ASA/PIX: Удаленный VPN-сервер с входящим NAT для трафика клиента VPN с CLI и примером конфигурации ASDM

Содержание

Введение

Этот документ описывает настройку устройства адаптивной защиты Cisco ASA серии 5500 для работы в качестве удаленного сервера VPN с использованием диспетчера устройств адаптивной защиты (ASDM) или командной строки и преобразования входящего трафика VPN-клиентов посредством NAT. Программа ASDM предоставляет возможность качественного управления и контроля за безопасностью с помощью интуитивно понятного и простого в использовании web-интерфейса управления. Как только конфигурация Cisco ASA завершена, она может быть проверена через Cisco VPN Client.

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. ASA, как также предполагается, настроен для Исходящего NAT. См. Позволяют Доступ для внутренних узлов Внешним сетям с использованием PAT для получения дополнительной информации о том, как настроить Исходящий NAT.

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
- Версия 5.x Менеджера устройств адаптивной безопасности (ASDM) 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 определенных соединений. Если вы не назначаете политику конкретной группы на пользователей, политика группы по умолчанию для соединения применяется.

Туннельная группа состоит из ряда записей, который определяет политику туннельного соединения. Эти записи определяют серверы, на которых туннельные пользователи аутентифицируются, а также учетные серверы, если таковые имеются, которому информация о соединении передается. Они также identifiy политика группы по умолчанию для соединений, и они содержат определяемые протоколом параметры подключения.

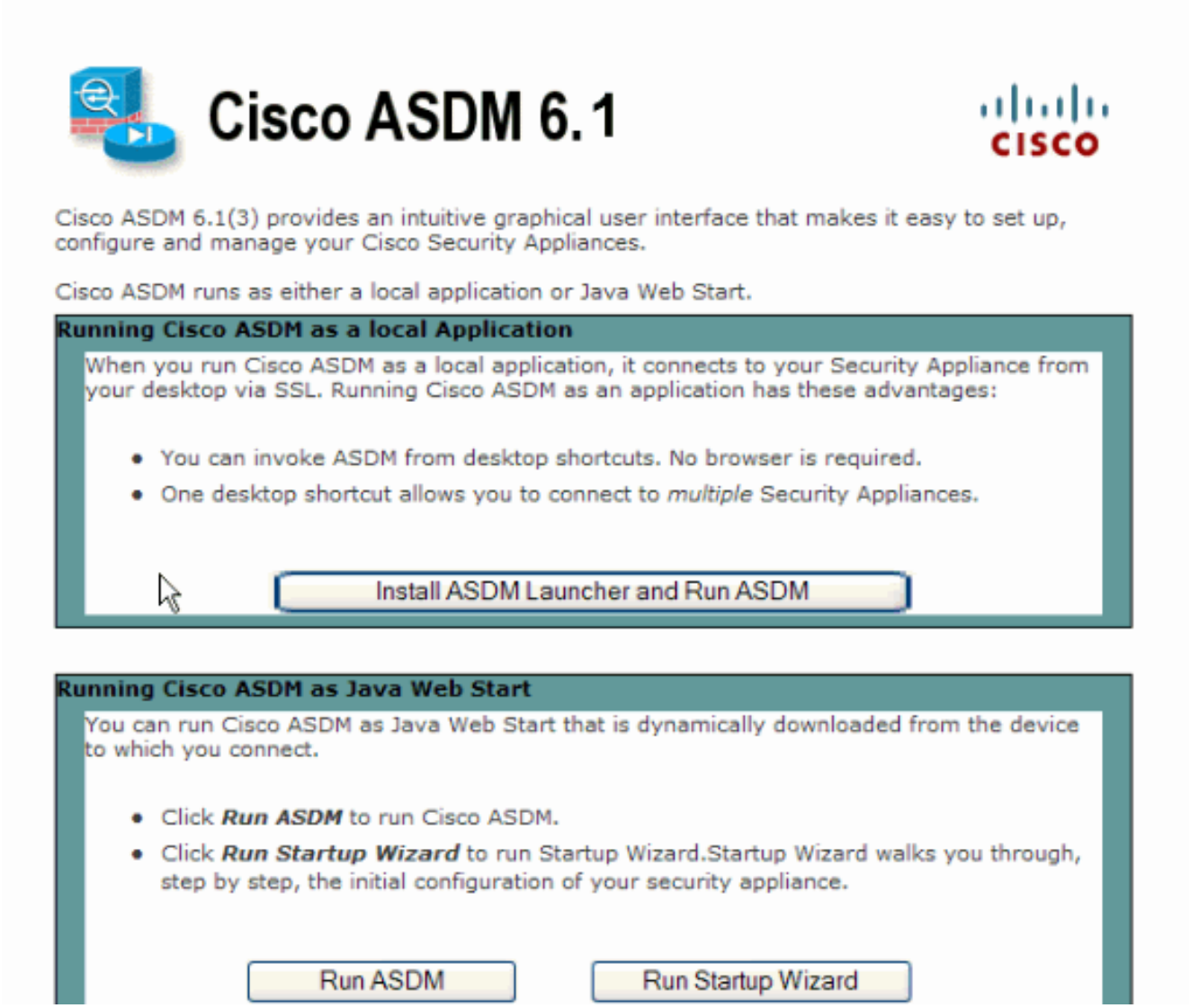
Туннельные группы включают небольшое количество атрибутов, которые принадлежат созданию самого туннеля. Туннельные группы включают указатель на групповую политику, которая определяет ориентированные пользователями атрибуты.

Конфигурации

Настройте ASA/PIX как Удаленный VPN-сервер с ASDM

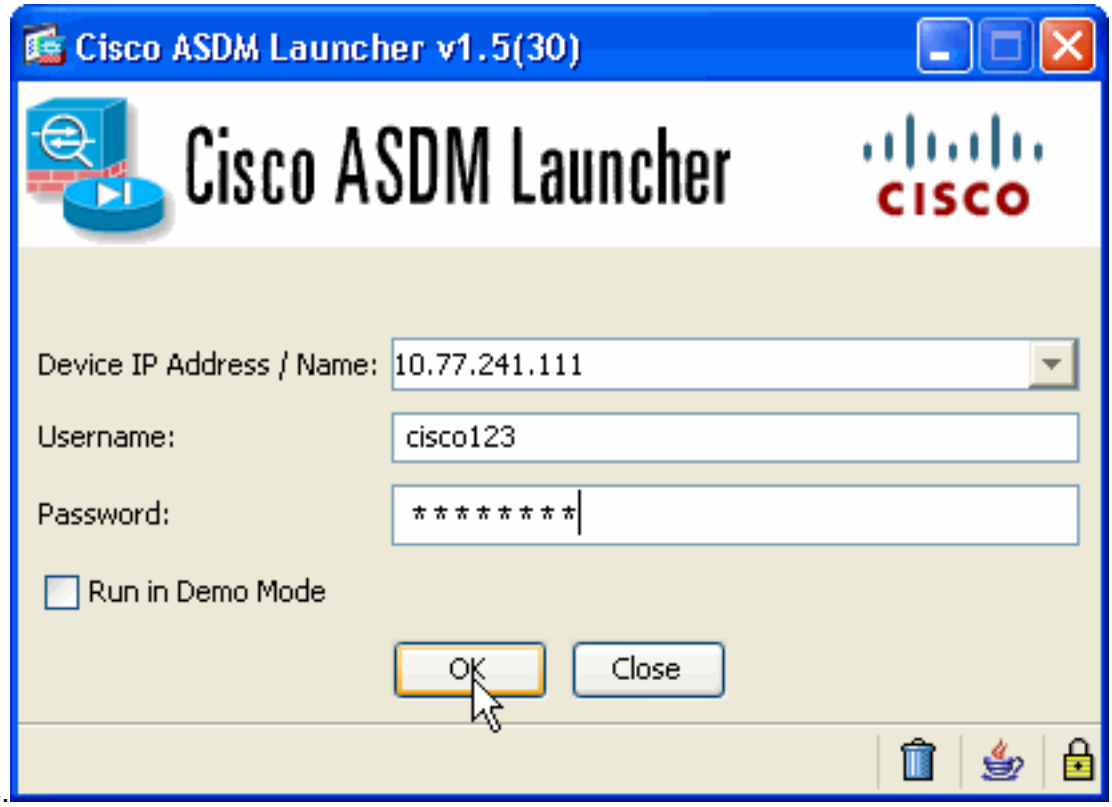
Выполните эти шаги для настройки Cisco ASA как удаленного VPN-сервера с ASDM:

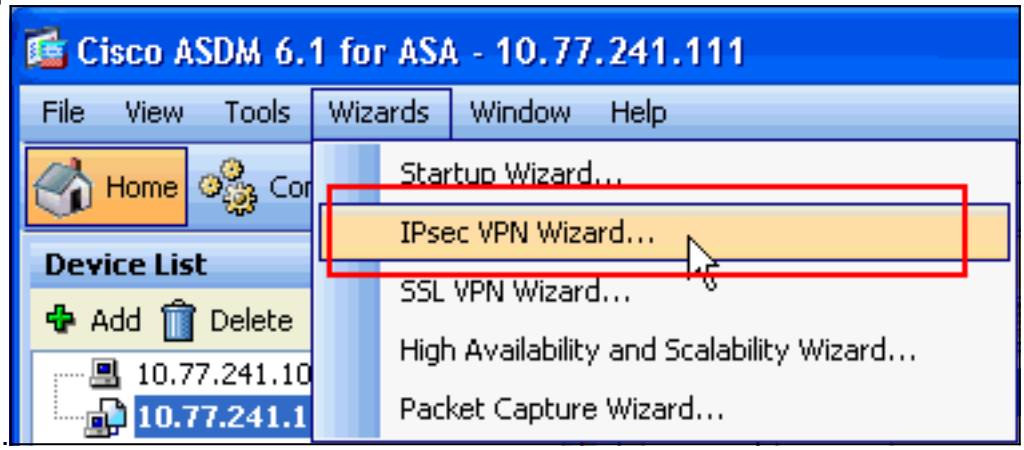
1. Откройте свой браузер и введите **https://<IP_Address интерфейса ASA, который был настроен для Доступа ASDM>** для доступа к ASDM на ASA.Отвечайте на все предупреждения, связанные с проверкой SSL-сертификата, выдаваемые браузером. По умолчанию имя пользователя и пароль являются пустыми.ASA отобразит следующее окно для загрузки приложения ASDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение Java.



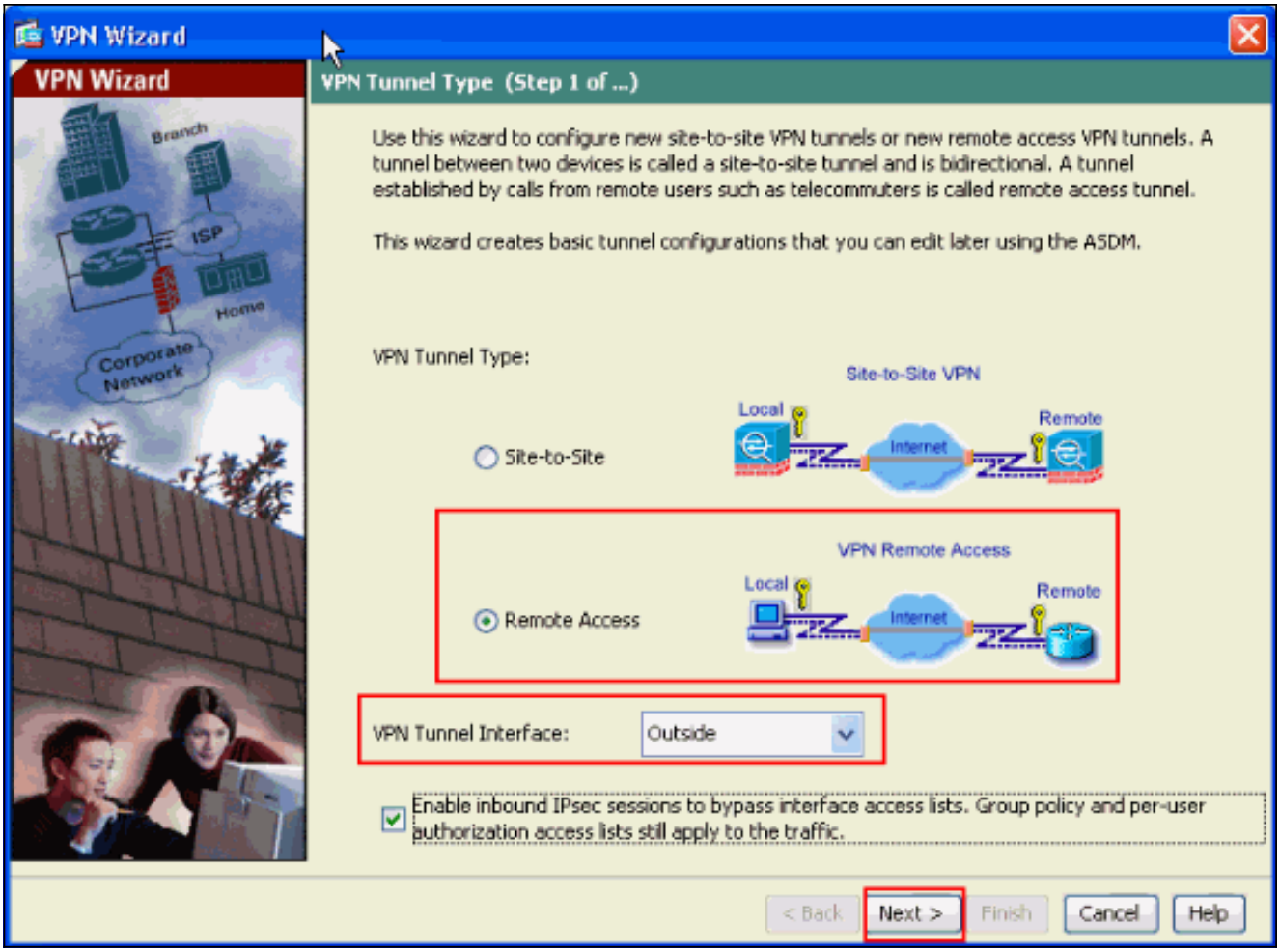
2. **Нажмите кнопку Download ASDM Launcher and Start ASDM, чтобы загрузить файл установки приложения ASDM.**
3. После загрузки ASDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска

Cisco ASDM Launcher.

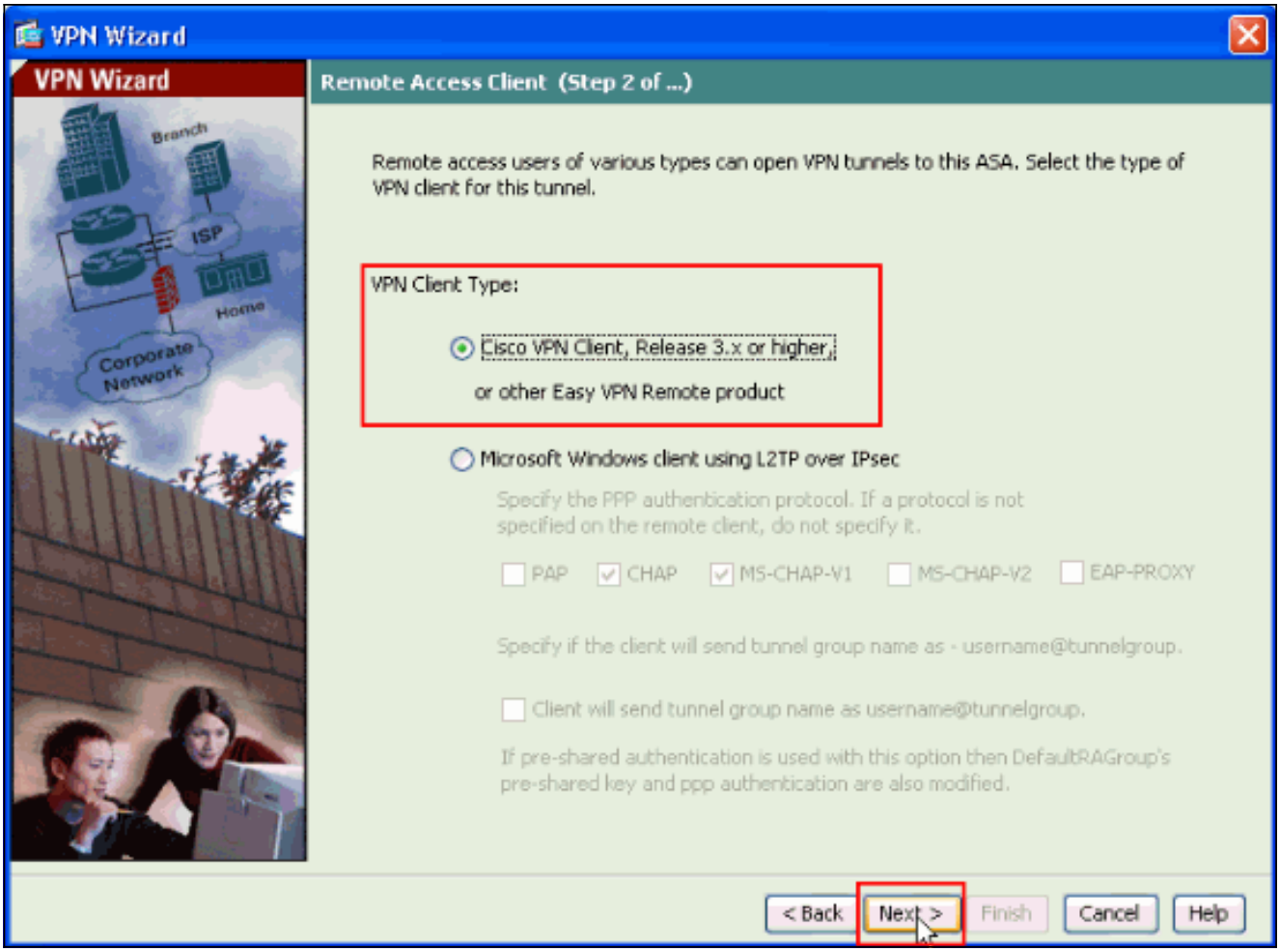
4. **Введите в поле Device IP Address IP-адрес настроенного интерфейса с помощью команды http -, а также имя пользователя (в поле Username) и пароль (в поле Password), если они были заданы.**Данный пример использует **cisco123** в качестве имени пользователя и **cisco123** как пароль. 

5. Выберите **Wizards> IPsec VPN Wizard** из окна Home. 

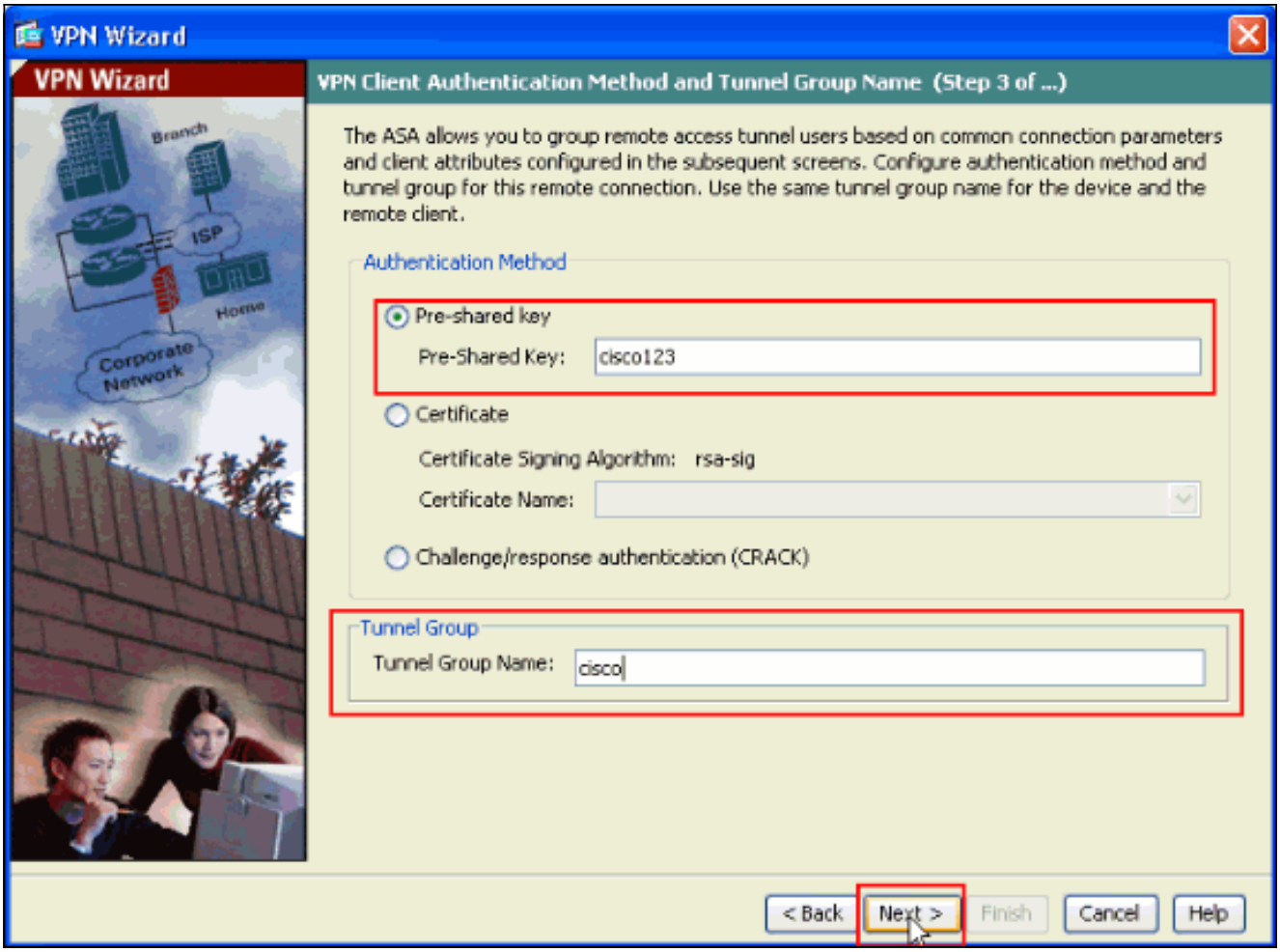
6. Выберите тип туннеля **VPN для удаленного доступа** и гарантируйте, что Интерфейс VPN-туннеля установлен, как желаемый, и нажмите **Next** как показано здесь.



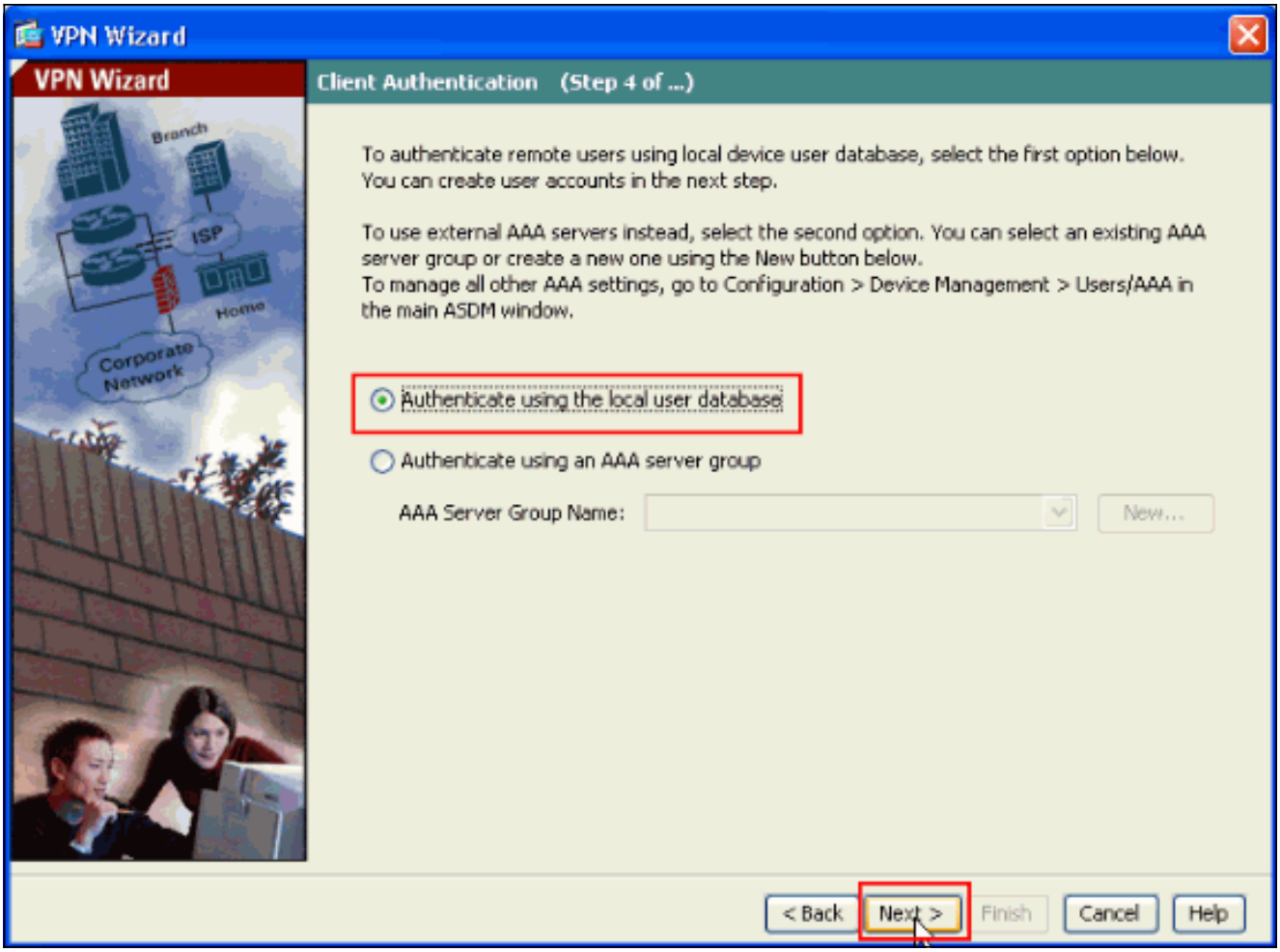
7. Тип Клиента VPN выбран, как показано. **Cisco VPN Client** выбран здесь. **Нажмите кнопку**
Next.



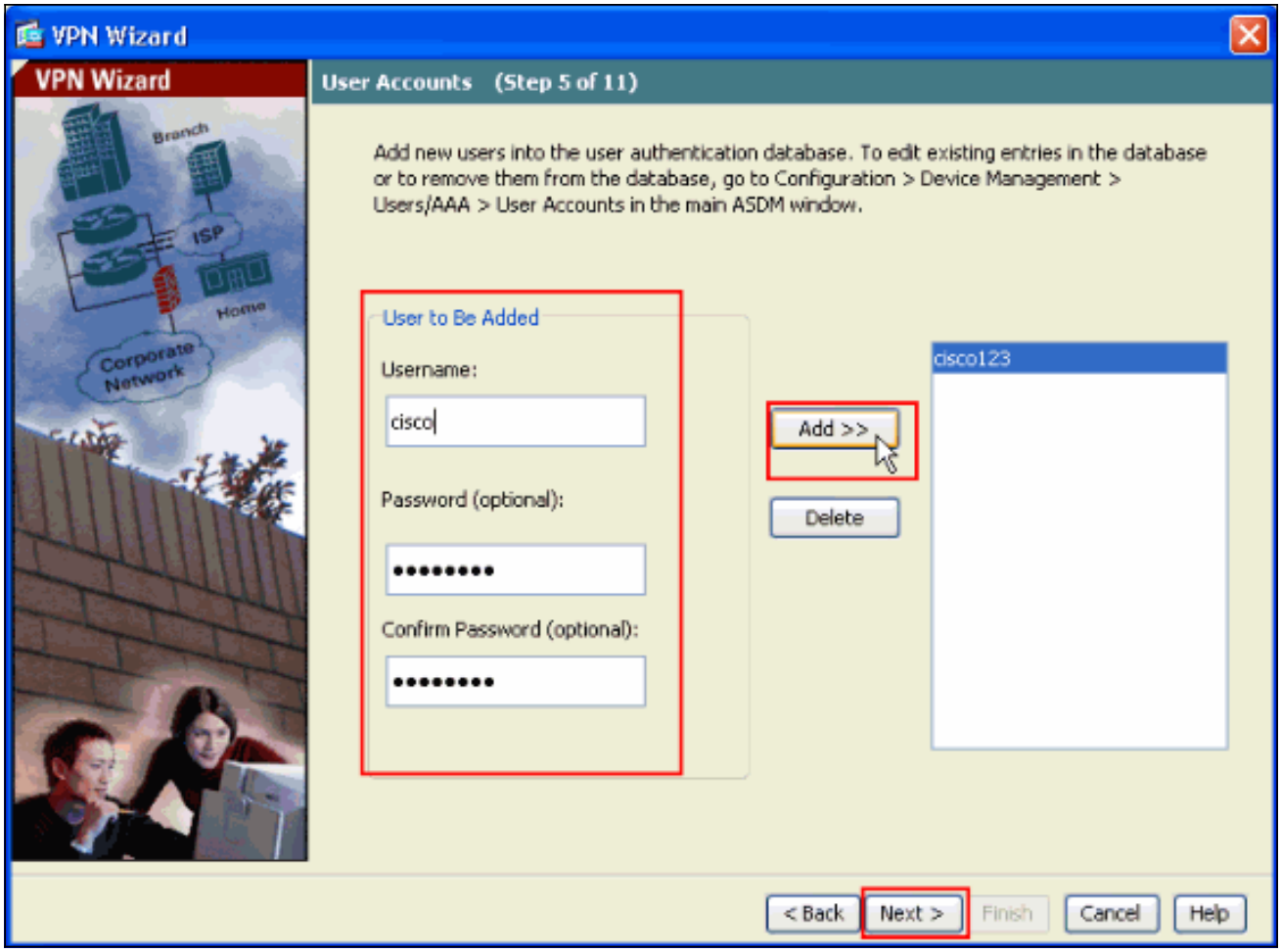
8. **Введите имя группы туннеля. Введите данные для аутентификации (в этом примере используется ключ, согласованный ранее). Название ключа cisco123.** Имя группы туннелей, используемое в данном примере, является **Cisco**. **Нажмите кнопку Next.**



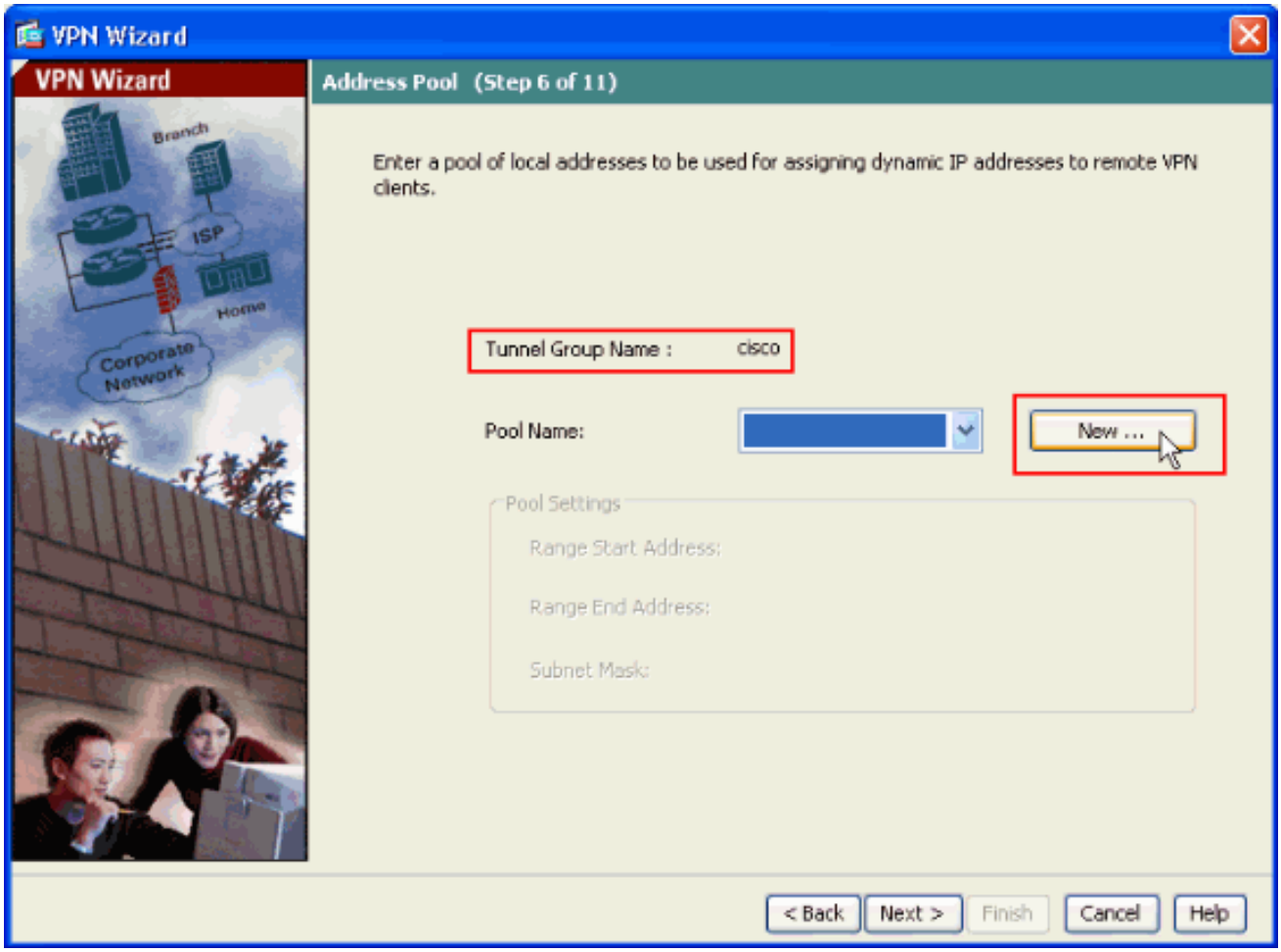
9. Выберите, хотите ли вы, чтобы удаленные пользователи аутентифицировались на базе локальных пользователей или на внешней группе AAA-серверов.**Примечание:** Вы добавляете пользователей к базе локальных пользователей в шаге 10.**Примечание:** См. PIX/ASA 7.x Группы серверов Проверки подлинности и авторизация для Пользователей VPN через Пример конфигурации ASDM для получения информации о том, как настроить внешнюю группу AAA-серверов с ASDM.



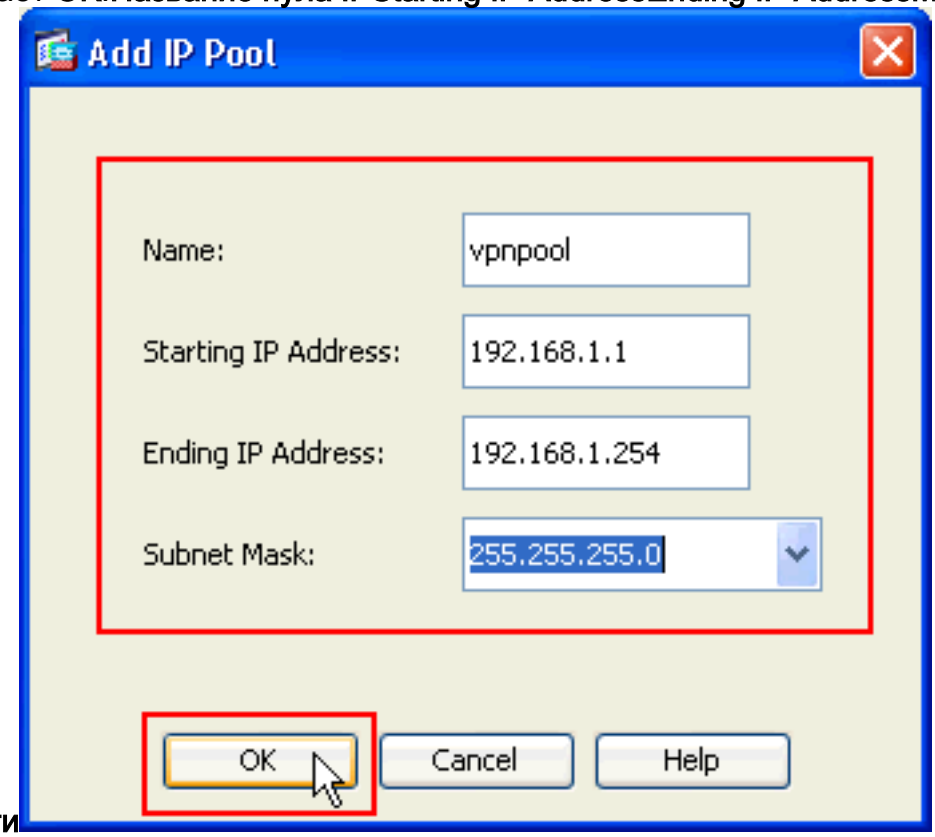
10. Введите **Имя пользователя** и дополнительный **Пароль** и **нажмите Add** для добавления новых пользователей к базе данных проверки подлинности пользователя. **Нажмите кнопку Next.Примечание:** Не удаляйте существующих пользователей из этого окна. Выберите **Configuration>> Users Device Management / AAA> Учетные записи пользователя** в главном окне ASDM, чтобы отредактировать существующие записи в базе данных или удалить их из базы
данных.



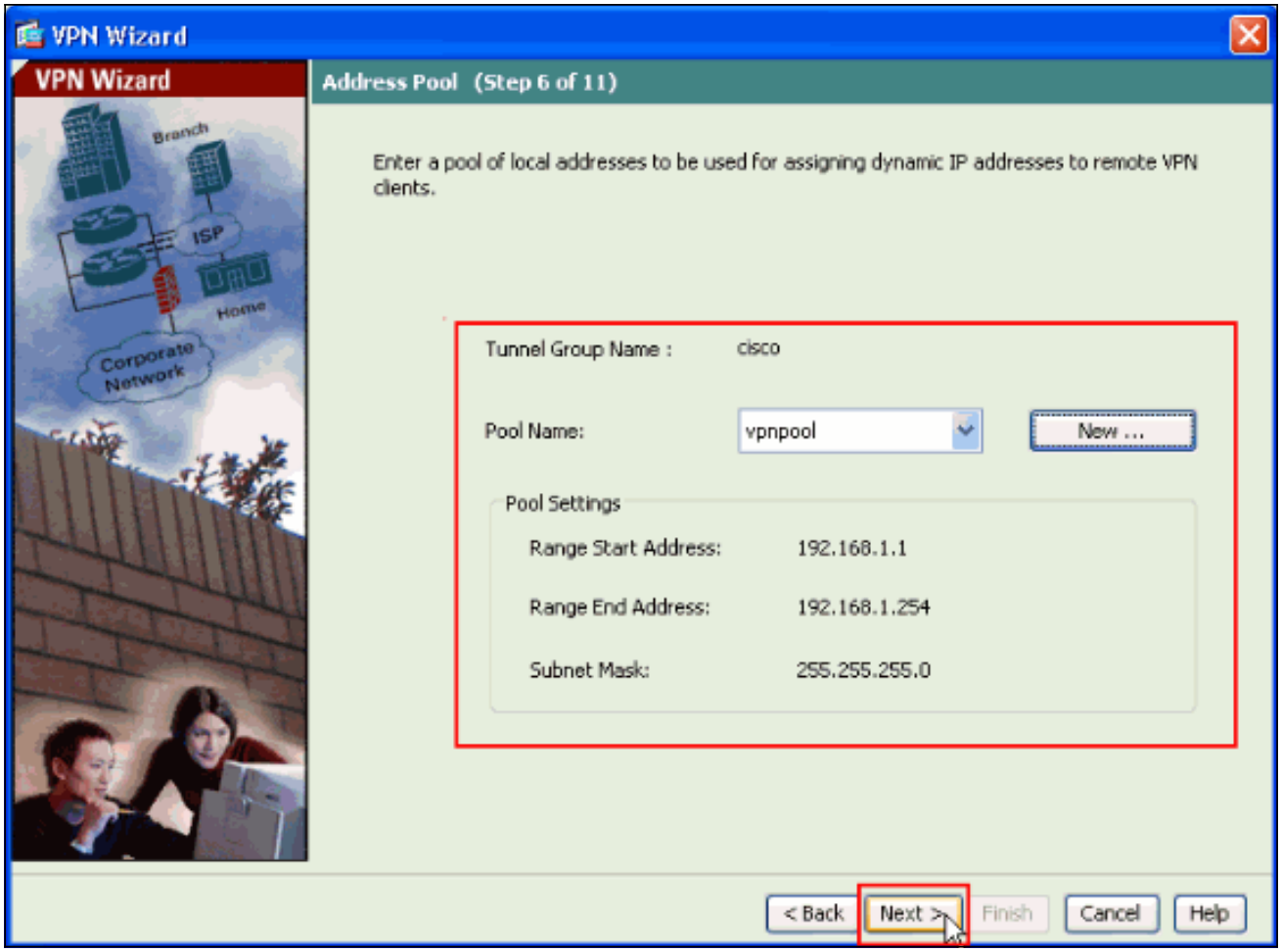
11. Для определения пула локальных адресов, которые будут динамично назначены на удаленных клиентов VPN, нажмите **New** для создания нового **Пула IP**.



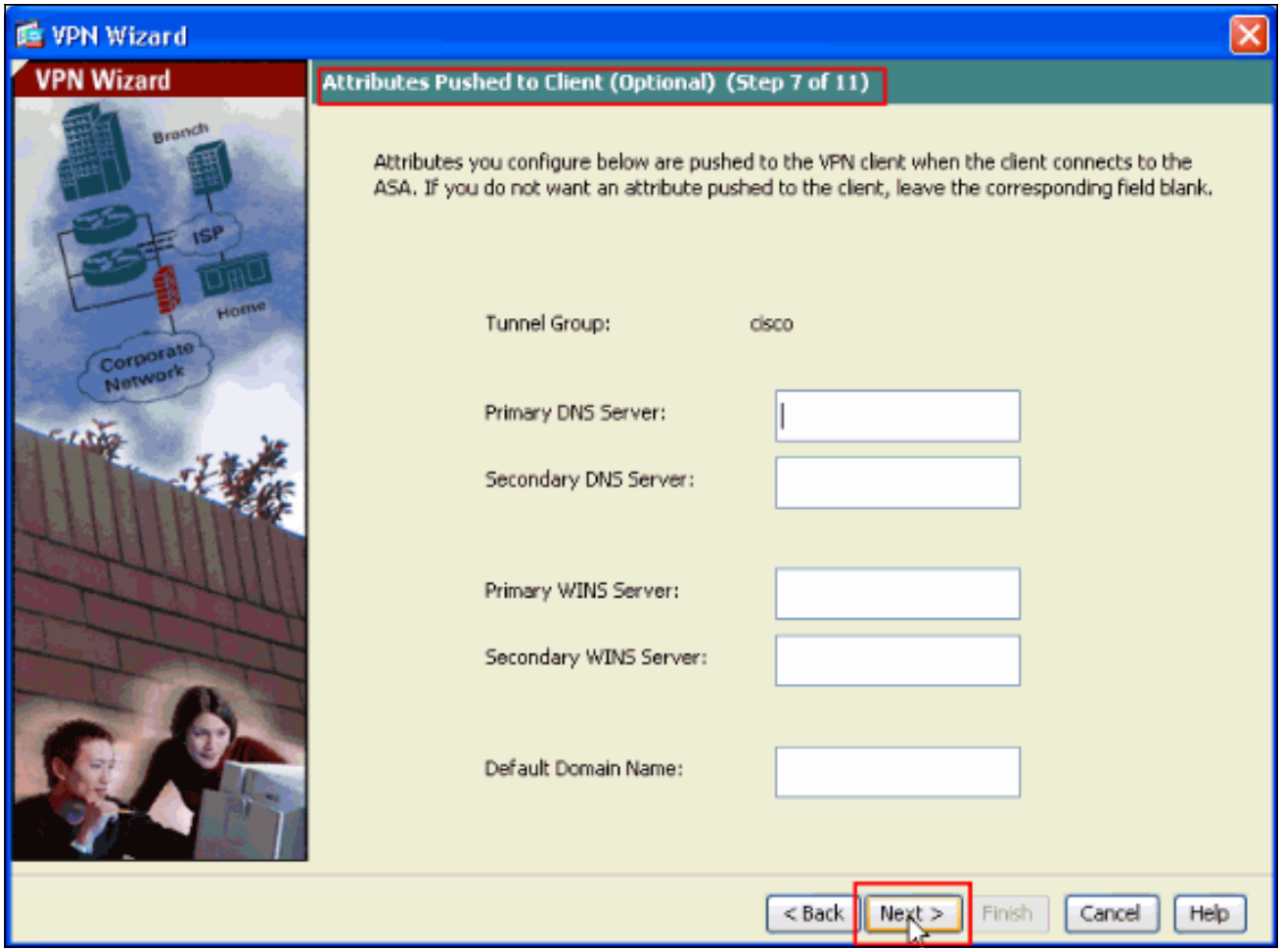
12. В названном новом окне **Добавляют, что Пул IP** предоставляет эту информацию и нажимает **OK.Название пула IPStarting IP AddressEnding IP AddressМаска подсети**



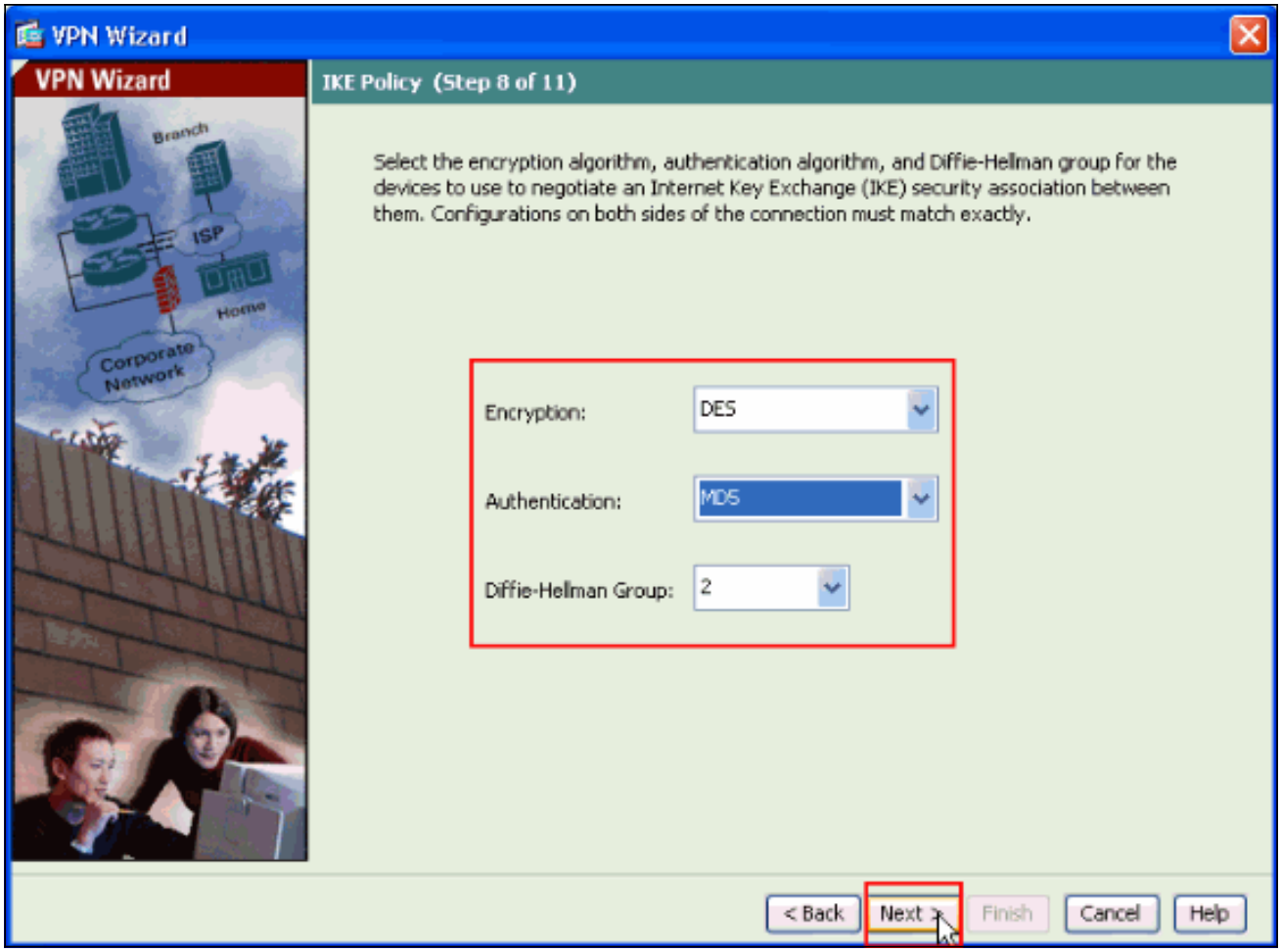
13. После определения пула локальных адресов, которые будут динамично назначены на удаленных клиентов VPN, когда они соединяются, нажмите **Next.**



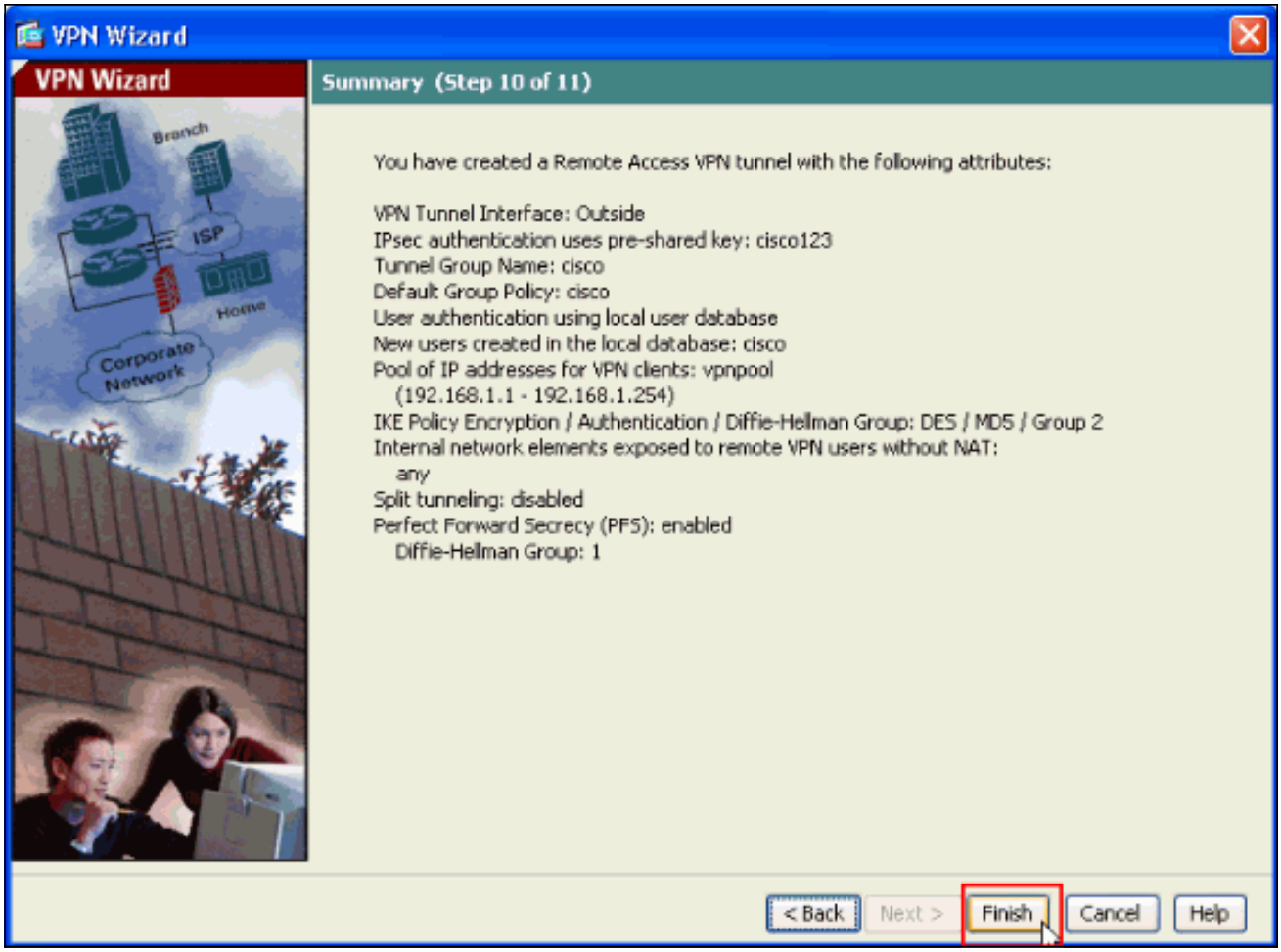
14. *Дополнительно:* Задайте DNS и информацию сервера WINS и Название Домена по умолчанию, которое будет выдвинуто к удаленным клиентам VPN.



15. 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.



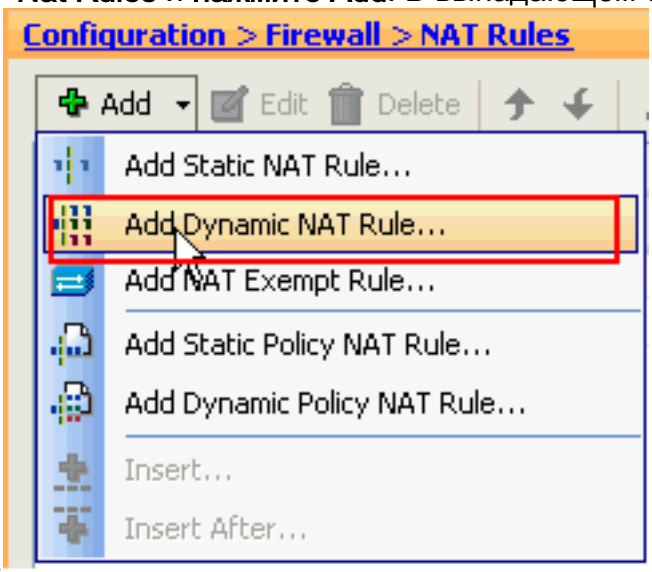
16. В этом окне показана сводка выполненных действий. **Нажмите Завершить, если настройка выполнена правильно.**



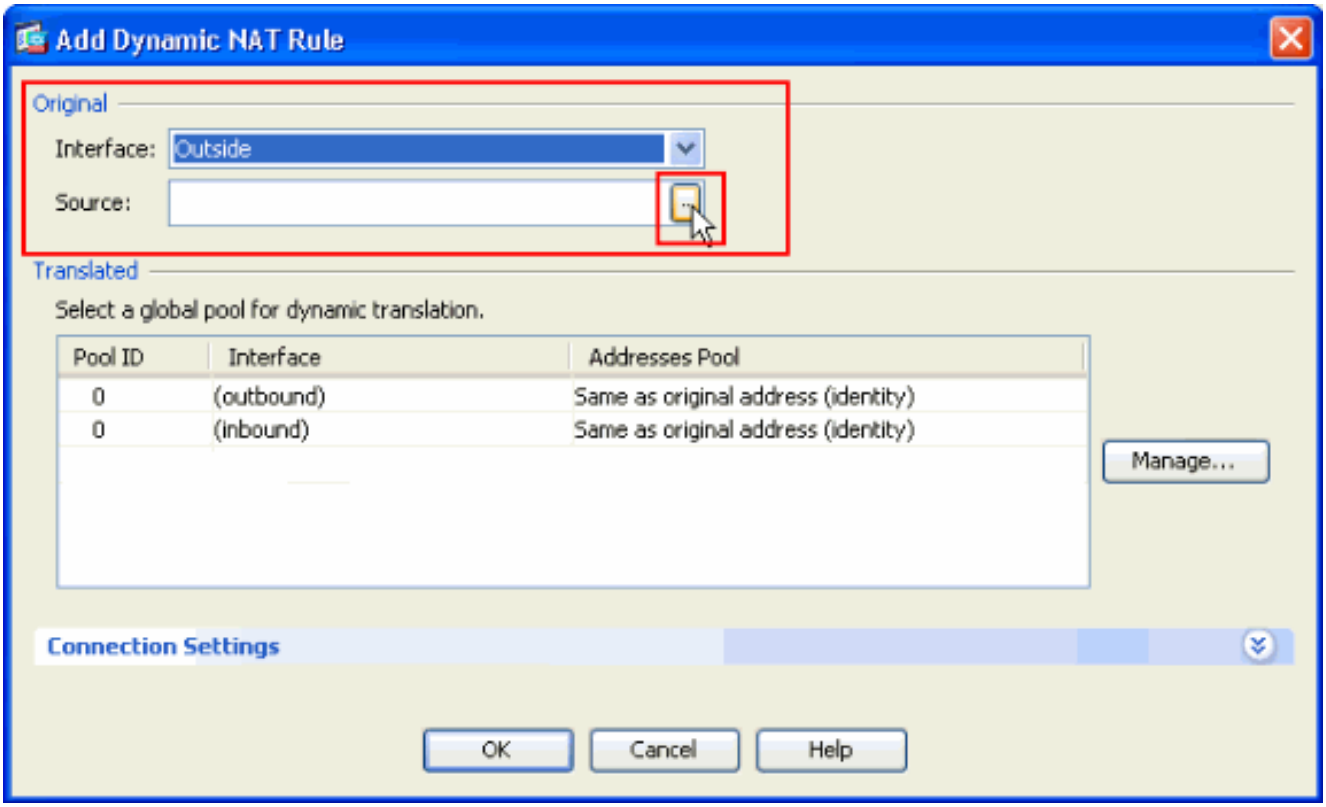
Настройте ASA/PIX к трафику клиента VPN NAT на входе с ASDM

Выполните эти шаги для настройки Cisco ASA к трафику клиента VPN NAT на входе с ASDM:

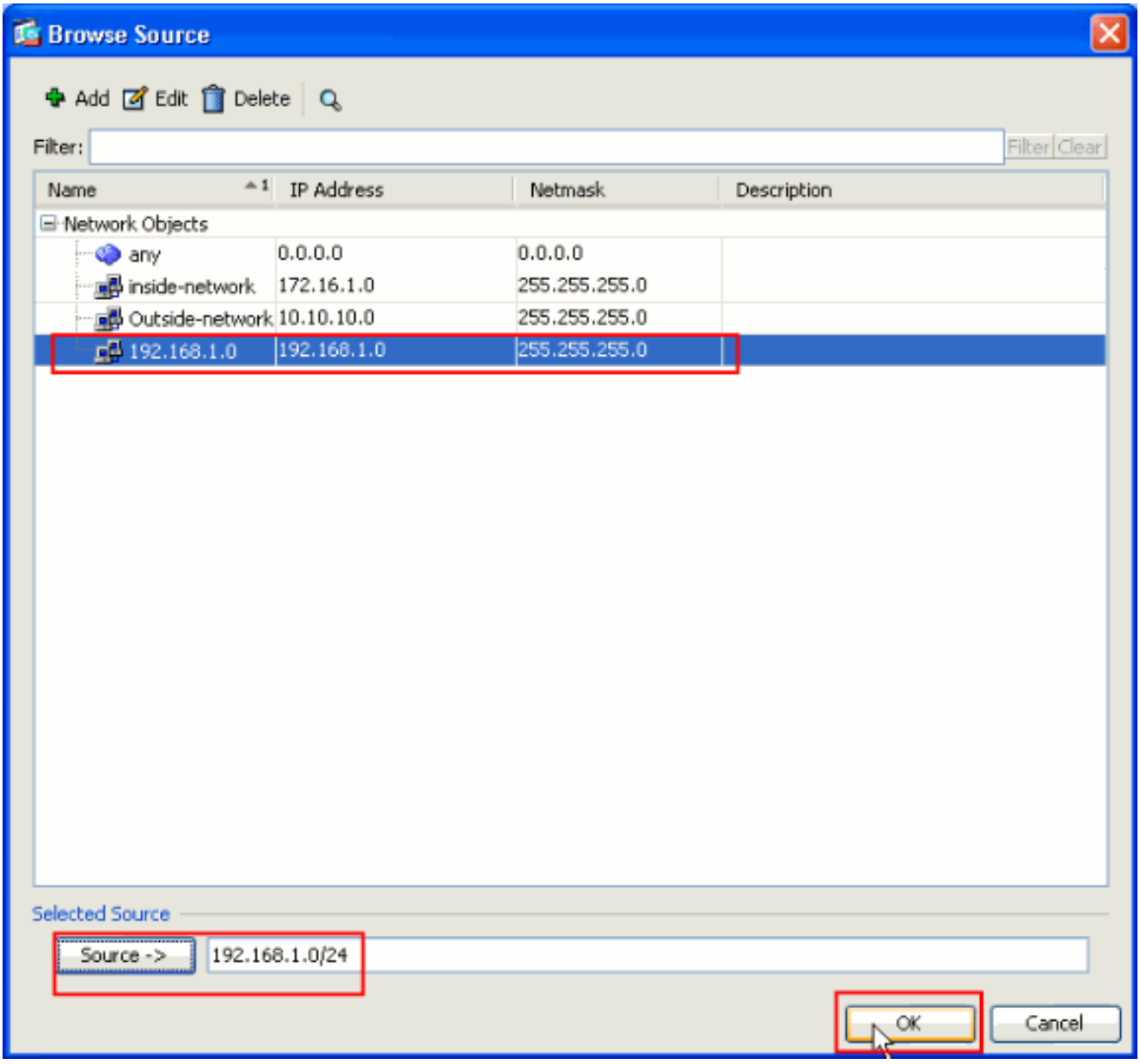
1. Выберите **Configuration> Firewall> Nat Rules** и **нажмите Add**. В выпадающем списке выберите **Add Dynamic NAT Rule**.



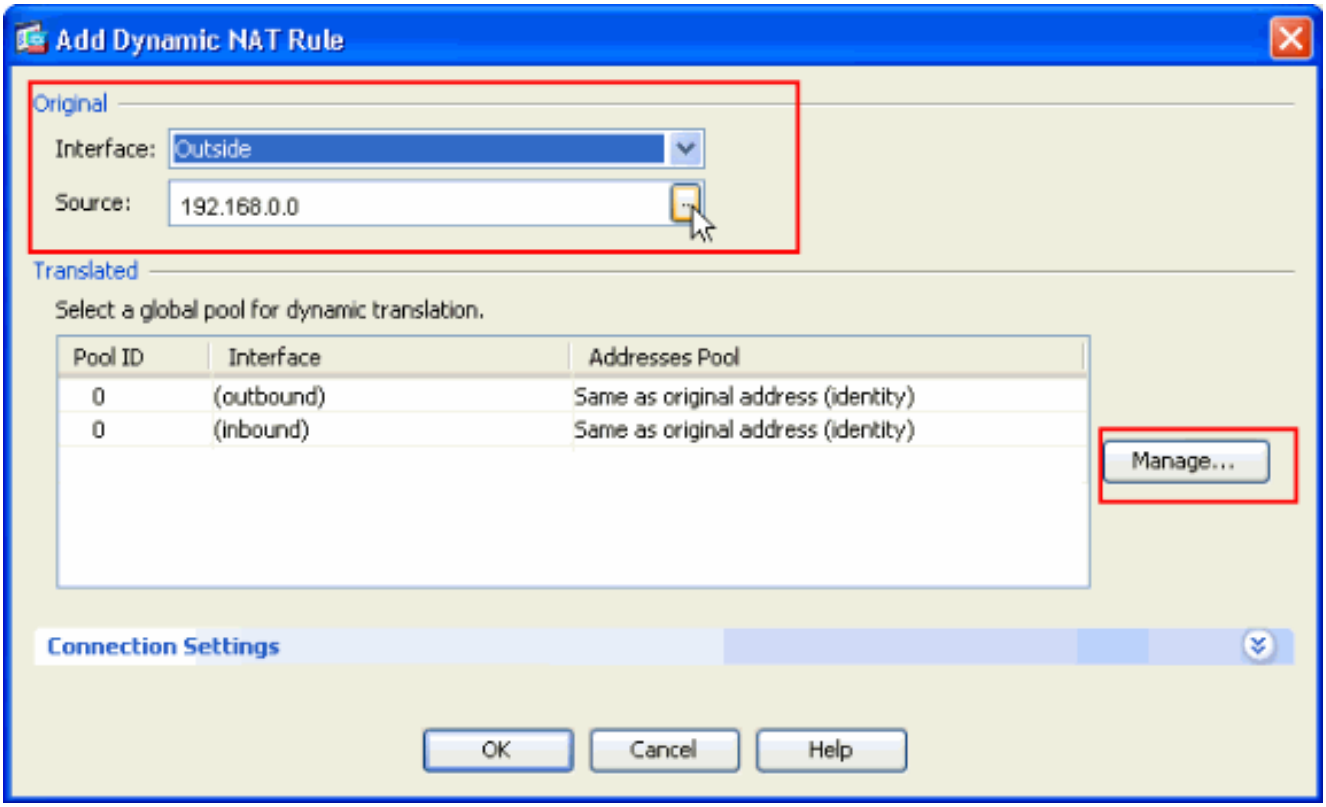
2. В окне **Add Dynamic NAT Rule** выберите **Outside** в качестве Интерфейса и нажмите кнопку обзора рядом с **Исходной** коробкой.



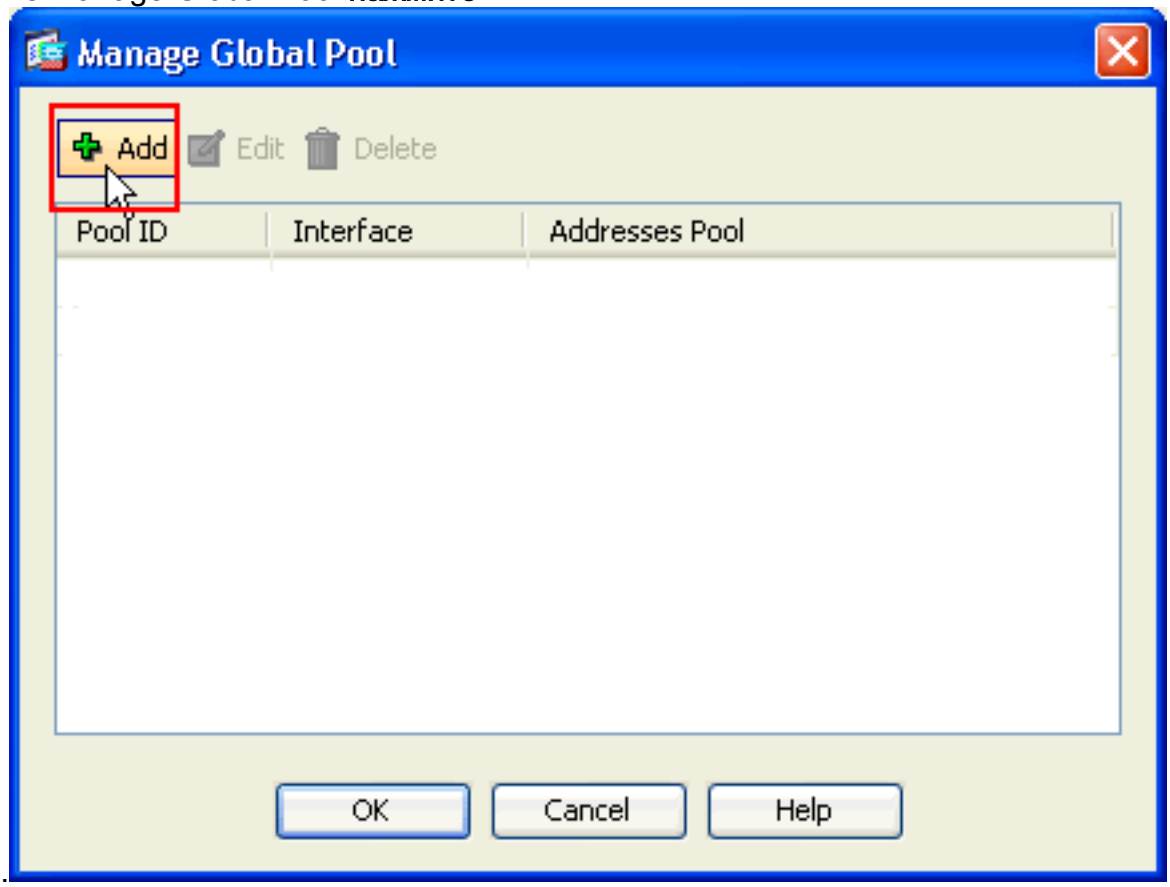
3. В окне Browse Source выберите объекты исправной сети и также выберите **источник** под Выбранным Исходным разделом и нажмите **OK**. Здесь 192.168.1.0 Сетевых объекта
выбраны.



4. Щелкните Manage (Управление).

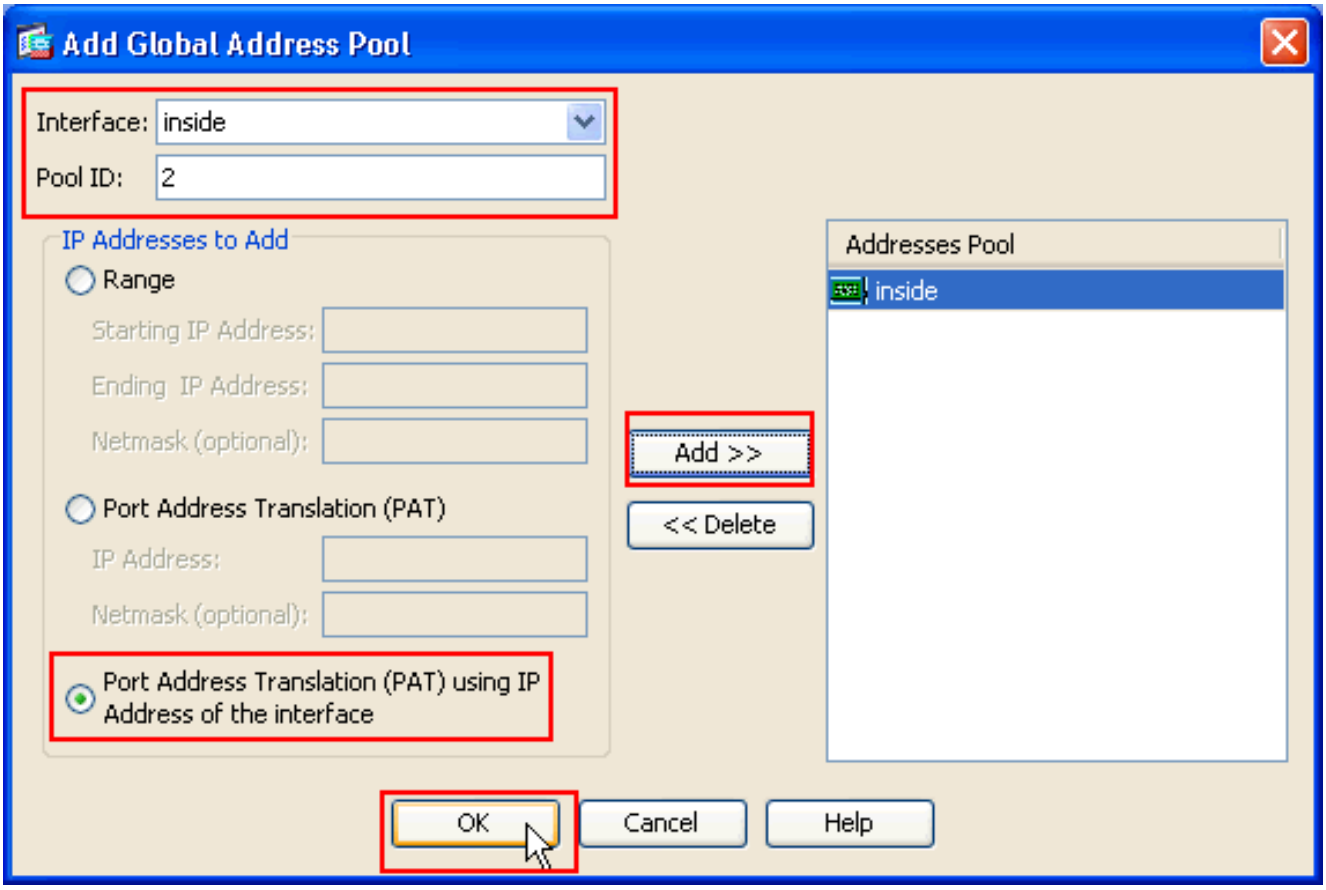


5. В окне Manage Global Pool **нажмите**

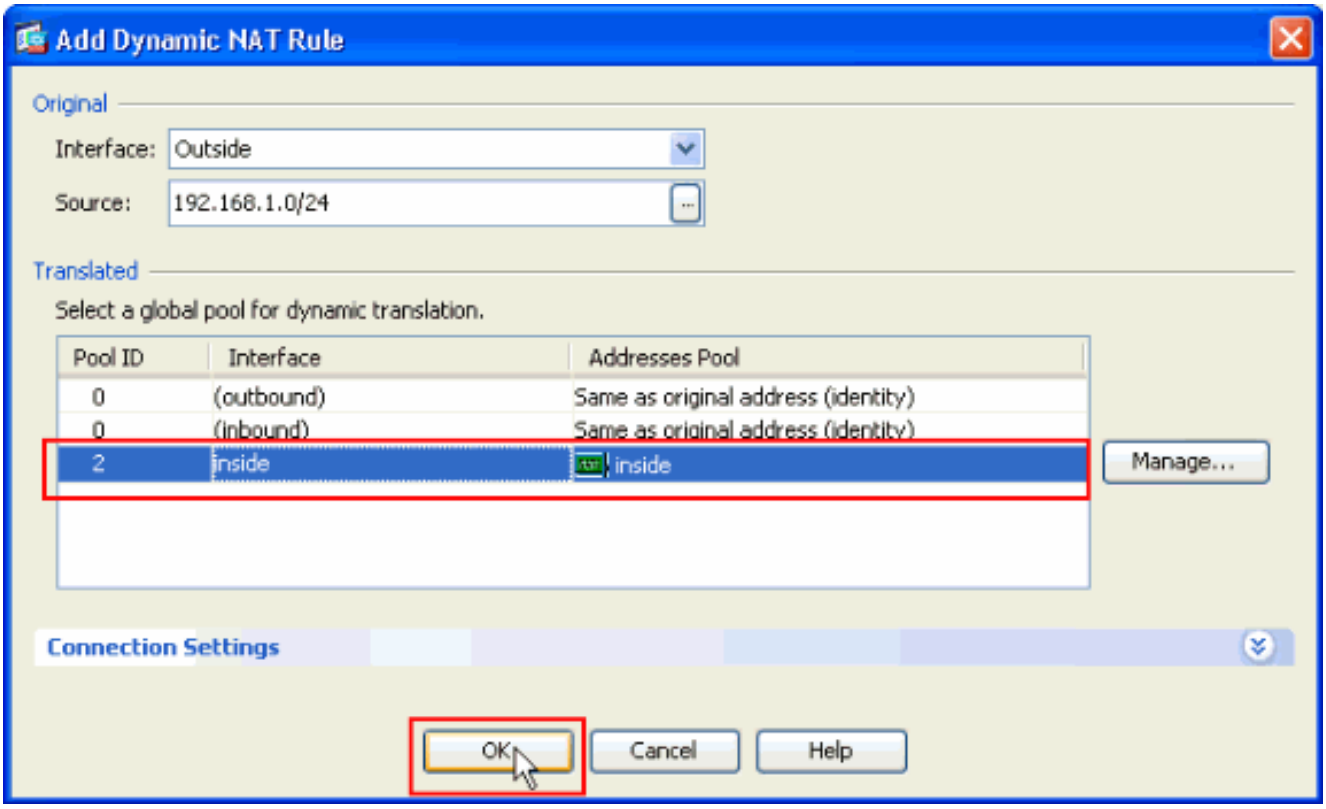


Add.

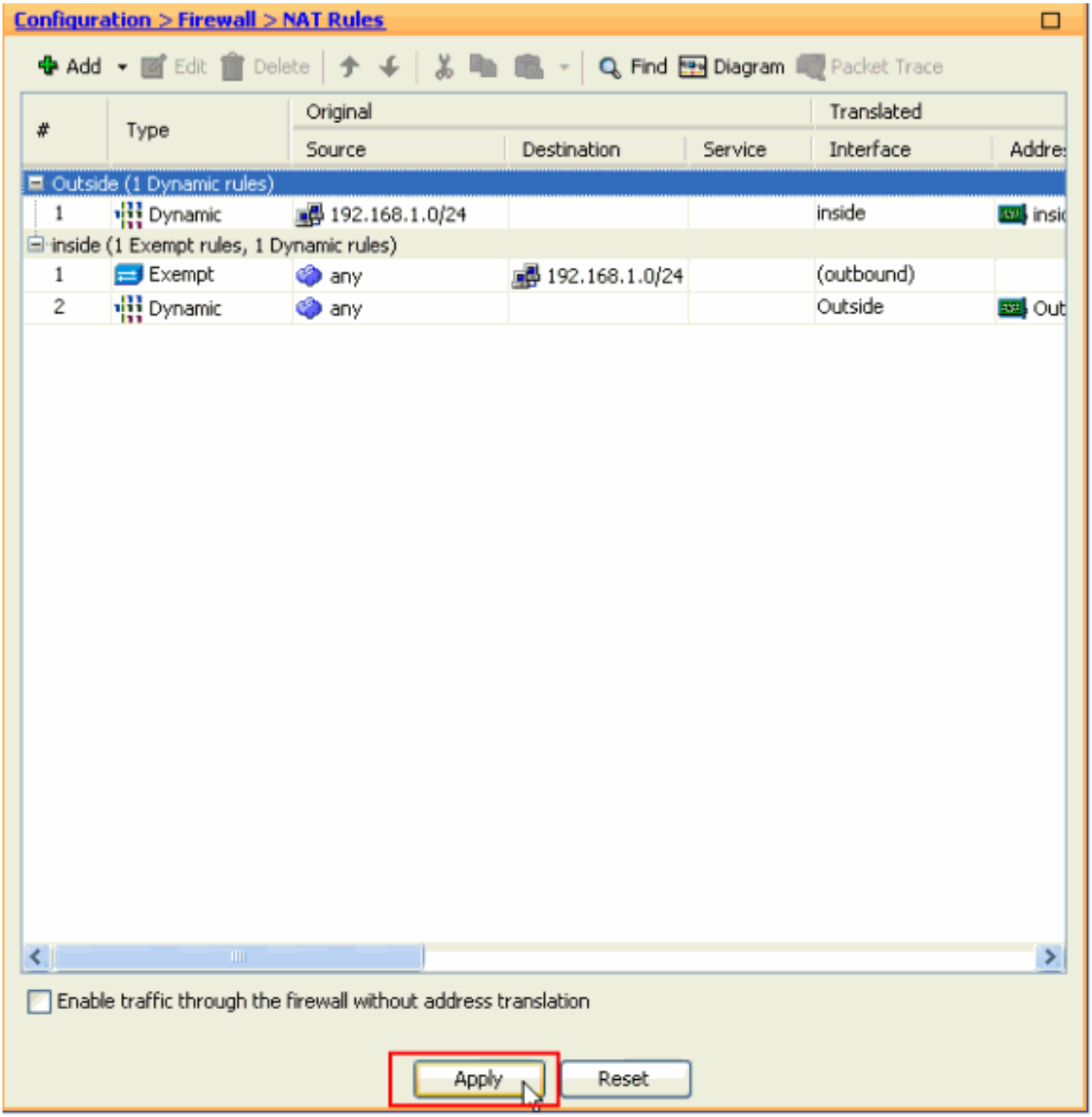
6. В окне Add Global Address Pool выберите **Inside** в качестве Интерфейса и **2** как **ID Пула**. Также удостоверьтесь, что установлен переключатель, следующий за **PAT с помощью IP-адреса интерфейса**. **Нажмите Add>>**, и затем нажмите **OK**.



7. Нажмите **OK** после выбора глобального пула **ID 2 Пула**, настроенным в предыдущем шаге.



8. Теперь нажмите **Apply** так, чтобы конфигурация была применена к ASA.This, завершает конфигурацию.



Настройте ASA/PIX как Удаленный VPN-сервер и для Входящего NAT с CLI

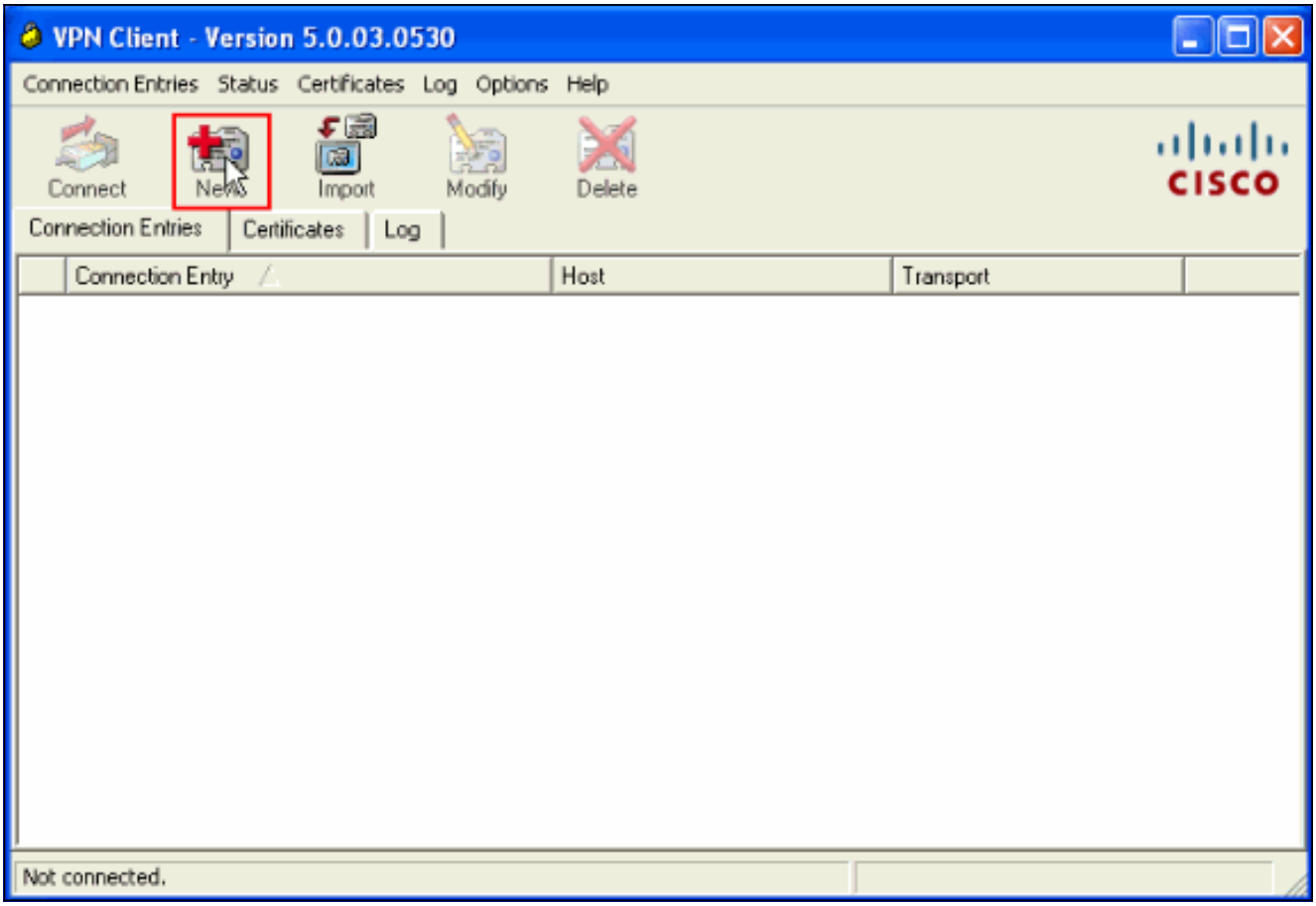
Выполнение Config на устройстве ASA
ciscoasa#**show running-config** : Saved ASA Version 8.0(3) ! hostname ciscoasa enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0 nameif Outside security-level 0 ip address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1 nameif inside security-level 100 ip address 172.16.1.2 255.255.255.0 ! ! passwd 2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa803-k8.bin ftp mode passive access-list inside_nat0_outbound extended permit ip any 192.168.1.0 255.255.255 0 pager lines 24 logging enable mtu Outside 1500 mtu inside 1500 **ip local pool vpnpool 192.168.1.1-192.168.1.254 mask 255.255.255.0** no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-615.bin asdm history enable arp timeout 14400 nat-control **global (Outside) 1 interface global (inside) 2 interface nat (Outside) 2 192.168.1.0 255.255.255.0 outside nat (inside) 0 access-**

```
list inside_nat0_outbound nat (inside) 1 0.0.0.0 0.0.0.0
route Outside 0.0.0.0 0.0.0.0 10.10.10.3 1 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 no snmp-server location no snmp-server
contact !--- Configuration for IPsec policies. !---
Enables the crypto transform configuration mode, !---
where you can specify the transform sets that are used
!--- during an IPsec negotiation. crypto ipsec
transform-set ESP-DES-SHA esp-des esp-sha-hmac crypto
ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set
pfs group1 crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP
65535 set transform-set ESP-DES-SH ESP-DES-MD5 crypto
map Outside_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP crypto map Outside_map
interface Outside crypto isakmp enable Outside !---
Configuration for IKE policies. !--- Enables the IKE
policy configuration (config-isakmp) !--- command mode,
where you can specify the parameters that !--- are used
during an IKE negotiation. Encryption and !--- Policy
details are hidden as the default values are chosen.
crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 2 lifetime 86400 crypto
isakmp policy 30 authentication pre-share encryption des
hash md5 group 2 lifetime 86400 telnet timeout 5 ssh
timeout 60 console timeout 0 management-access inside
threat-detection basic-threat threat-detection
statistics access-list group-policy cisco internal
group-policy cisco attributes vpn-tunnel-protocol IPSec
!--- Specifies the username and password with their !---
respective privilege levels username cisco123 password
ffIRPGpDSOJh9YLq encrypted privilege 15 username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 0 username
cisco attributes vpn-group-policy cisco tunnel-group
cisco type remote-access tunnel-group cisco general-
attributes address-pool vpnpool default-group-policy
cisco !--- Specifies the pre-shared key "cisco123" which
must !--- be identical at both peers. This is a global
!--- configuration mode command. tunnel-group cisco
ipsec-attributes pre-shared-key * ! class-map
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns migrated_dns_map_1
parameters message-length maximum 512 policy-map
global_policy class inspection_default inspect dns
migrated_dns_map_1 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:f2ad6f9d5bf23810a26f5cb464e1fdf3 : end
ciscoasa#
```

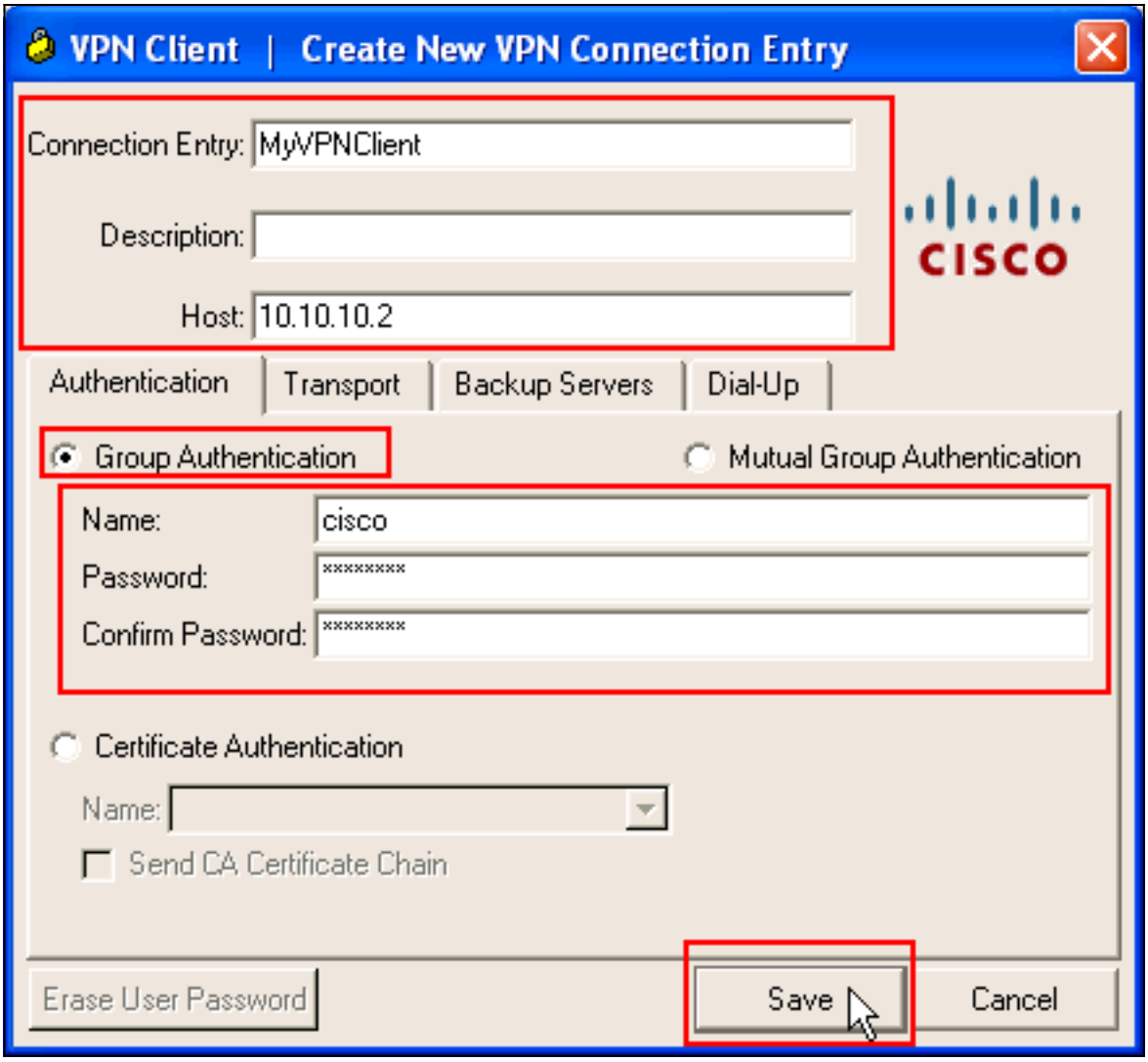
Проверка

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

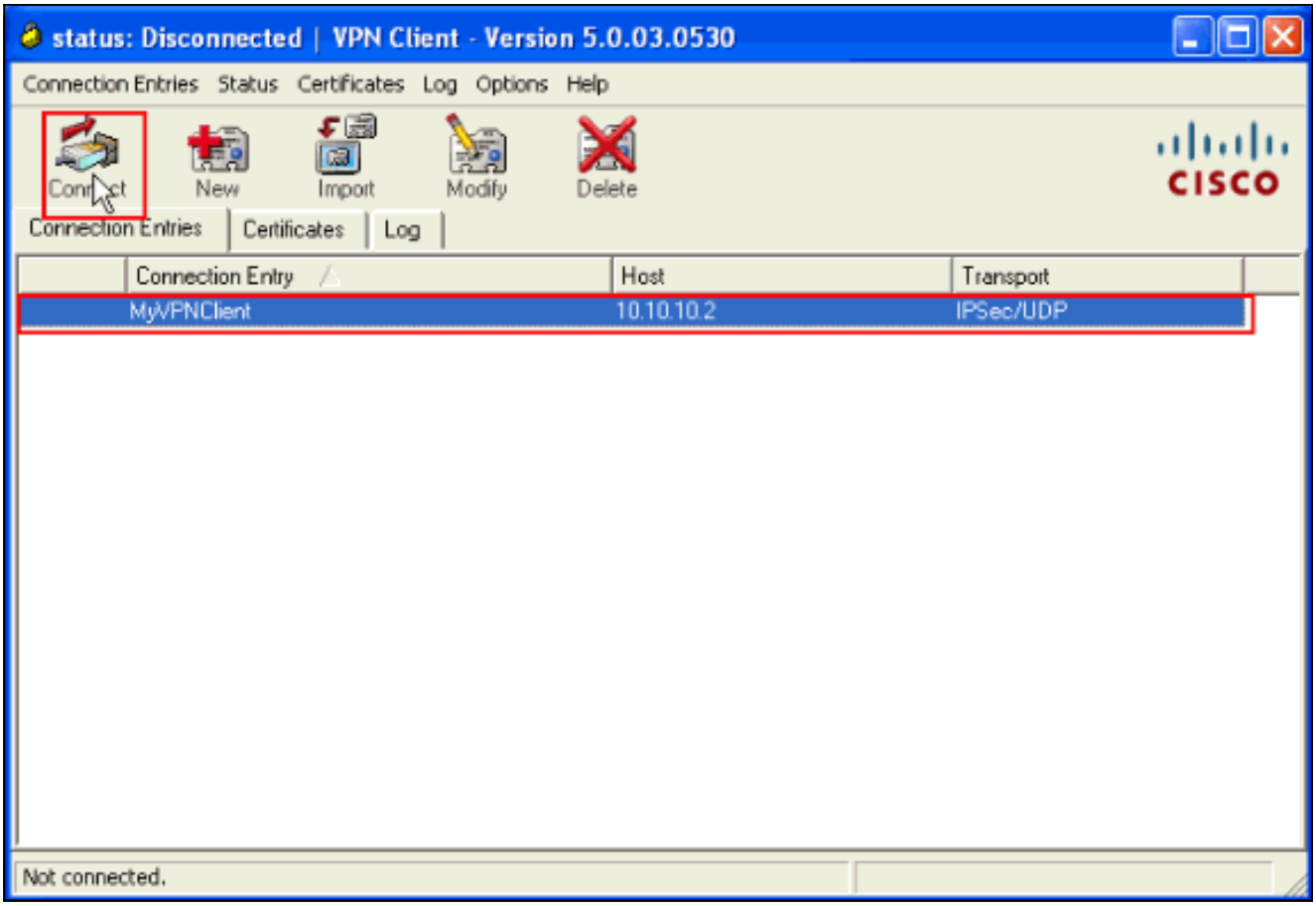
1. **Щелкните New.**



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.



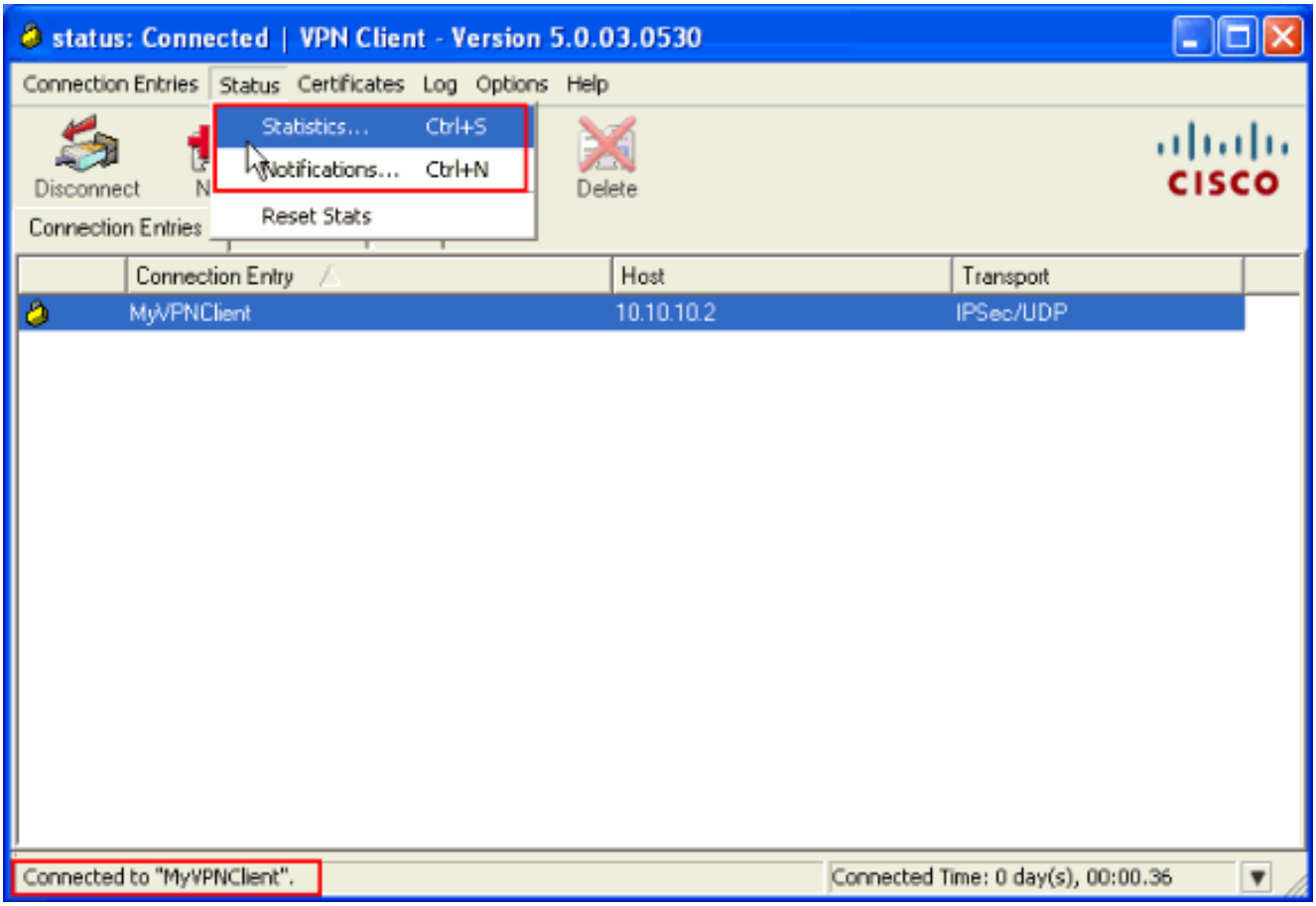
3. Выберите только что созданное подключение и нажмите Соединить.



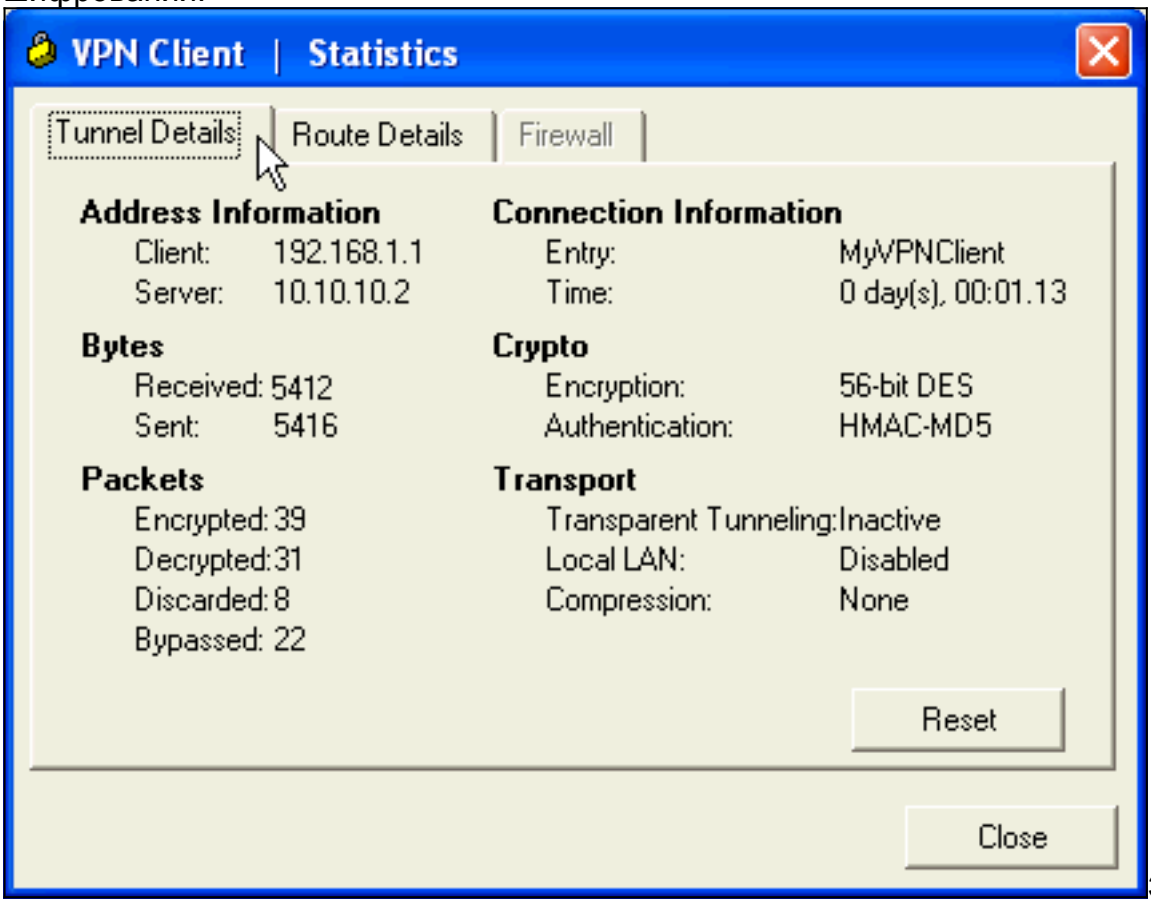
4. Введите имя пользователя и пароль для расширенной проверки подлинности. Эта информация должна совпасть, это задало в **шагах 5 и**

6.

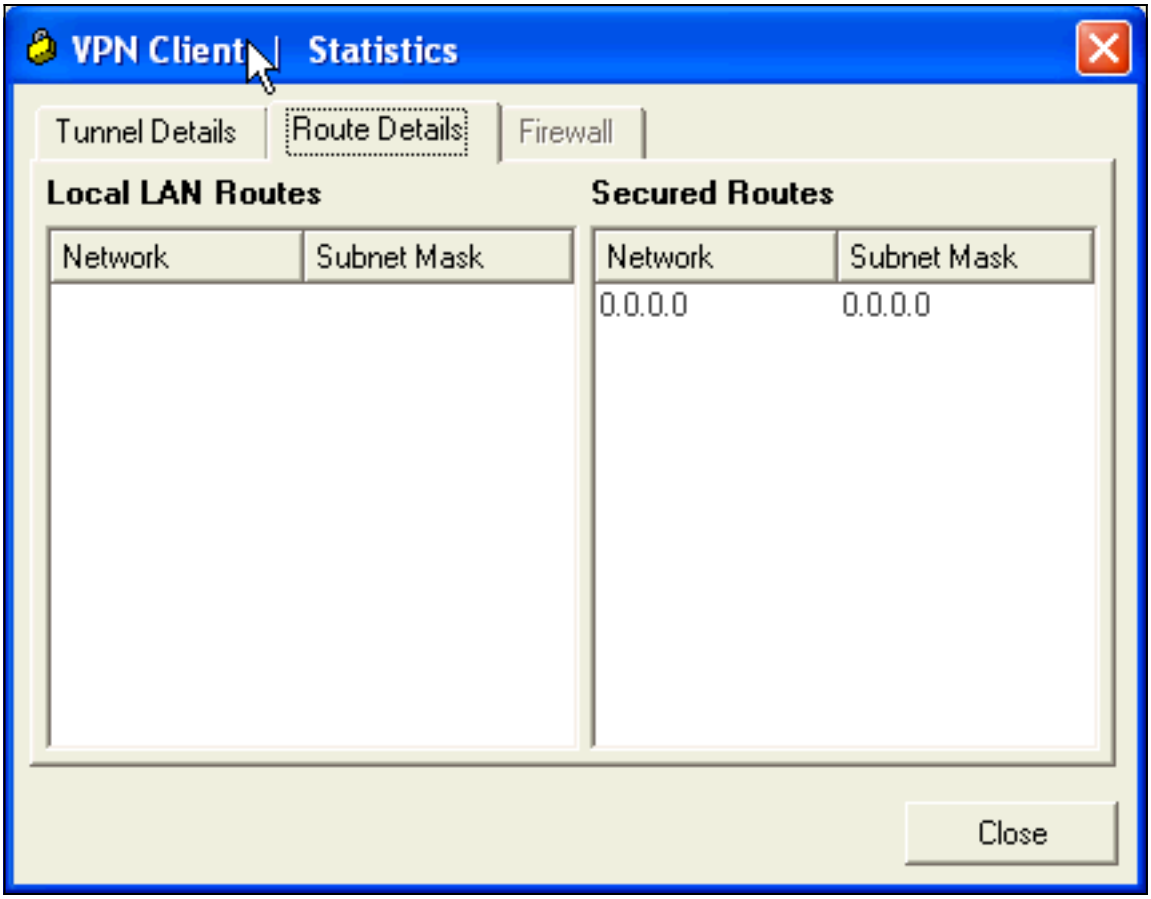
5. Как только соединение успешно установлено, выберите **Statistics** из Меню состояния для проверки подробных данных
туннеля.



В этом окне показана информация о трафике и шифровании:



Это окно показывает информацию о разделенном туннелировании:



Команды «show» устройства защиты ASA/PIX

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE узла.**ASA#**show crypto isakmp sa** Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.10.10.1 Type : user Role : responder Rekey : no State : AM_ACTIVE
- **show crypto ipsec sa — отображает все текущие ассоциации безопасности (SA) IPsec узла.**ASA#**show crypto ipsec sa** interface: Outside **Crypto map tag: SYSTEM_DEFAULT_CRYPTO_MAP, seq num: 65535, local addr: 10.10 .10.2 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/0/0) current_peer: 10.10.10.1, username: cisco123 dynamic allocated peer ip: 192.168.1.1 #pkts encaps: 20, #pkts encrypt: 20, #pkts digest: 20 #pkts decaps: 74, #pkts decrypt: 74, #pkts verify: 74 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 20, #pkts comp failed: 0, #pkts decomp failed: 0** #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #recv errors: 0 **local crypto endpt.: 10.10.10.2, remote crypto endpt.: 10.10.10.1** path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: F49F954C inbound esp sas: spi: 0x3C10F9DD (1007745501) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0xF49F954C (4104099148) transform: esp-des esp-md5-hmac none in use settings ={RA, Tunnel, } slot: 0, conn_id: 24576, crypto-map: SYSTEM_DEFAULT_CRYPTO_MAP sa timing: remaining key lifetime (sec): 27255 IV size: 8 bytes replay detection support: Y
- ciscoasa(config)#**debug icmp trace** *!--- Inbound Nat Translation is shown below for Outside to Inside* **ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1** ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=7936 len=3 2 *!--- Inbound Nat Translation is shown below for Inside to Outside* **ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768** ICMP echo request from Outside:192.168.1.1 to inside:172.16.1.3 ID=768 seq=8192 len=32 ICMP echo request translating Outside:192.168.1.1/768 to inside:172.16.1.2/1 ICMP echo reply from inside:172.16.1.3 to Outside:172.16.1.2 ID=1 seq=8192 len=3 2 ICMP echo reply untranslating inside:172.16.1.2/1 to Outside:192.168.1.1/768 ICMP echo request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8448 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768 seq=8448 len=32 ICMP echo

```
request from 192.168.1.1 to 172.16.1.2 ID=768 seq=8704 len=32 ICMP echo reply from
172.16.1.2 to 192.168.1.1 ID=768 seq=8704 len=32 ICMP echo request from 192.168.1.1 to
172.16.1.2 ID=768 seq=8960 len=32 ICMP echo reply from 172.16.1.2 to 192.168.1.1 ID=768
seq=8960 len=32
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

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

См. Решения для Устранения проблем IPSEC VPN Наиболее распространенного соединения L2L и Удаленного доступа для получения дополнительной информации о том, как устранить неполадки VPN Узла Узла.

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- Устранение неполадок и работа с оповещениями устройств адаптивной защиты Cisco ASA серии 5500
- Cisco Systems – техническая поддержка и документация