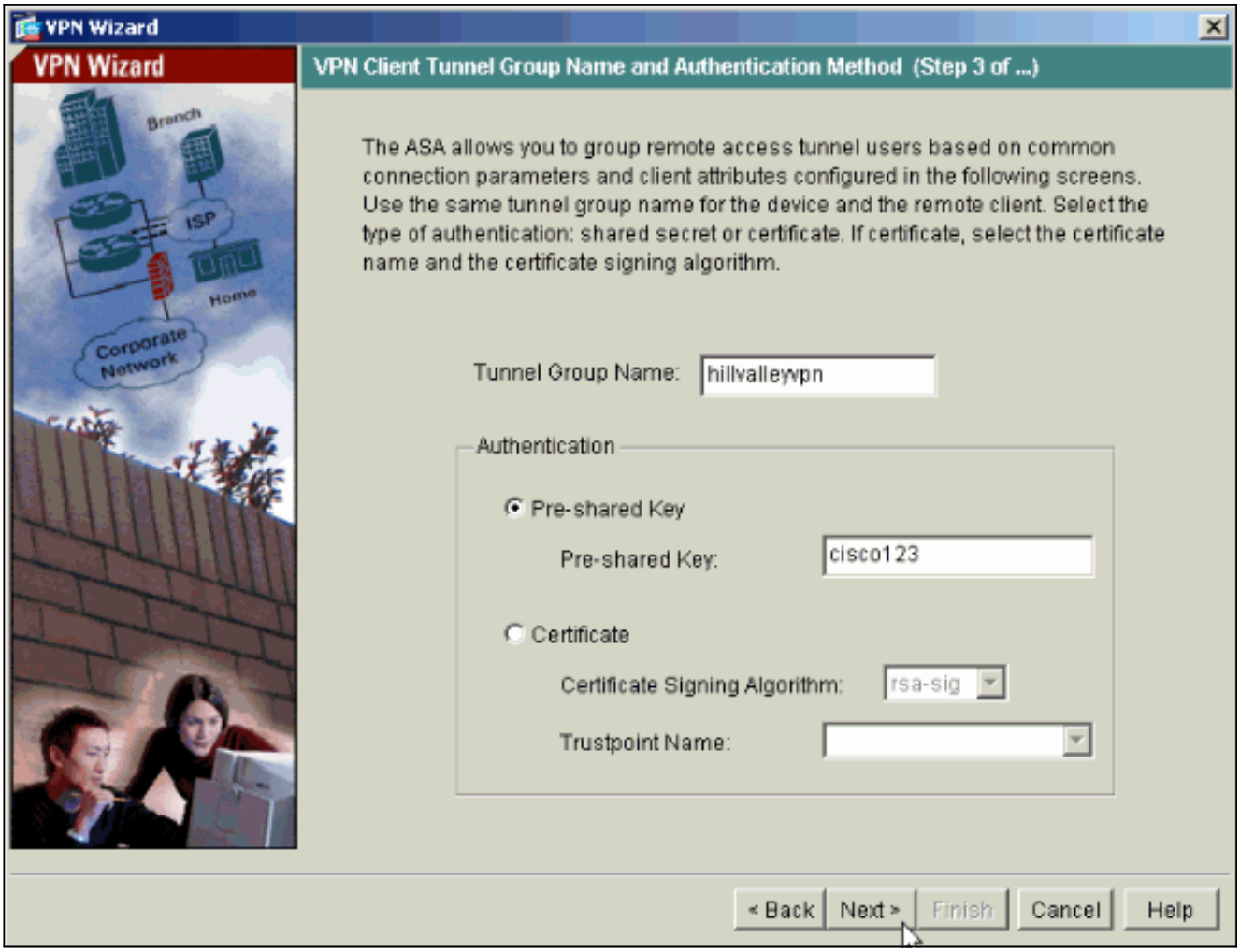
2. Выберите тип туннеля **VPN для удаленного доступа** и гарантируйте, что Интерфейс VPN-туннеля установлен, как желаемый.



3. Единственный доступный Тип Клиента VPN уже выбран. **Нажмите кнопку Next.**

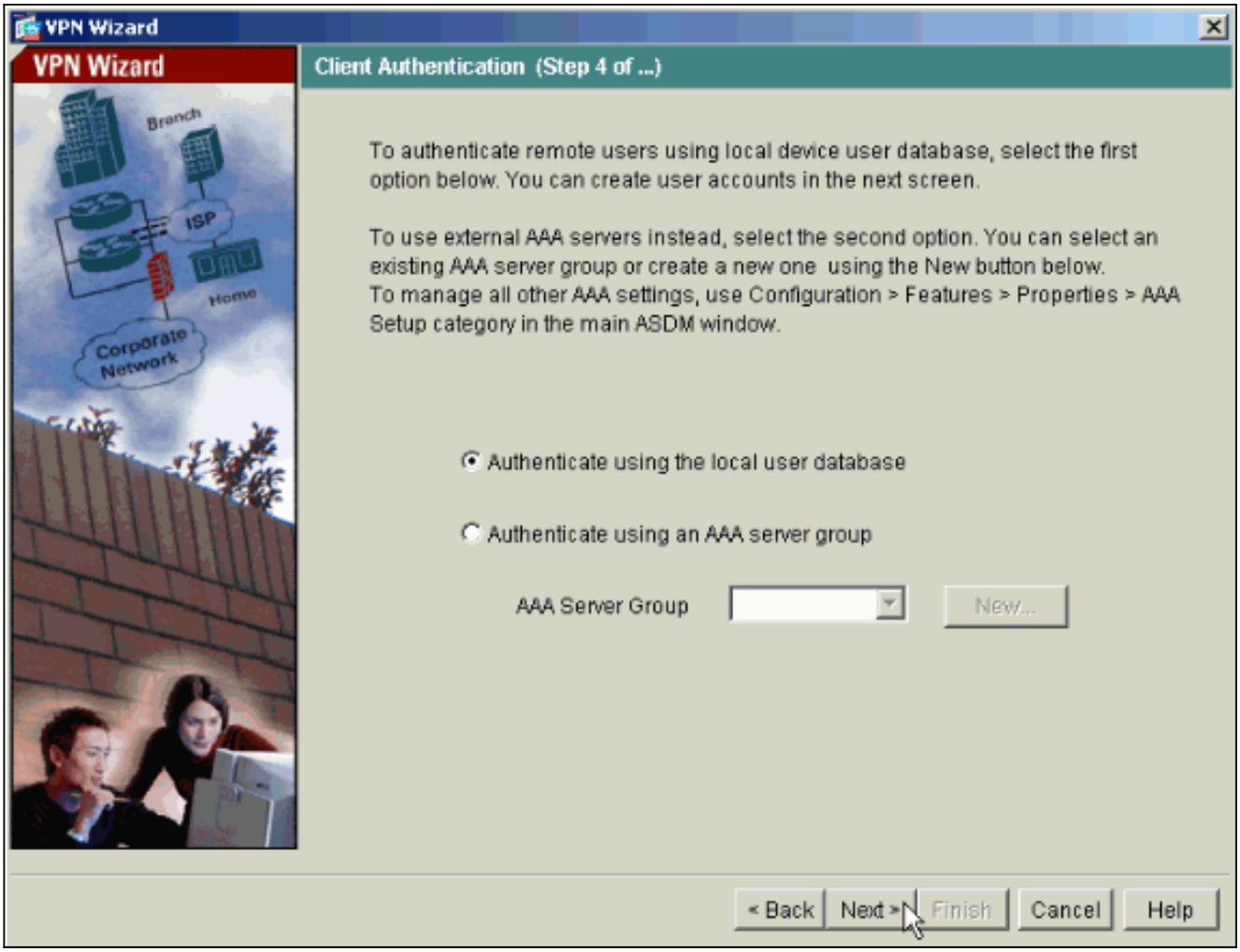


4. Введите имя группы туннеля. Предоставьте информацию для аутентификации для использования.**Предварительный общий ключ** выбран в данном примере.

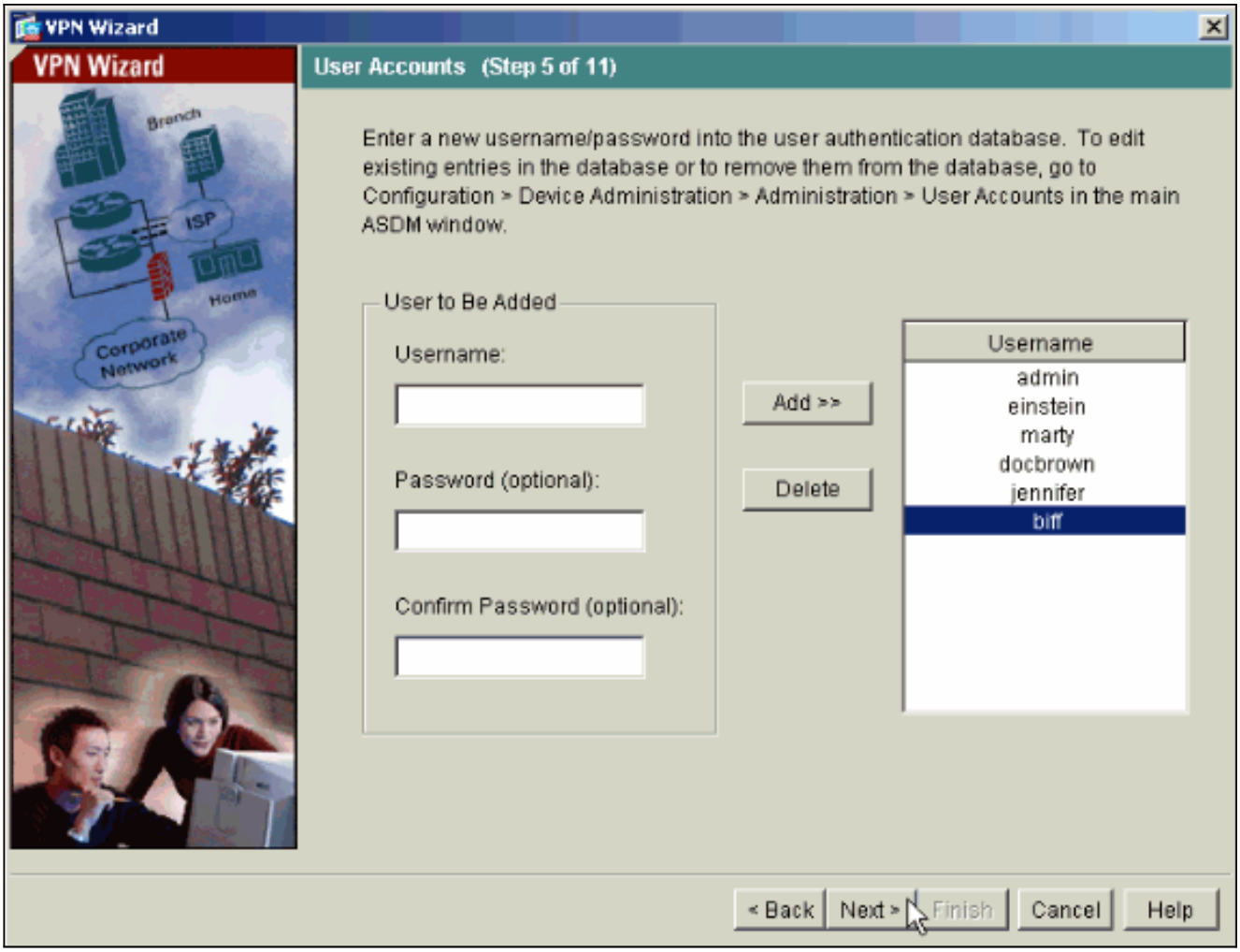


Примечание: Нет способа скрываться/шифровать предварительный общий ключ на ASDM. Причина состоит в том, что ASDM должен только использоваться людьми, которые настраивают ASA или людьми, которые помогают клиенту с этой конфигурацией.

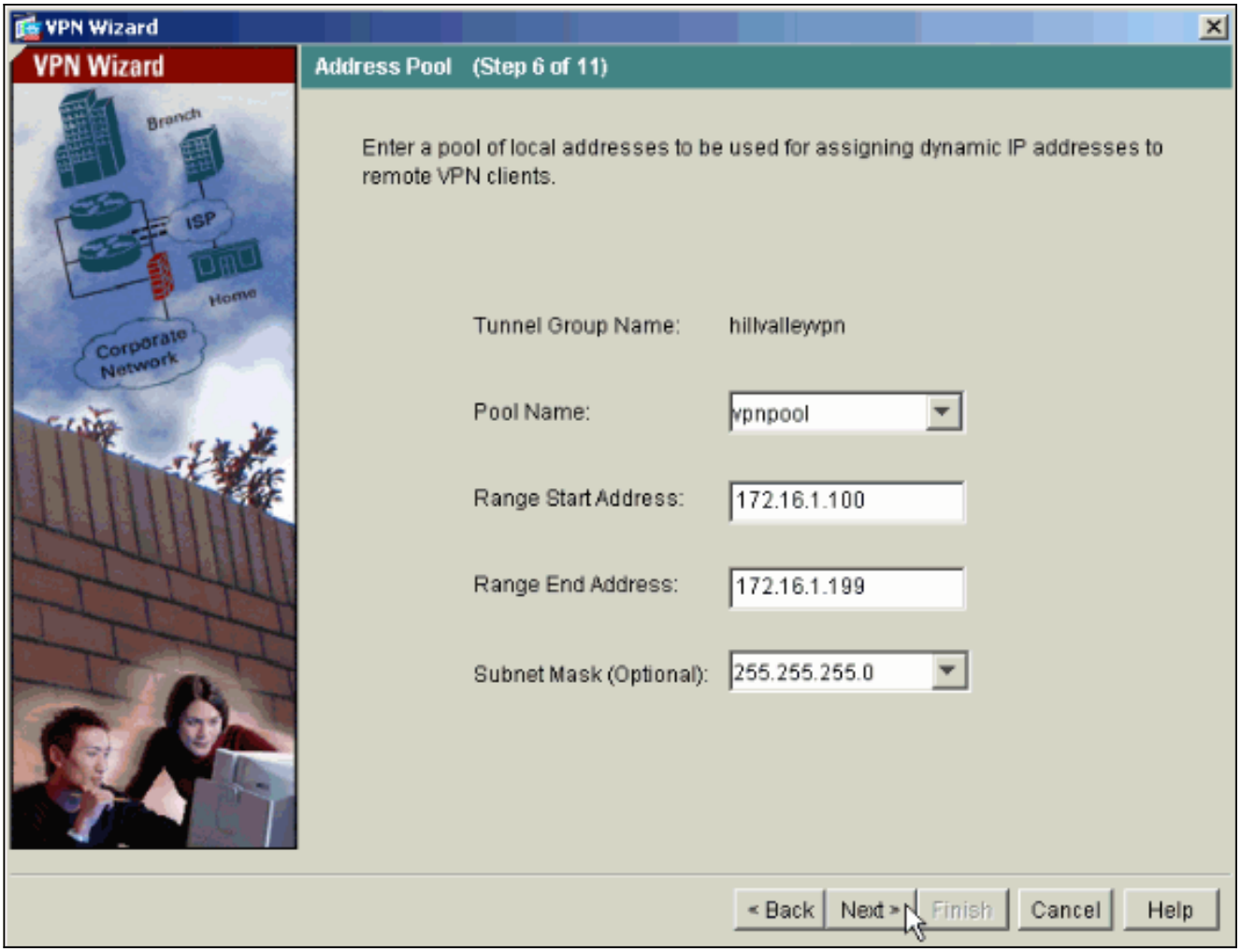
5. Выберите, хотите ли вы, чтобы удаленные пользователи аутентифицировались на базе локальных пользователей или на внешней группе AAA-серверов.**Примечание:** Вы добавляете пользователей к базе локальных пользователей в шаге 6.**Примечание:** См. PIX/ASA 7.x Группы серверов Проверки подлинности и авторизация для Пользователей VPN через Пример конфигурации ASDM для получения информации о том, как настроить внешнюю группу AAA-серверов через ASDM.



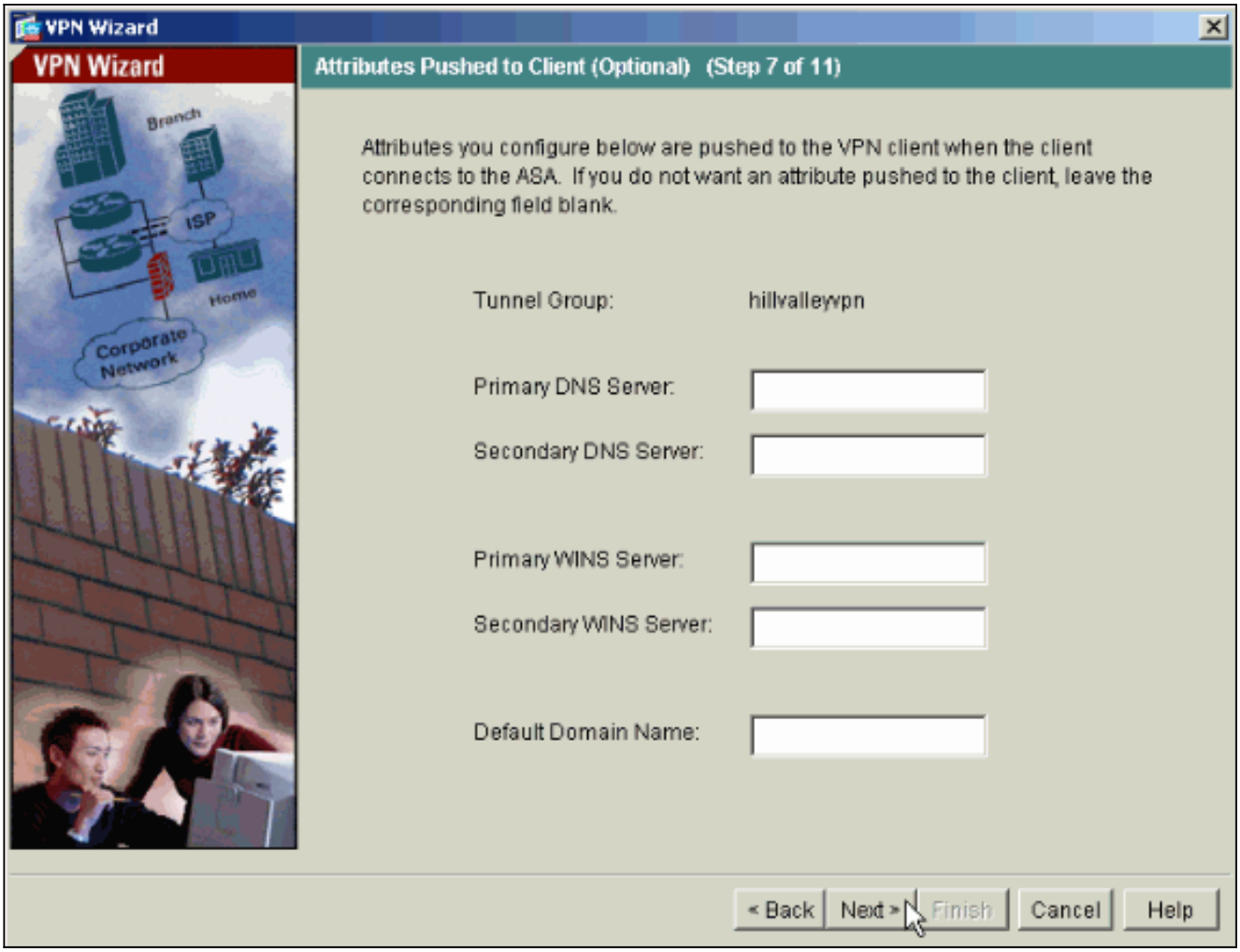
6. Добавьте пользователей к локальной базе данных при необходимости.**Примечание:** Не удаляйте существующих пользователей из этого окна. Выберите **Configuration> Device Administration> Administration> User Accounts в главном окне ASDM**, чтобы отредактировать существующие записи в базе данных или удалить их из базы данных.



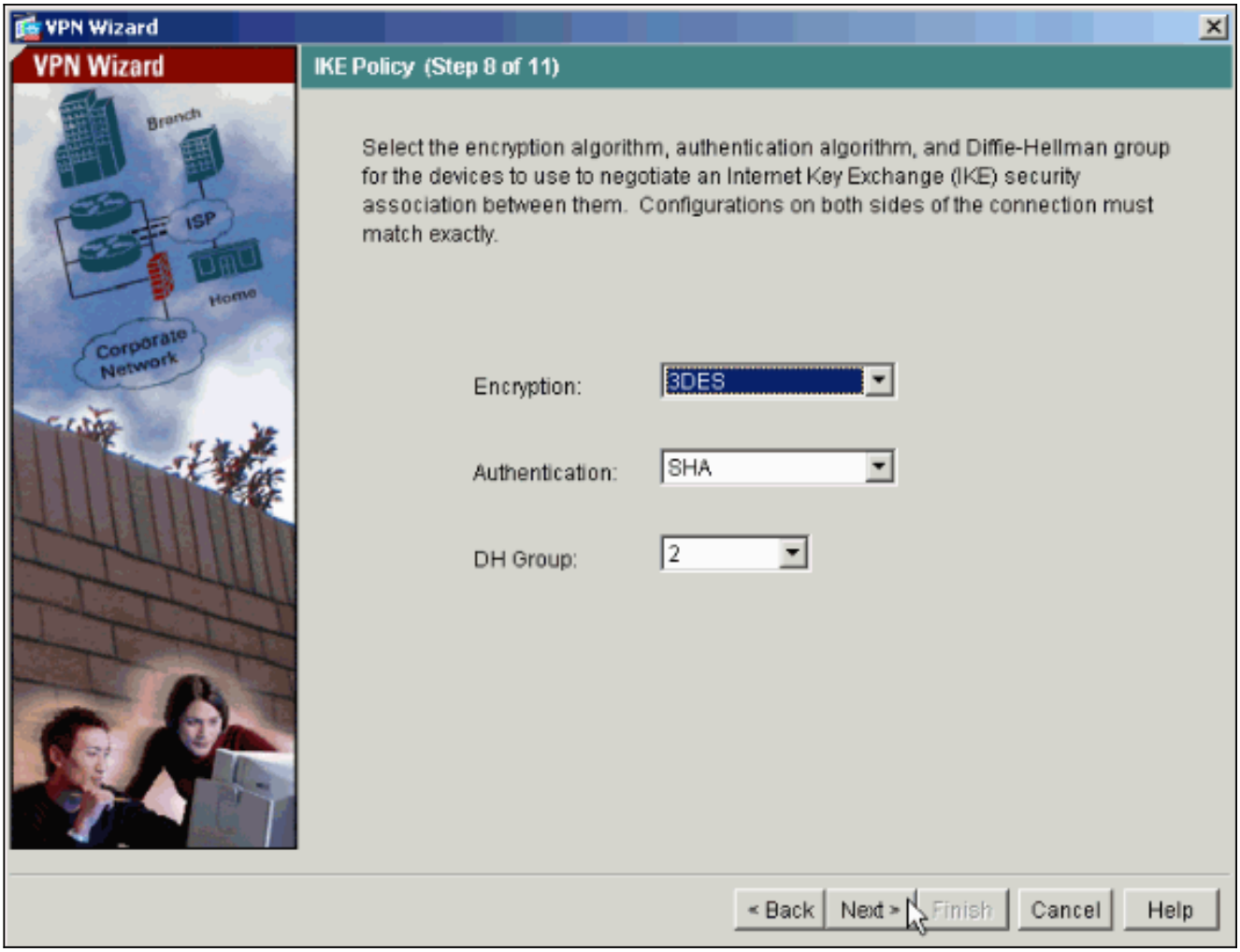
7. Определите пул локальных адресов, которые будут динамично назначены на удаленных клиентов VPN, когда они соединятся.



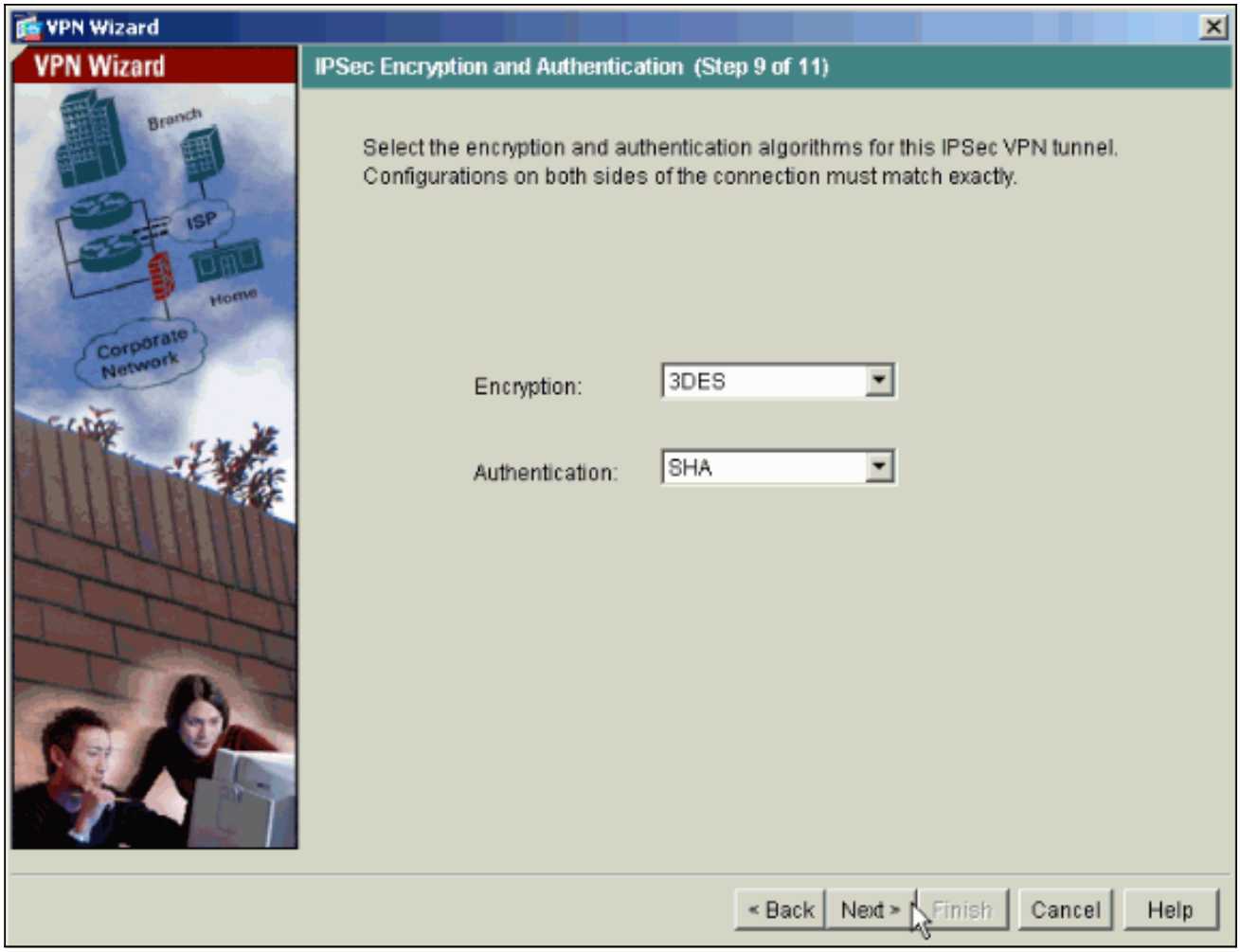
8. *Дополнительно:* Задайте DNS и информацию сервера WINS и Название Домена по умолчанию, которое будет выдвинуто к удаленным клиентам VPN.



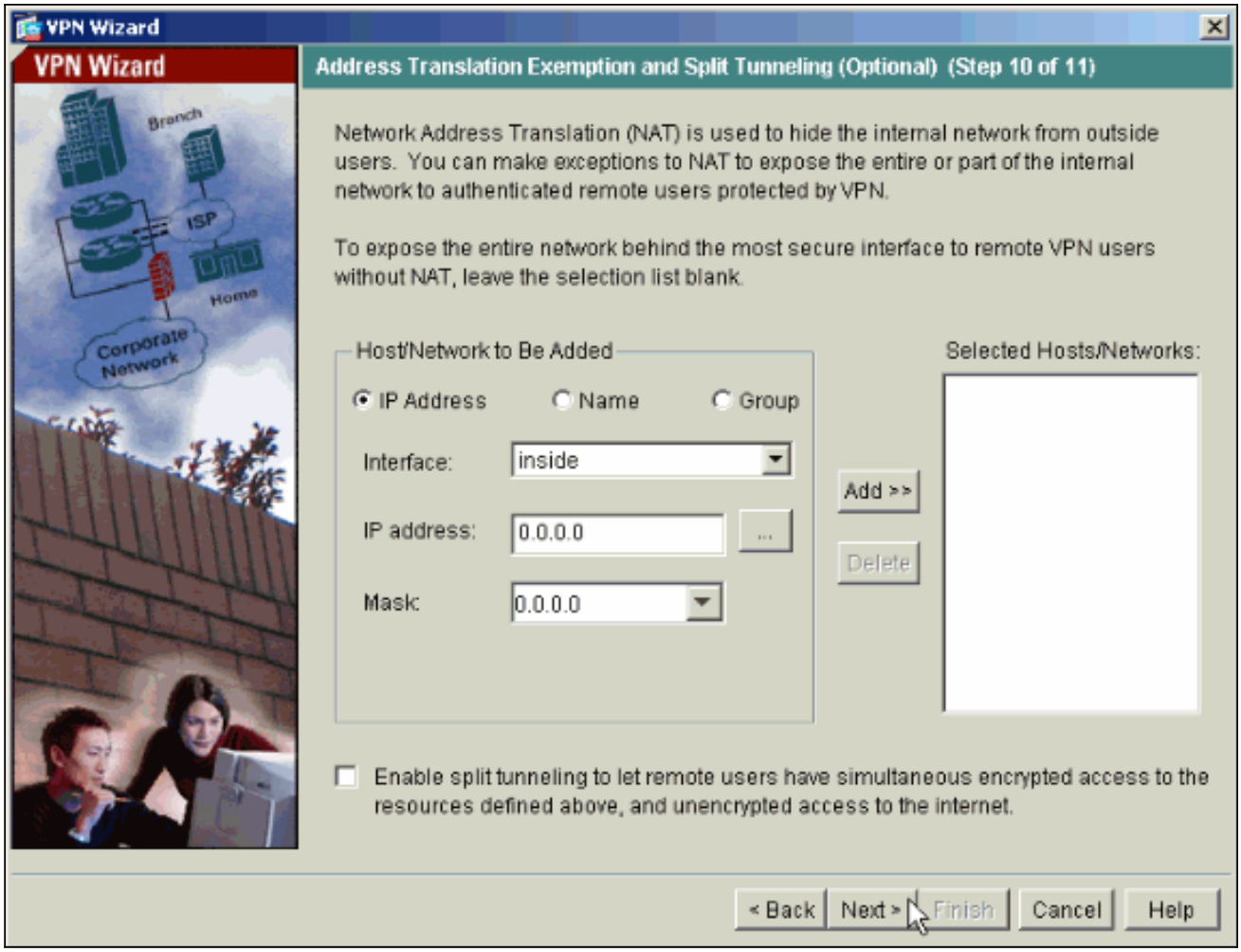
9. Задайте параметры для IKE, также известного как 1-ая фаза протокола IKE.Настройки на обеих сторонах туннеля должны точно совпадать. Тем не менее, Cisco VPN Client автоматически выбирает правильную конфигурацию для себя. Таким образом, настройка IKE для ПК клиента не
требуется.



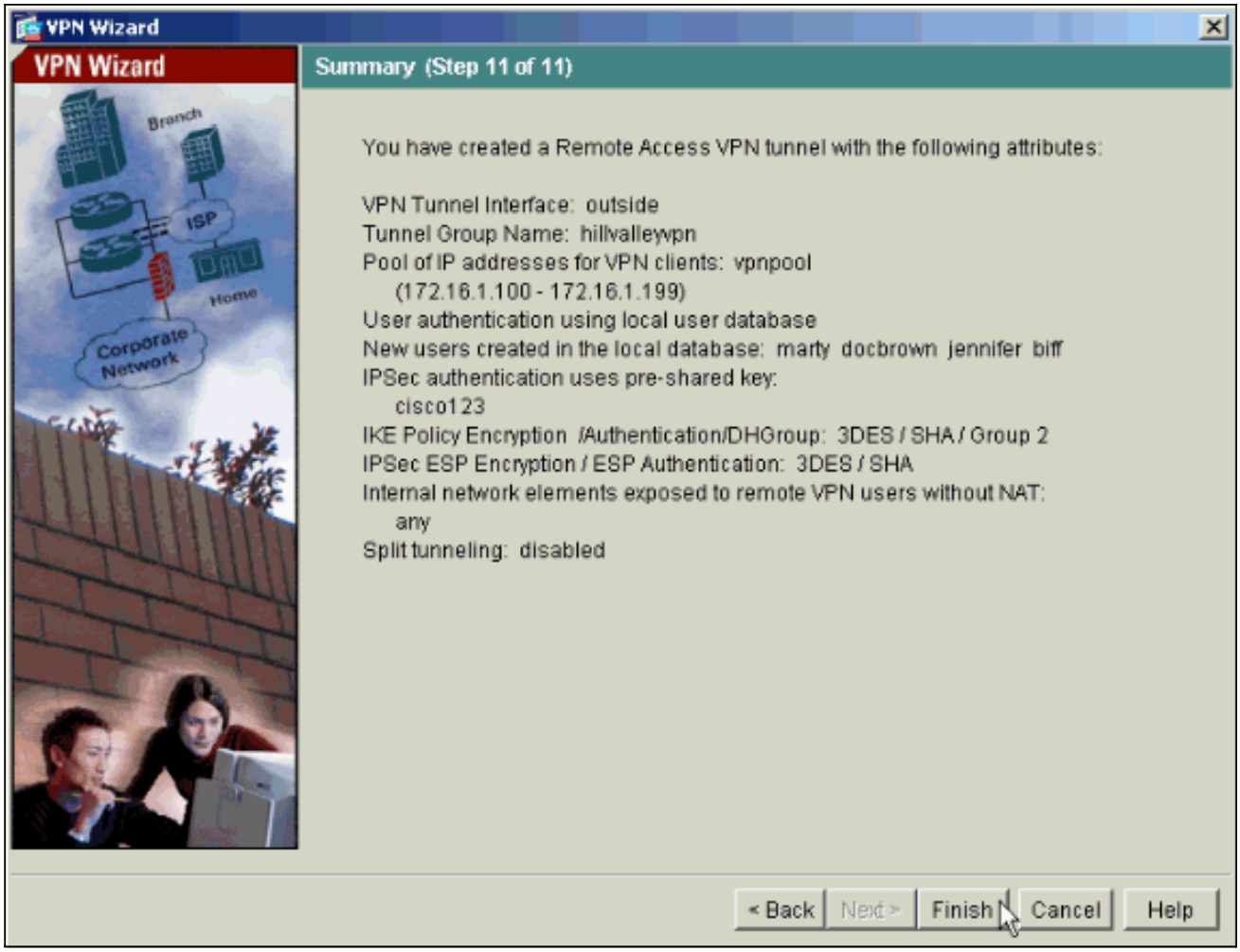
10. Задайте параметры для IPSec, также известного как 2-ая фаза протокола IKE.Настройки на обеих сторонах туннеля должны точно совпадать. Тем не менее, Cisco VPN Client автоматически выбирает правильную конфигурацию для себя. Таким образом, настройка IKE для ПК клиента не
требуется.



11. Задайте, который, если таковые имеются, внутренние хосты или сети должны быть представлены удаленным пользователям VPN.При отъезде этого списка пустым он позволяет удаленным пользователям VPN обращаться ко всей внутренней сети ASA.Можно также включить разделенное туннелирование на этом окне. Разделенное туннелирование шифрует трафик к ресурсам, определенным ранее в этой процедуре, и предоставляет дешифрованный доступ к Интернету в целом, не туннелируя тот трафик. Если разделенное туннелирование *не* включено, весь трафик от удаленных пользователей VPN туннелирован к ASA. Это может стать очень пропускной способностью и сом интенсивной загрузкой процессора, на основе вашей конфигурации.



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



Настройте ASA/PIX как Удаленный VPN-сервер с помощью CLI

Выполните эти шаги для настройки удаленного Сервера доступа VPN из командной строки. Дополнительные сведения о каждой из используемых команд см. в документах Настройка сетей VPN для удаленного доступа и Справочник по командам устройств адаптивной защиты Cisco ASA серии 5500.

1. Введите **команду ip local pool** в режим глобальной конфигурации для настройки пулов IP-адреса для использования для туннелей удаленного доступа VPN. Для удаления пулов адресов введите эту команду с параметром no.Устройство безопасности использует пулы адресов на основе туннельной группы для соединения. При настройке нескольких пулов адресов для туннельной группы устройство безопасности использует их в заказе, в котором они настроены. Выполните эту команду для создания пула локальных адресов, которые могут использоваться для присвоения динамических адресов на Клиенты VPN удаленного доступа:`ASA-AIP-CLI(config)#ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`
2. Введите следующую команду:`ASA-AIP-CLI(config)#username marty password 12345678`
3. Выполните этот набор команд для настройки определенного туннеля:CLI AIP ASA (config) **#isakmp политика 1 authentication pre-share**CLI AIP ASA (config) **#isakmp политика 1 шифрование 3des**CLI AIP ASA (config) **#isakmp политика 1 хэш sha**CLI AIP ASA (config) **#isakmp политика 1 группа 2**CLI AIP ASA (config) **#isakmp политика 1 срок действия 43200**CLI AIP ASA (config) **#isakmp включает снаружи**CLI AIP ASA (config) **#crypto transform-set ipsec ESP-3DES-SHA особенно-3des esp-sha-hmac**CLI AIP ASA (config) **#crypto set transform-set outside_dyn_map 10 динамической схемы ESP-3DES-**

SHACLI AIP ASA (config) **#crypto set reverse-route outside_dyn_map 10 динамической схемы**CLI AIP ASA (config) **#crypto секунды outside_dyn_map 10 set security-association lifetime динамической схемы 288000**CLI AIP ASA (config) **#crypto сопоставляет isakmp ipsec outside_map 10 динамический outside_dyn_map**CLI AIP ASA (config) **#crypto сопоставляет интерфейс outside_map снаружи**CLI AIP ASA (config) **#crypto туземный обход isakmp**

4. *Дополнительно:* Если вы хотели бы, чтобы соединение обошло access-list, который применен к интерфейсу, выполните эту команду:`ASA-AIP-CLI(config)#` **`sysopt connection permit-ipsec`** **Примечание:** Эта команда продолжает работать 7.x образы прежде 7.2 (2). При использовании образ 7.2 (2), выполняете `CLI AIP ASA (config) #sysopt permit-vpn .`
5. Введите следующую команду:`ASA-AIP-CLI(config)#` **`group-policy hillvalleyvpn internal`**
6. Выполните эти команды для настройки параметров настройки клиентского соединения:CLI AIP ASA (config) **#group-policy hillvalleyvpn атрибуты**CLI AIP ASA (config) # (групповая политика config) **#dns-server оценивает 172.16.1.11**CLI AIP ASA (config) # (групповая политика config) **#vpn-tunnel-protocol IPSec**CLI AIP ASA (config) # (групповая политика config) **#default-domain оценивает test.com**
7. Введите следующую команду:`ASA-AIP-CLI(config)#` **`tunnel-group hillvalleyvpn ipsec-ra`**
8. Введите следующую команду:`ASA-AIP-CLI(config)#` **`tunnel-group hillvalleyvpn ipsec-attributes`**
9. Введите следующую команду:`ASA-AIP-CLI(config-tunnel-ipsec)#` **`pre-shared-key cisco123`**
10. Введите следующую команду:`ASA-AIP-CLI(config)#` **`tunnel-group hillvalleyvpn general-attributes`**
11. Выполните эту команду для обращения базы локальных пользователей для аутентификации.`ASA-AIP-CLI(config-tunnel-general)#` **`authentication-server-group LOCAL`**
12. Привяжите групповую политику к туннельной группе`ASA-AIP-CLI(config-tunnel-ipsec)#` **`default-group-policy hillvalleyvpn`**
13. Выполните эту команду, в то время как в режиме общих атрибутов hillvalleyvpn туннельной группы для присвоения vpnpool создал в шаге 1 в hillvalleyvpn группу.`ASA-AIP-CLI(config-tunnel-general)#` **`address-pool vpnpool`**

Выполнение Config 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
default-group-policy hillvalleyvpn 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 пароля Cisco VPN Client

Если у вас есть многочисленные клиенты Cisco VPN, очень трудно помнить все имена пользователя и пароли Клиента VPN. Для хранения паролей в машине Клиента VPN настройте ASA/PIX и Клиент VPN, как этот раздел описывает.

ASA/PIX

Используйте **команду group-policy attributes** в режиме глобальной конфигурации:

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

Cisco VPN Client

Отредактируйте **файл .pcf** и модифицируйте эти параметры:

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

Отключите расширенную проверку подлинности

В режиме туннельной группы введите эту команду для отключения расширенной проверки подлинности, которая включена по умолчанию на PIX/ASA 7. x:

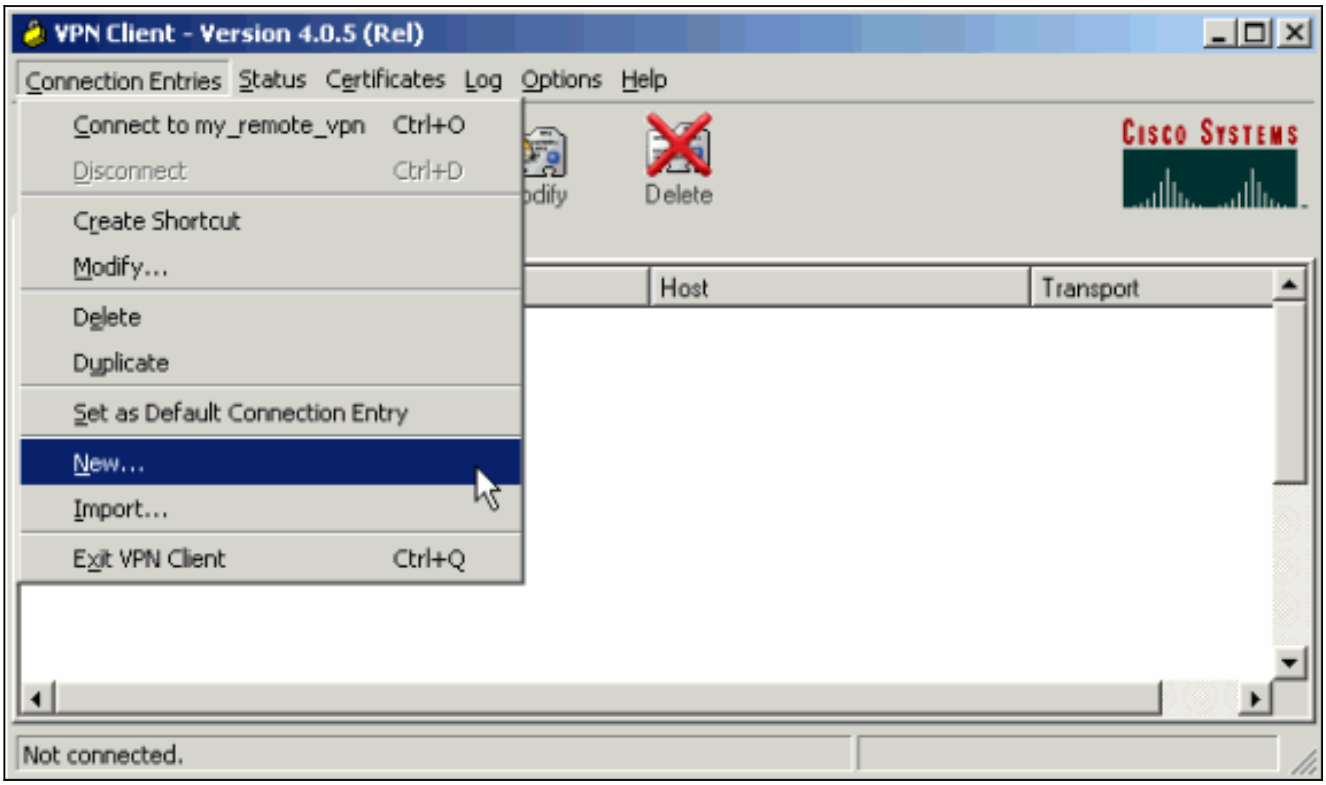
```
asa(config)#tunnel-group client ipsec-attributes asa(config-tunnel-ipsec)#isakmp ikev1-user-
authentication none
```

После отключения расширенной проверки подлинности Клиенты VPN не всплывают имя пользователя/пароль для аутентификации (Xauth). Поэтому ASA/PIX не требует, чтобы конфигурация имени пользователя и пароля аутентифицировала Клиенты VPN.

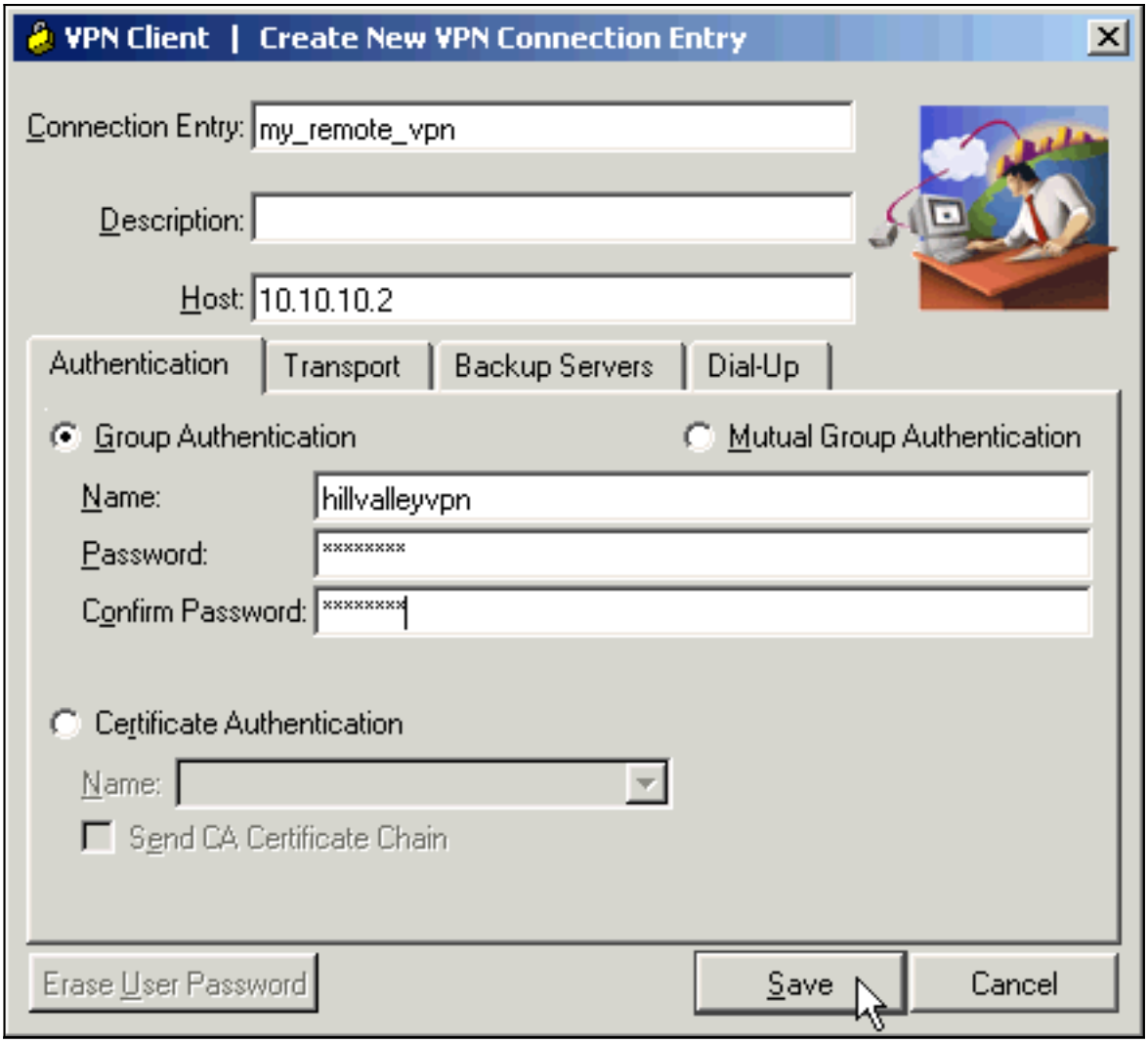
Проверка

Попытайтесь соединиться с Cisco ASA с помощью Cisco VPN Client, чтобы проверить, что успешно настроен ASA.

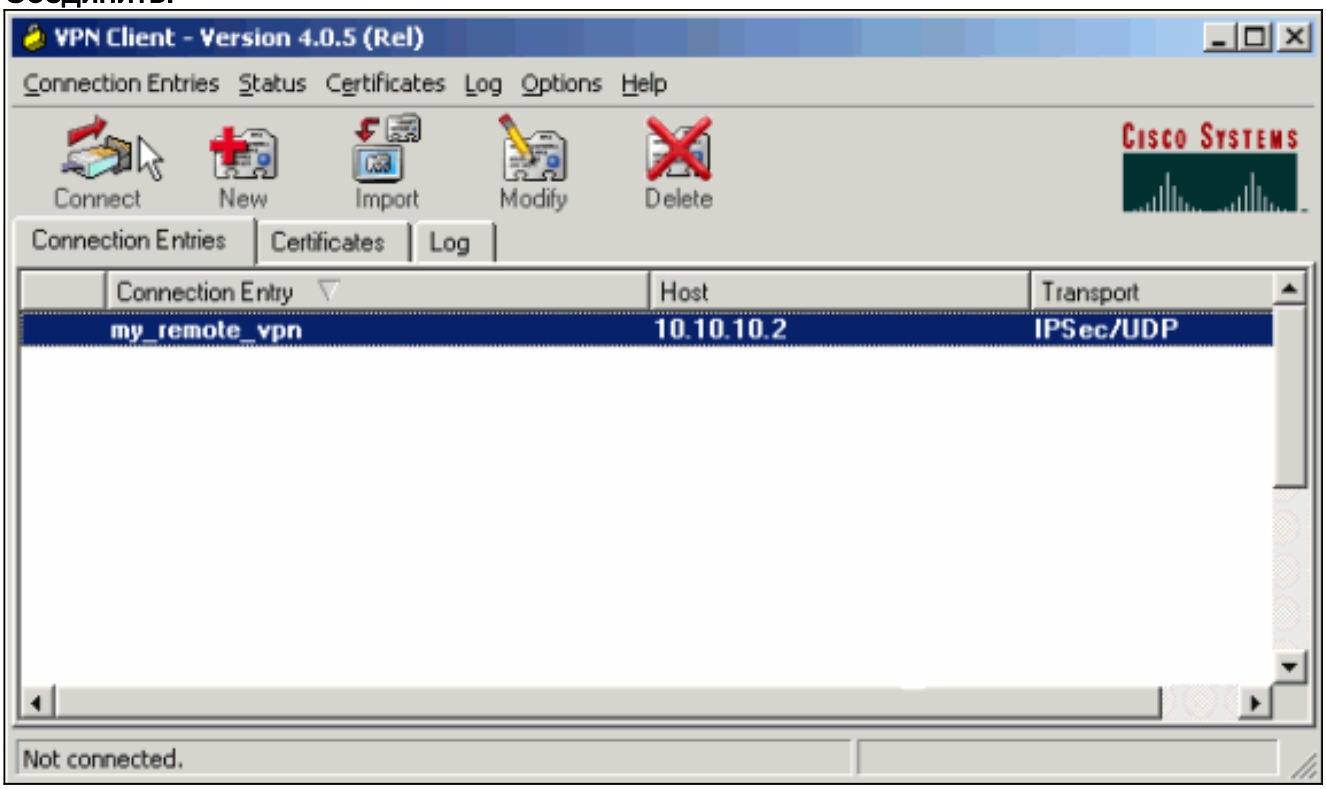
1. **Выберите Connection Entries > New.**



2. Введите данные нового подключения.Поле Host должно содержать IP-адрес или имя хоста ранее настроенного Cisco ASA. Информация о Групповой аутентификации должна соответствовать используемому в шаге 4. Нажмите **Save**, когда вы будете закончены.



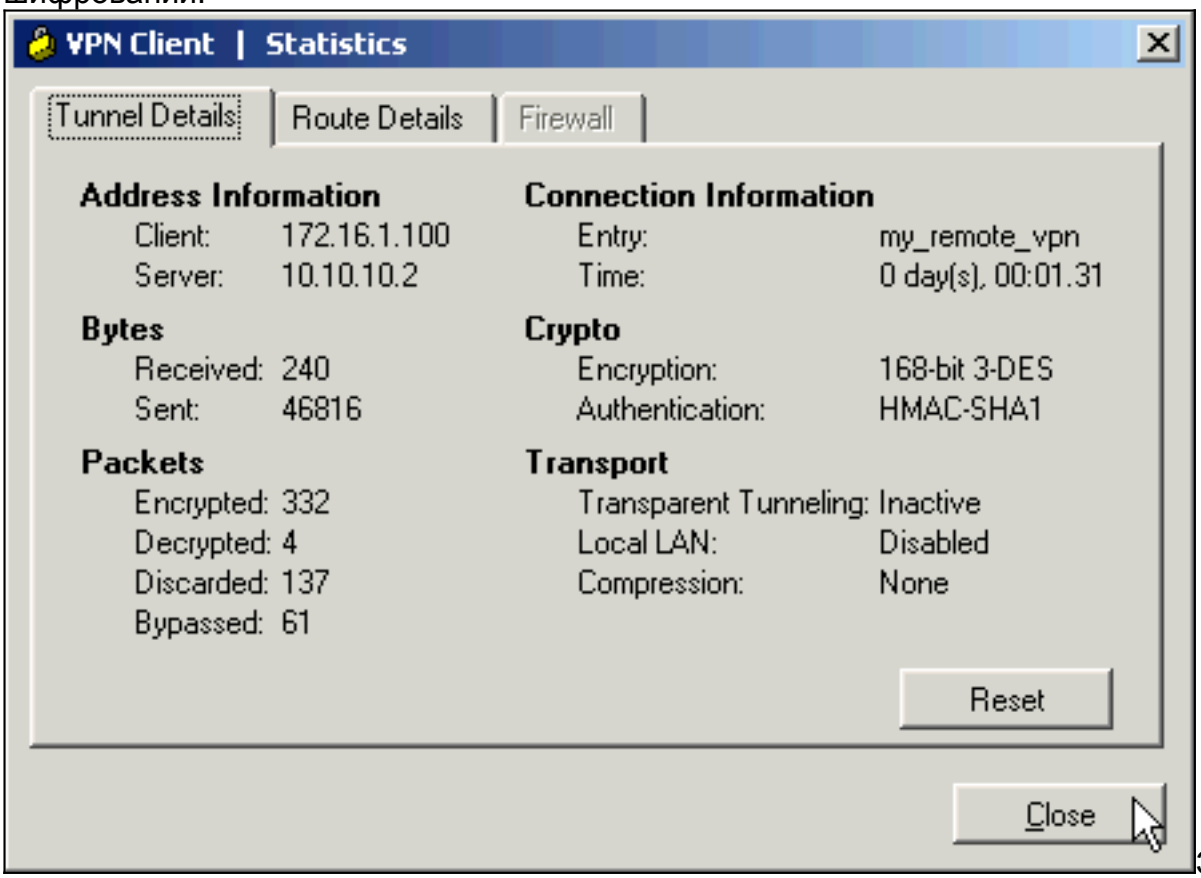
3. **Выберите только что созданное подключение и нажмите Соединить.**



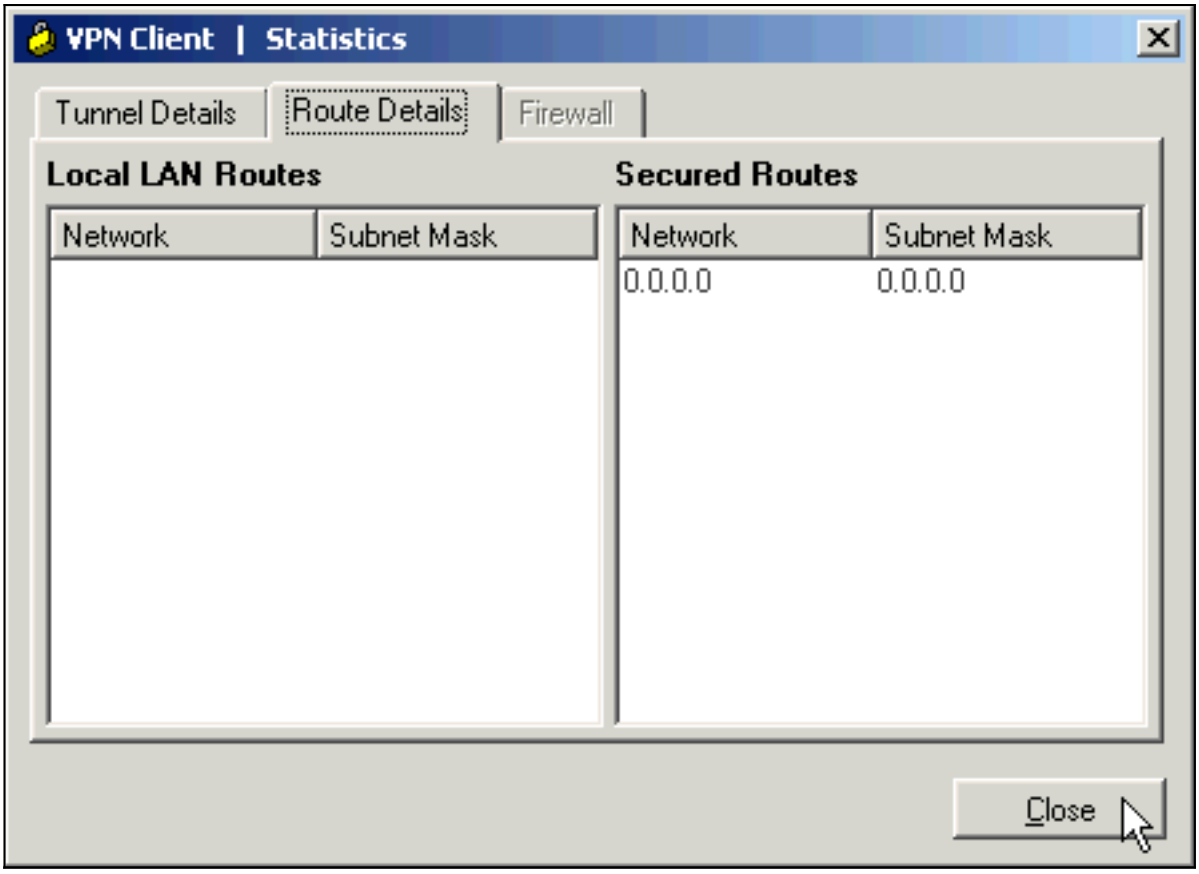
4. Введите имя пользователя и пароль для расширенной проверки подлинности. Эта информация должна совпасть, это задало в [шагах 5 и]

6.

5. **После успешного установления соединения выберите пункт Статистика в меню Status ("Состояние"), чтобы проверить данные туннеля.**В этом окне показана информация о трафике и
шифровании:



Это окно показывает информацию о разделенном
туннелировании:



Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Неправильный крипто-ACL

ASDM 5.0 (2), как известно, создает и применяет крипто-список контроля доступа (ACL), который может вызвать проблемы для Клиентов VPN, которые используют разделенное туннелирование, а также для аппаратных клиентов в режиме расширения сети. Используйте версию 5.0 (4.3) ASDM или позже избежать этой проблемы. См. идентификатор ошибки Cisco CSCsc10806 (только зарегистрированные клиенты) для получения дополнительной информации.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- Устранение неполадок и работа с оповещениями устройств адаптивной защиты Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация