SDM: Пример настройки сети IPSec VPN типа "сеть-сеть" между ASA/PIX и маршрутизатором под управлением IOS

Содержание

Введение

В этом документе приводится пример настройки туннеля IPsec "ЛВС-ЛВС" между устройствами защиты Cisco ASA/PIX и маршрутизатором Cisco IOS. Для упрощения используются статические маршруты.

Для получения дополнительных сведений об аналогичном сценарии, при котором устройства защиты PIX/ASA работают под управлением ПО версии 7.x, обратитесь к документу Пример настройки IPsec-туннеля ЛВС-ЛВС от устройства защиты PIX/ASA 7.x к маршрутизатору Cisco IOS.

Предварительные условия

Требования

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

- Перед выполнением шагов по настройке согласно данному документу необходимо установить IP-подключение между конечными узлами.
- Необходимо активировать лицензию устройства защиты для стандарта шифрования DES (на минимальном уровне шифрования).

Используемые компоненты

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

- Устройство адаптивной защиты Cisco ASA с ПО версии 8.x и более поздних версий
- ASDM версии 6.x и выше
- Маршрутизатор Cisco 1812 под управлением операционной системы Cisco IOS® версии 12.3
- Диспетчер устройств защиты CISCO SDM версии 2.5

Примечание: Сведения о том, как разрешить настройку ASA с помощью ASDM см. в документе Включение HTTPS-доступа для ASDM.

Примечание: См. Базовую настройку маршрутизатора с помощью SDM, чтобы позволить маршрутизатору быть настроенным SDM.

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.

Примечание: См. Профессионала Конфигурации: VPN Защищенного взаимодействия между сетями Site-to-Site IPsec Между ASA/PIX и Примером конфигурации Маршрутизатора IOS для подобной конфигурации с помощью Cisco Configuration Professional на маршрутизаторе.

Родственные продукты

Эту конфигурацию также можно использовать для устройств защиты Cisco PIX серии 500, работающих под управлением ПО версии 7.x и более поздних версий.

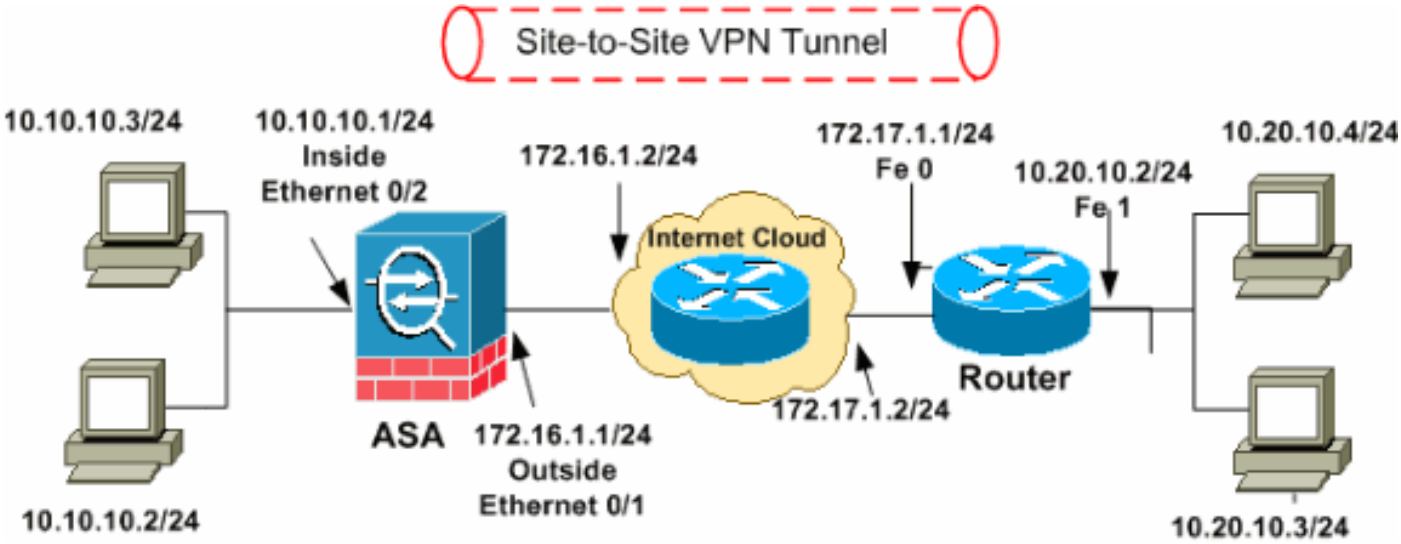
Условные обозначения

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

!--- конфигурацию

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



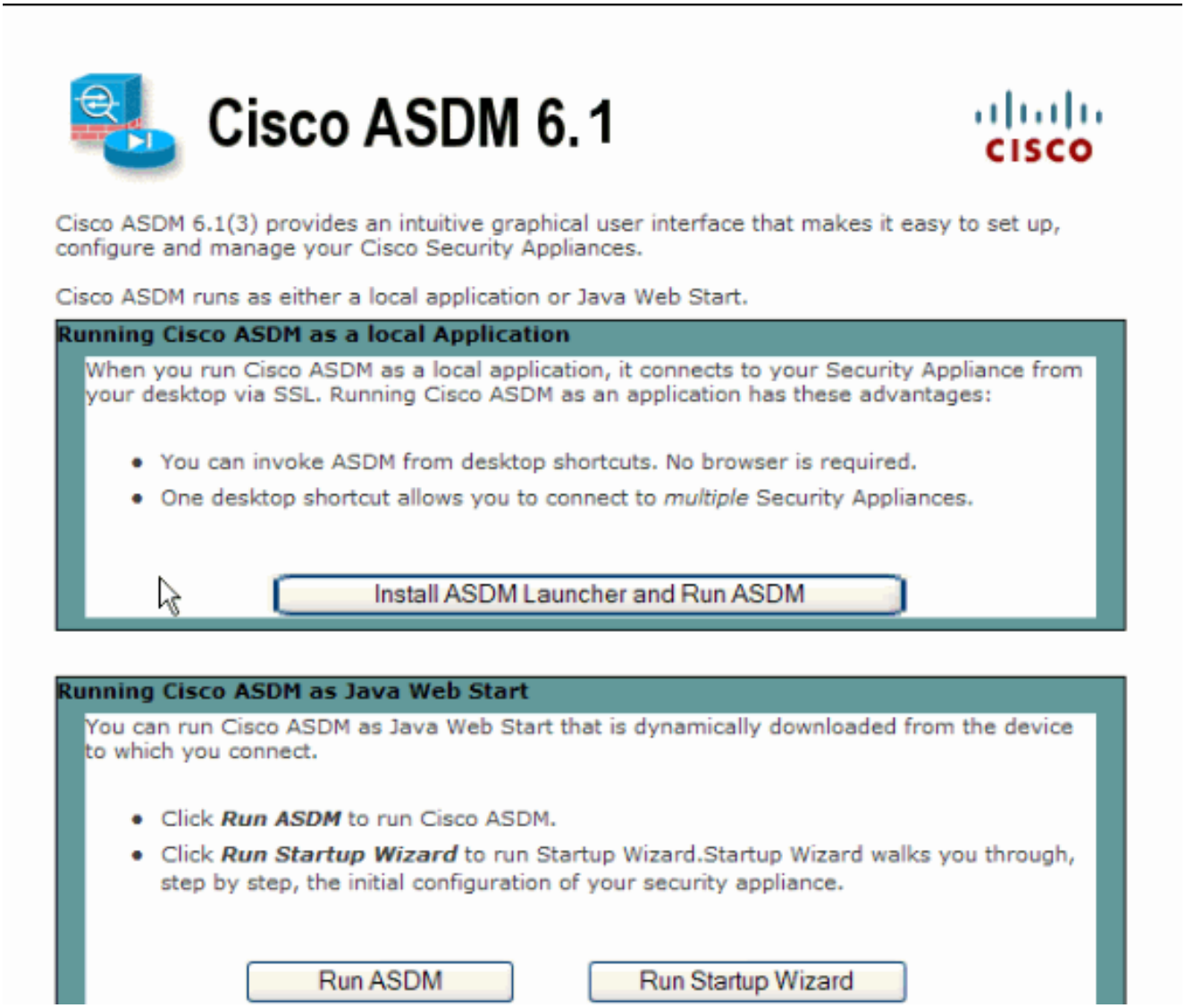
Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

- Настройка VPN-туннеля для ASDM
- Настройка маршрутизатора с помощью SDM
- Конфигурация ASA в интерфейсе командной строки
- Настройка маршрутизатора с помощью интерфейса командной строки

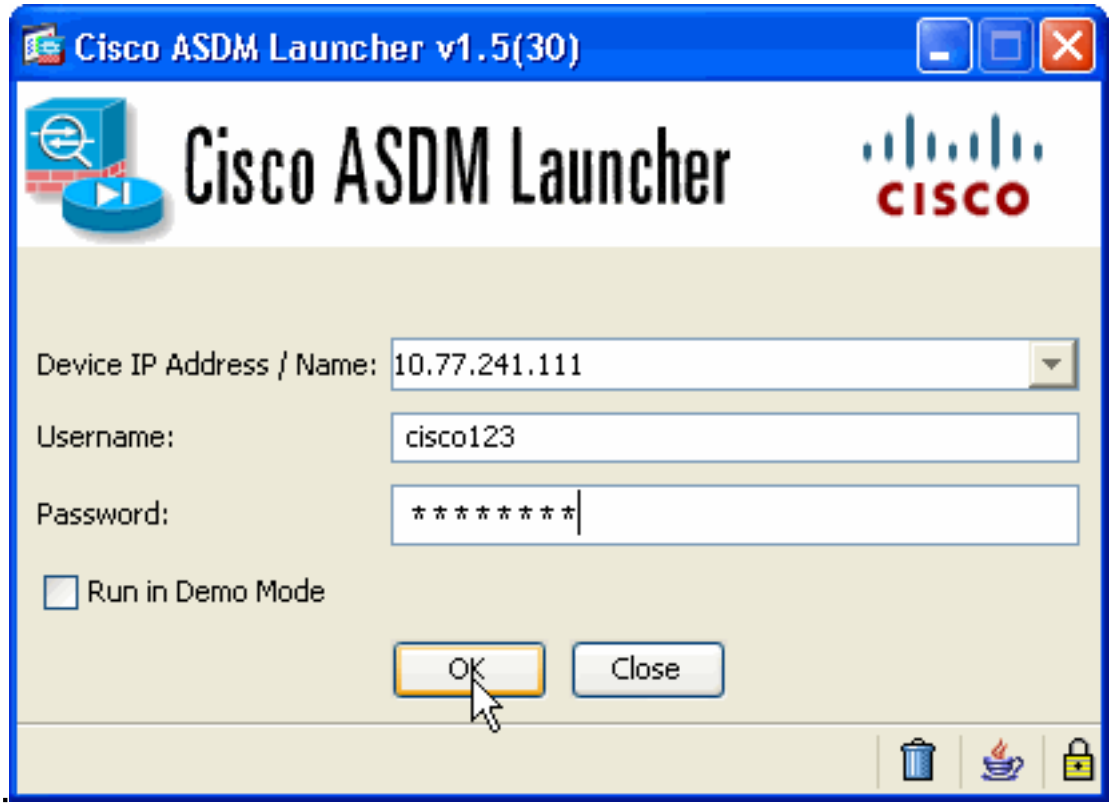
Настройка VPN-туннеля для ASDM

Выполните эти шаги для создания VPN-туннеля:

1. **Откройте браузер и введите адрес https://<IP_адрес интерфейса_ASA,_который_необходимо_настроить_для_доступа_ASDM>, чтобы подключиться 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.

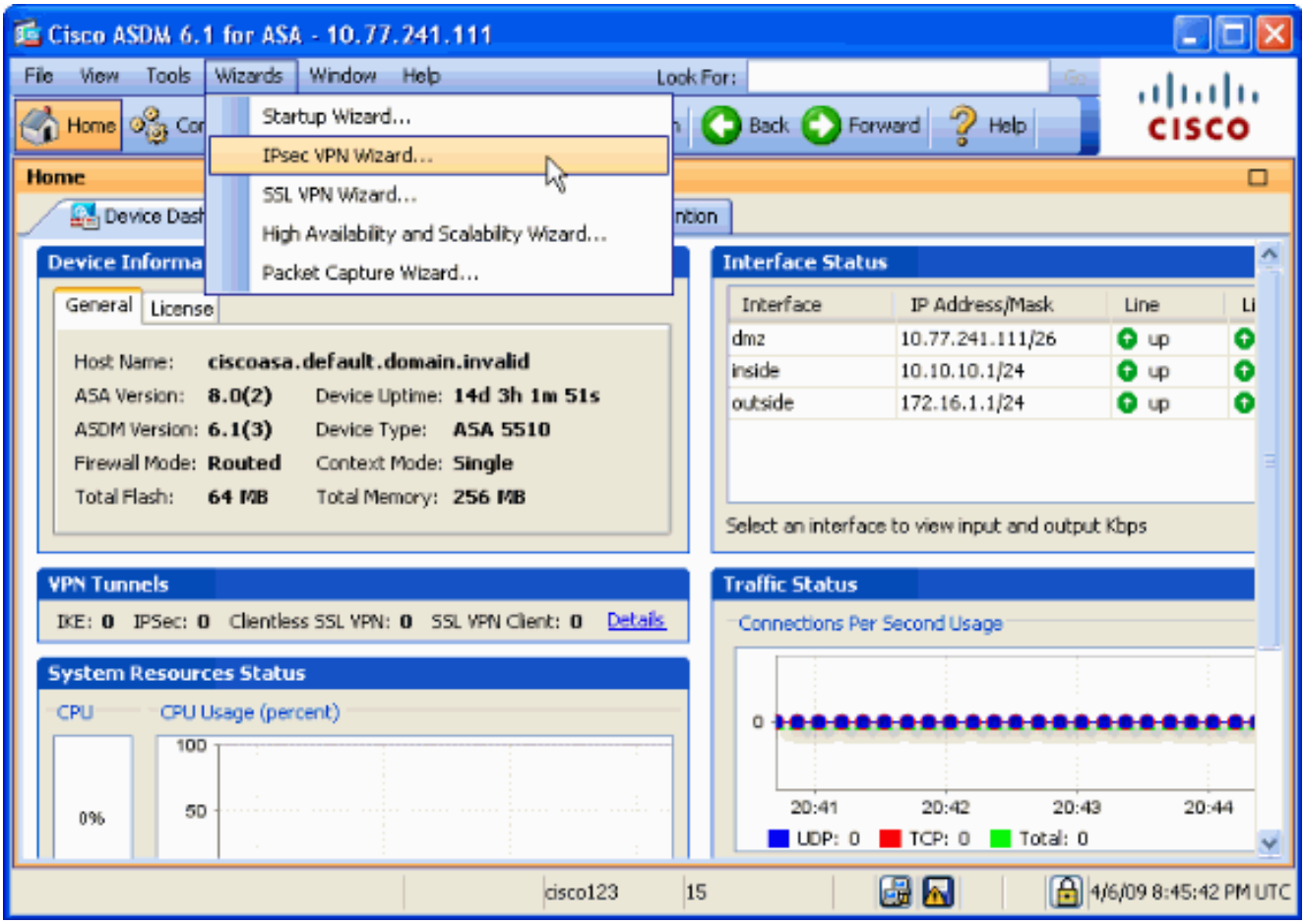


2. **Нажмите кнопку Download ASDM Launcher and Start ASDM, чтобы загрузить файл установки приложения ASDM.**
3. После загрузки ASDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco ASDM Launcher.
4. **Введите в поле Device 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.В этом примере используется имя пользователя cisco123 и пароль**

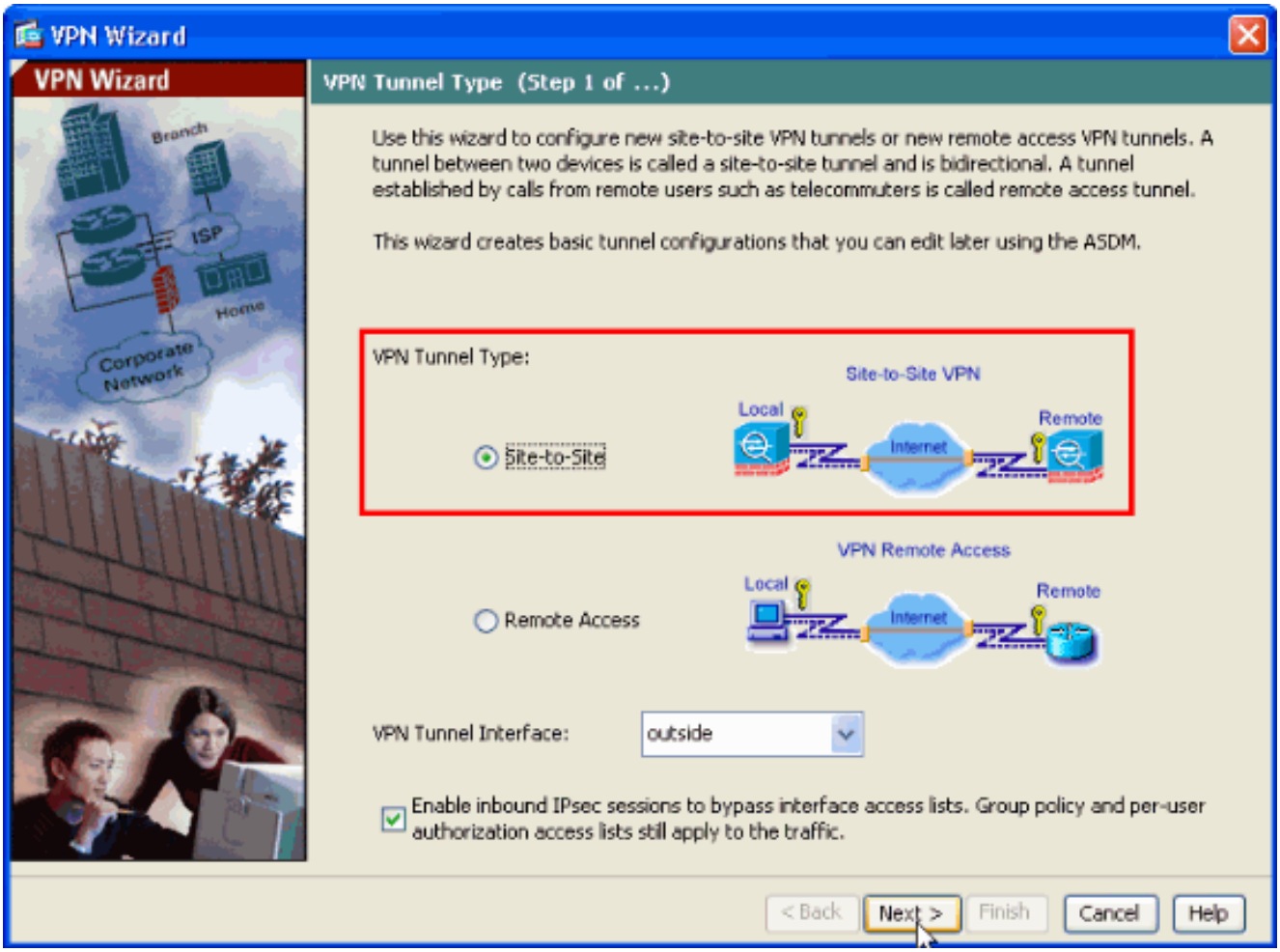


cisco123.

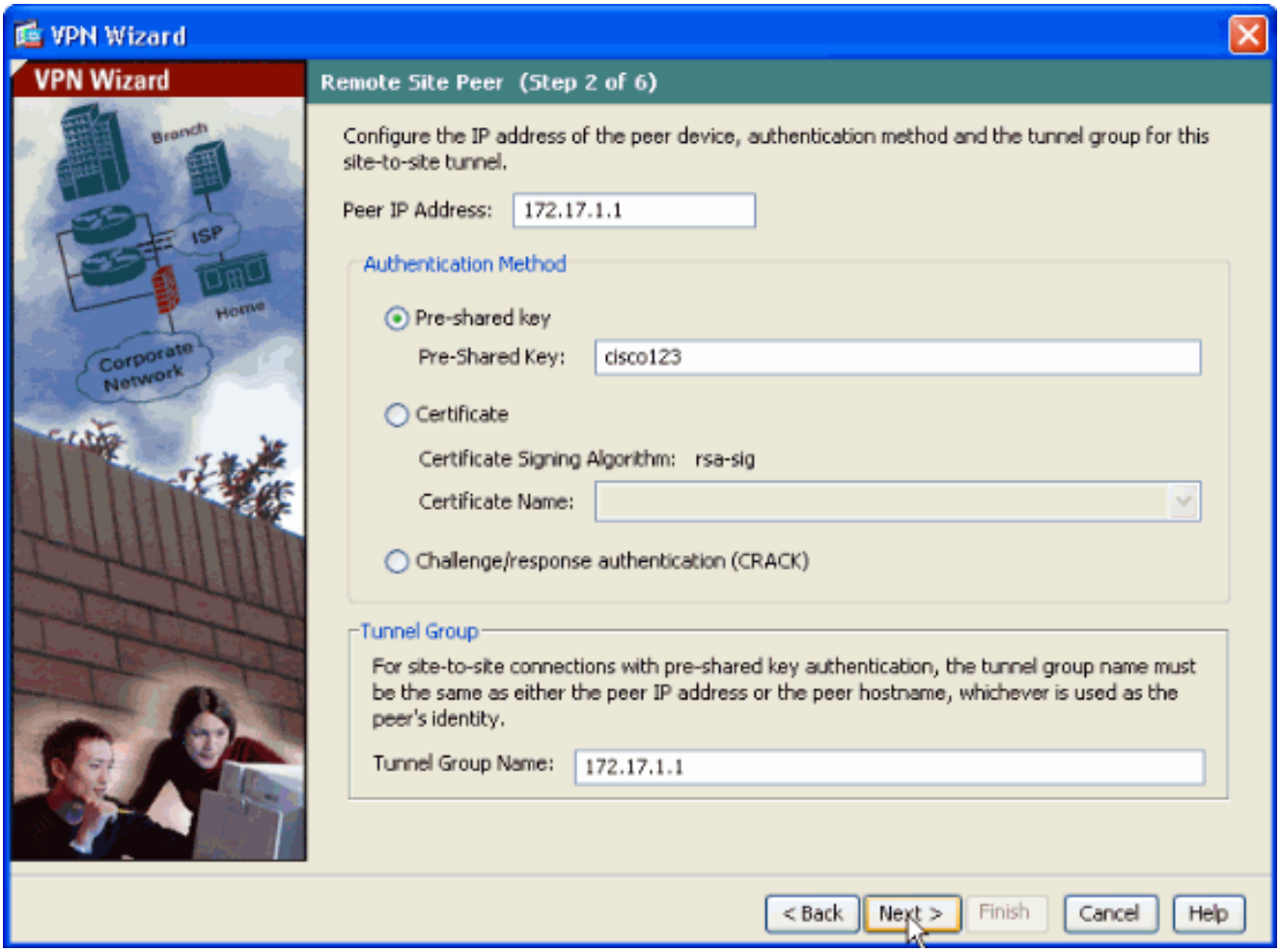
5. Запустите мастер настройки IPsec VPN Wizard, когда приложение ASDM соединится с ASA.



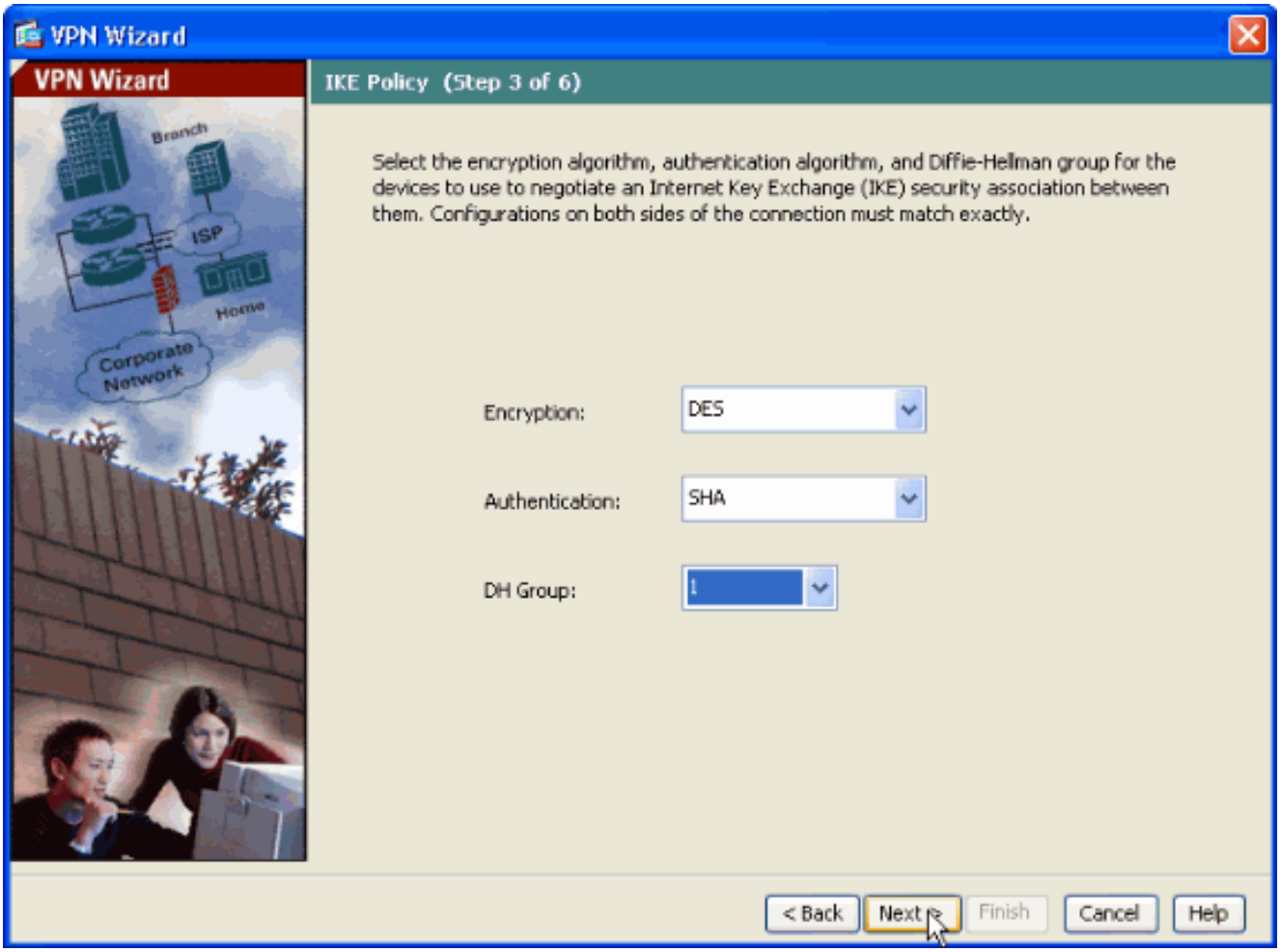
6. Установите переключатель "IPsec VPN tunnel type" в положение Site-to-Site и нажмите кнопку Next, как показано на
рисунке.



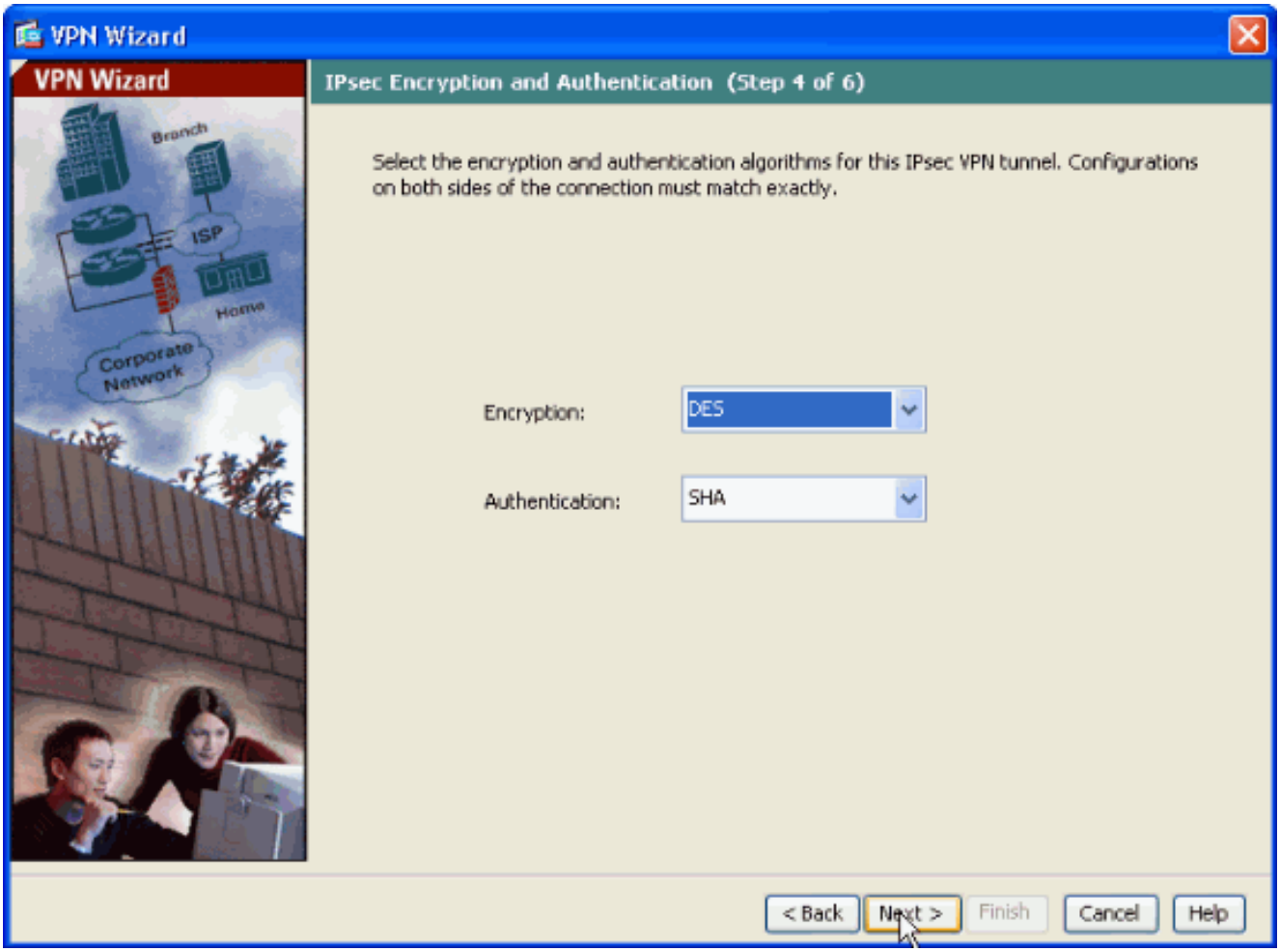
7. Укажите внешний IP-адрес удаленного узла. Введите данные для аутентификации (в этом примере используется ключ, согласованный ранее). **Название ключа cisco123. При настройке VPN-соединения ЛВС-ЛВС внешним IP-адресом по умолчанию будет Tunnel Group Name. Нажмите кнопку**
Next.



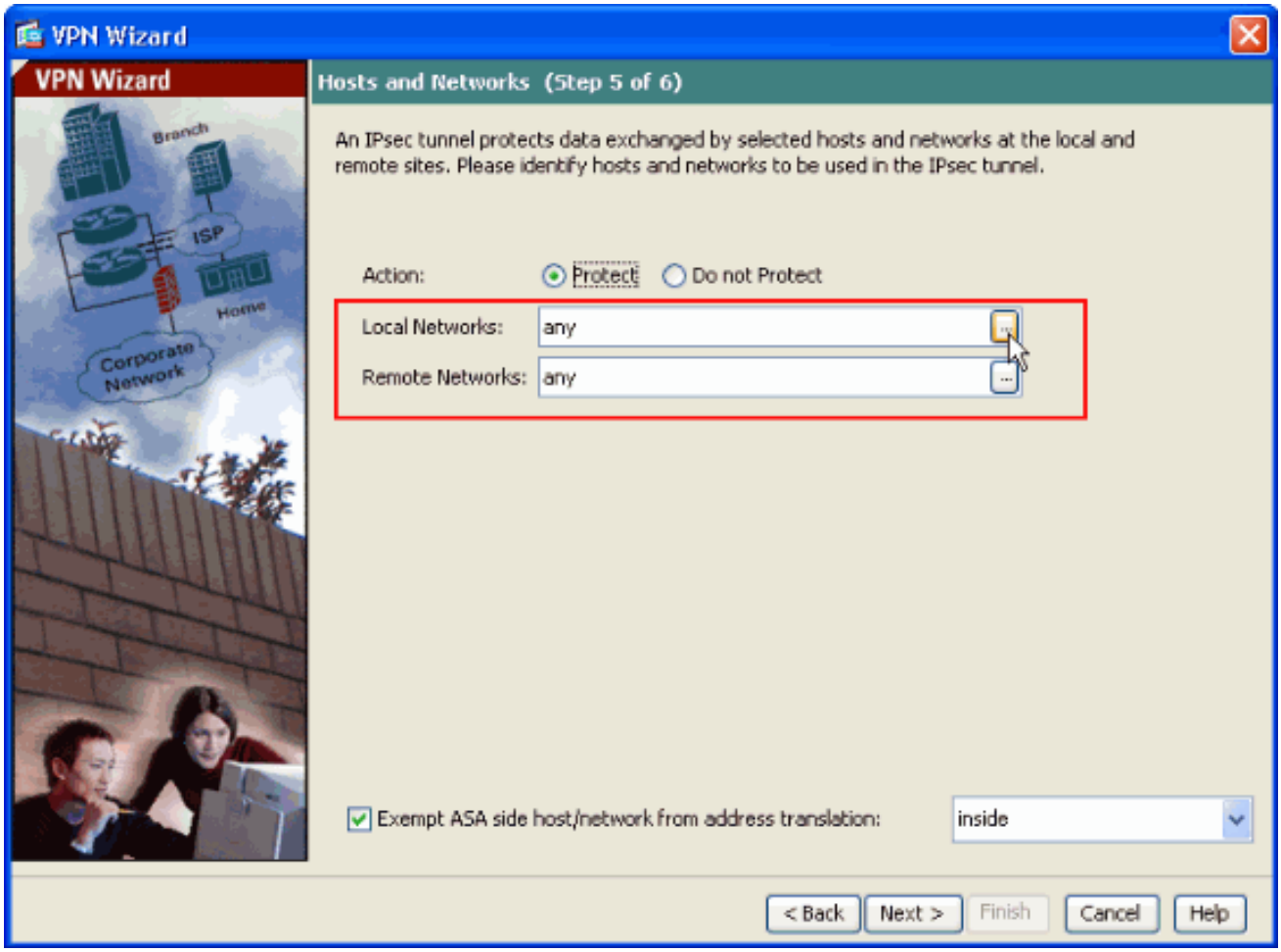
8. Укажите для IKE атрибуты (этот этап известен как "Фаза 1"). Эти атрибуты на устройстве защиты ASA и маршрутизаторе IOS должны быть одинаковыми. **Нажмите кнопку Next.**



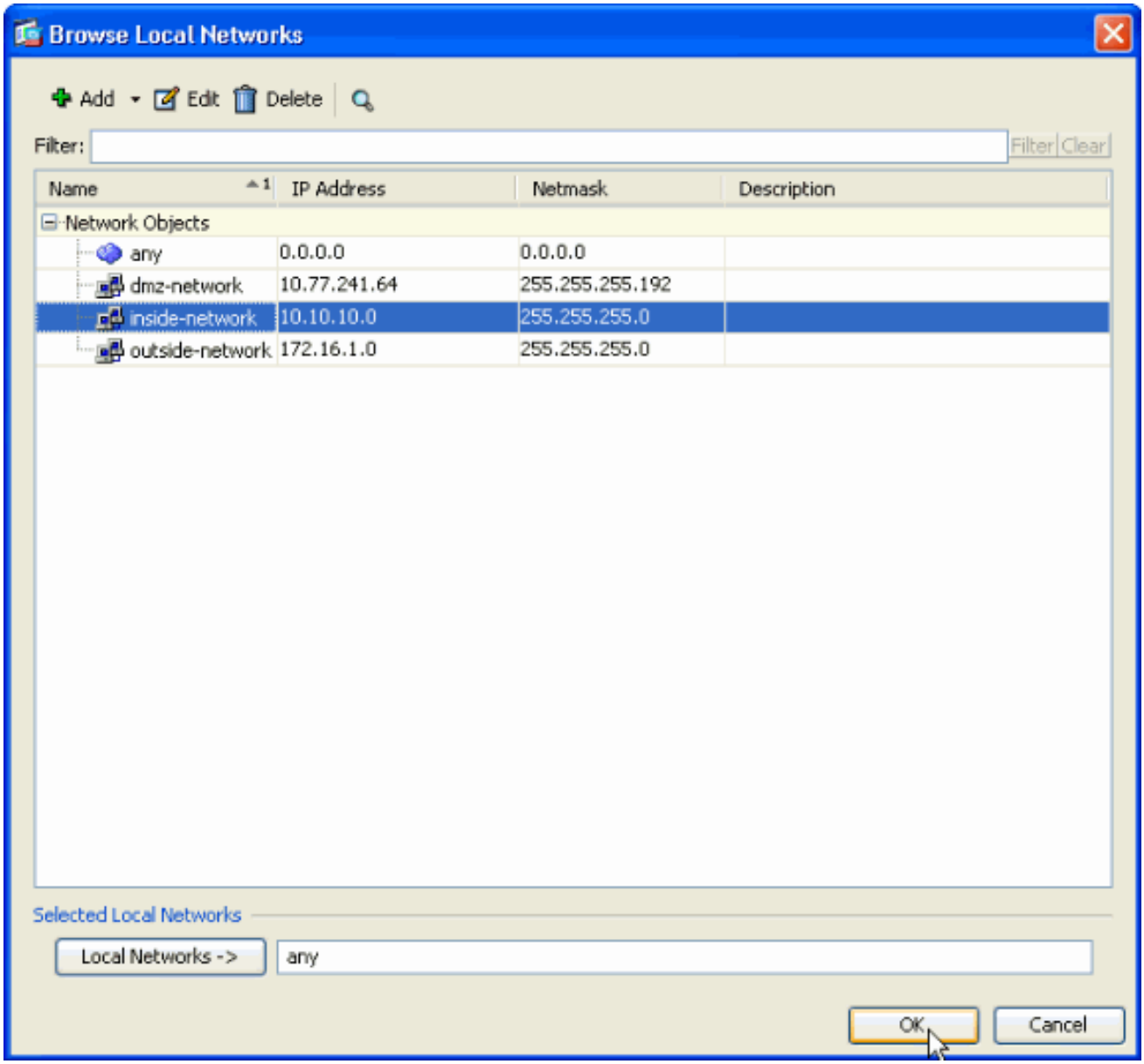
9. Укажите атрибуты для использования протокола IPsec (это "Этап 2"). Эти атрибуты на устройстве защиты ASA и маршрутизаторе IOS должны быть одинаковыми. **Нажмите кнопку Next.**



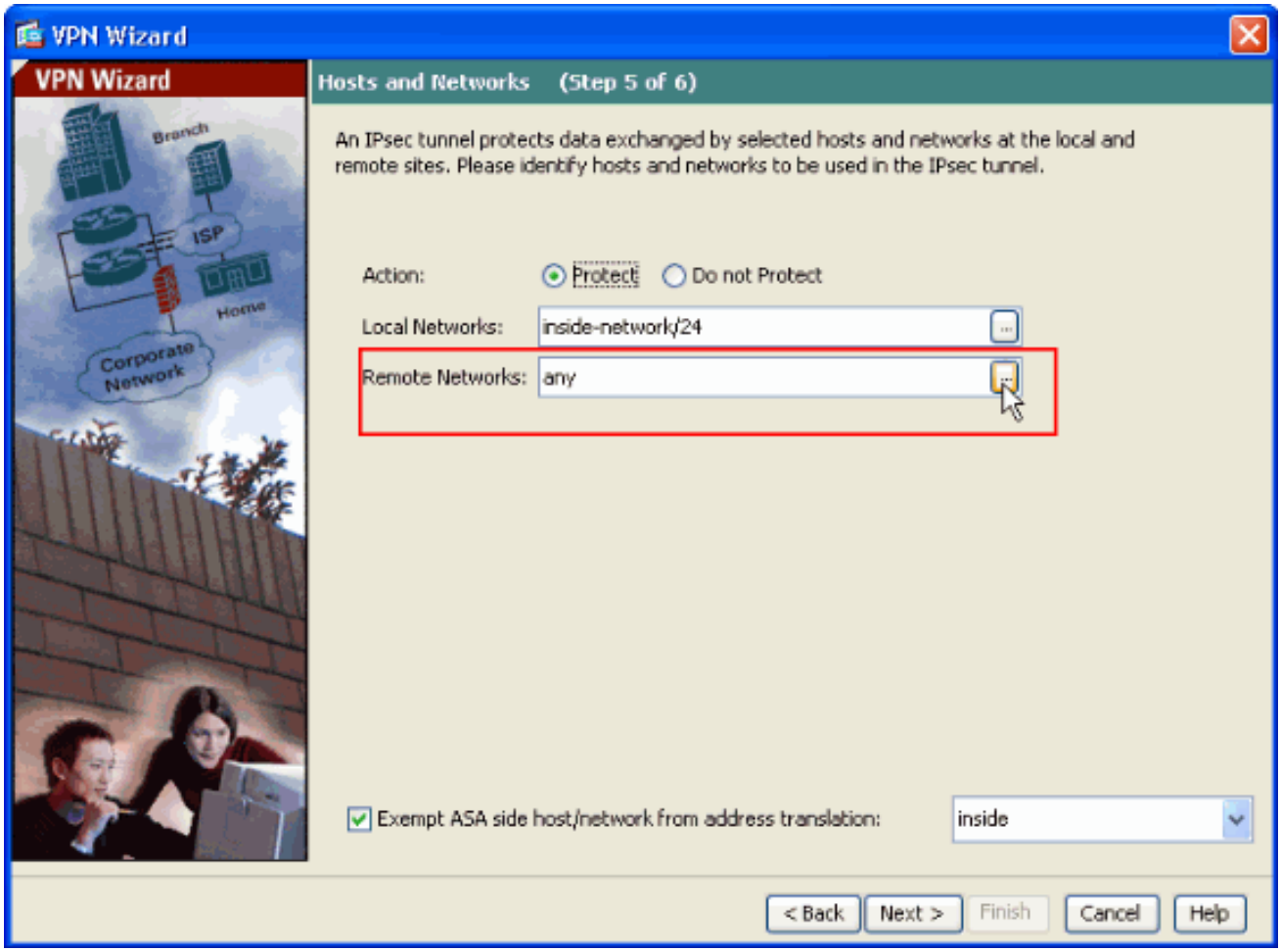
10. Укажите хосты, трафик которых будет разрешен через VPN-туннель. **На этом шаге необходимо будет указать локальную (Local) и удаленные (Remote Networks) сети для VPN-туннеля. Нажмите на кнопку, расположенную рядом с полем Local Networks, как показано на рисунке, чтобы выбрать адрес локальной сети из раскрывающегося списка.**



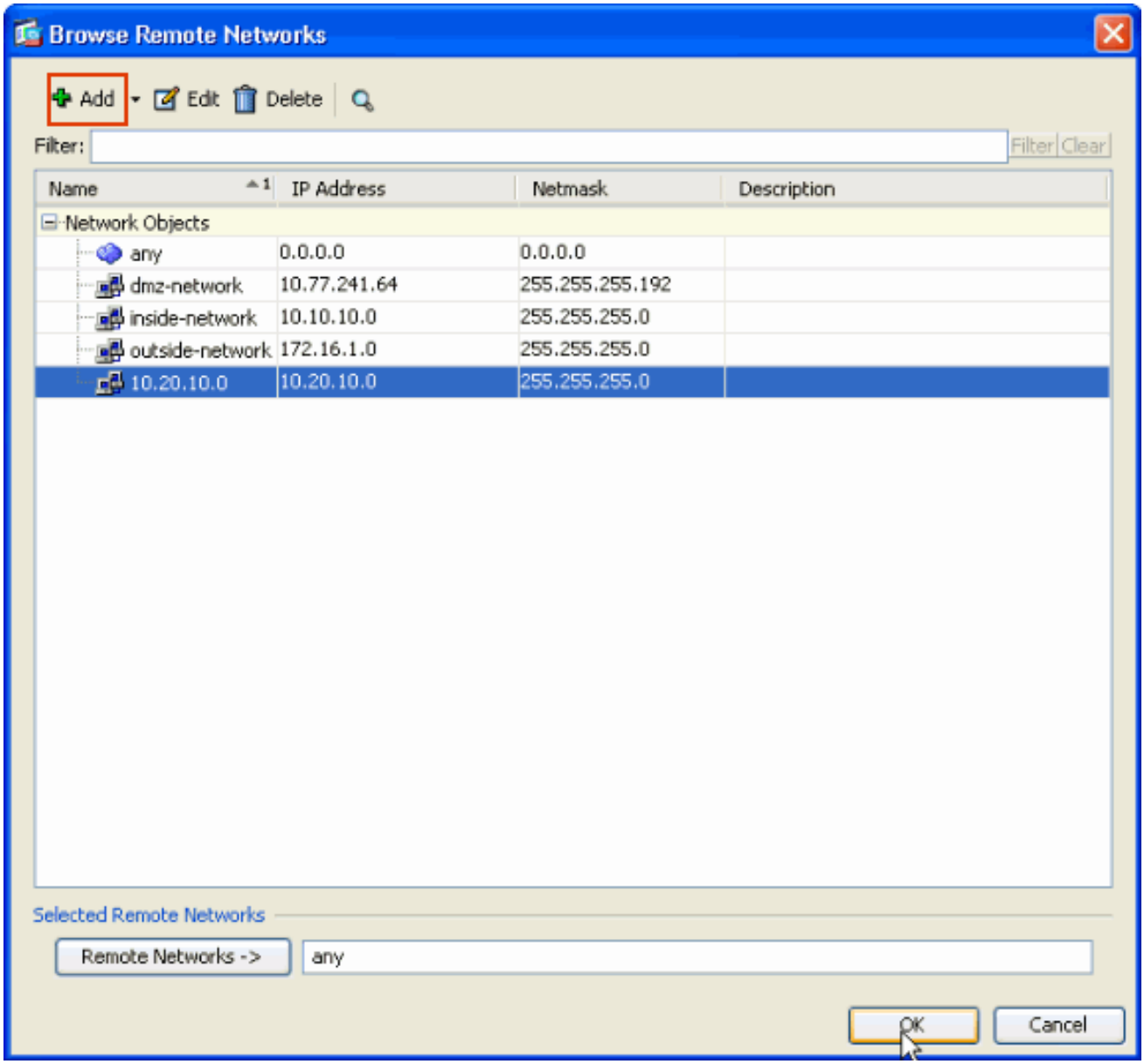
11. Выберите адрес локальной сети и нажмите кнопку OK, как показано на рисунке.



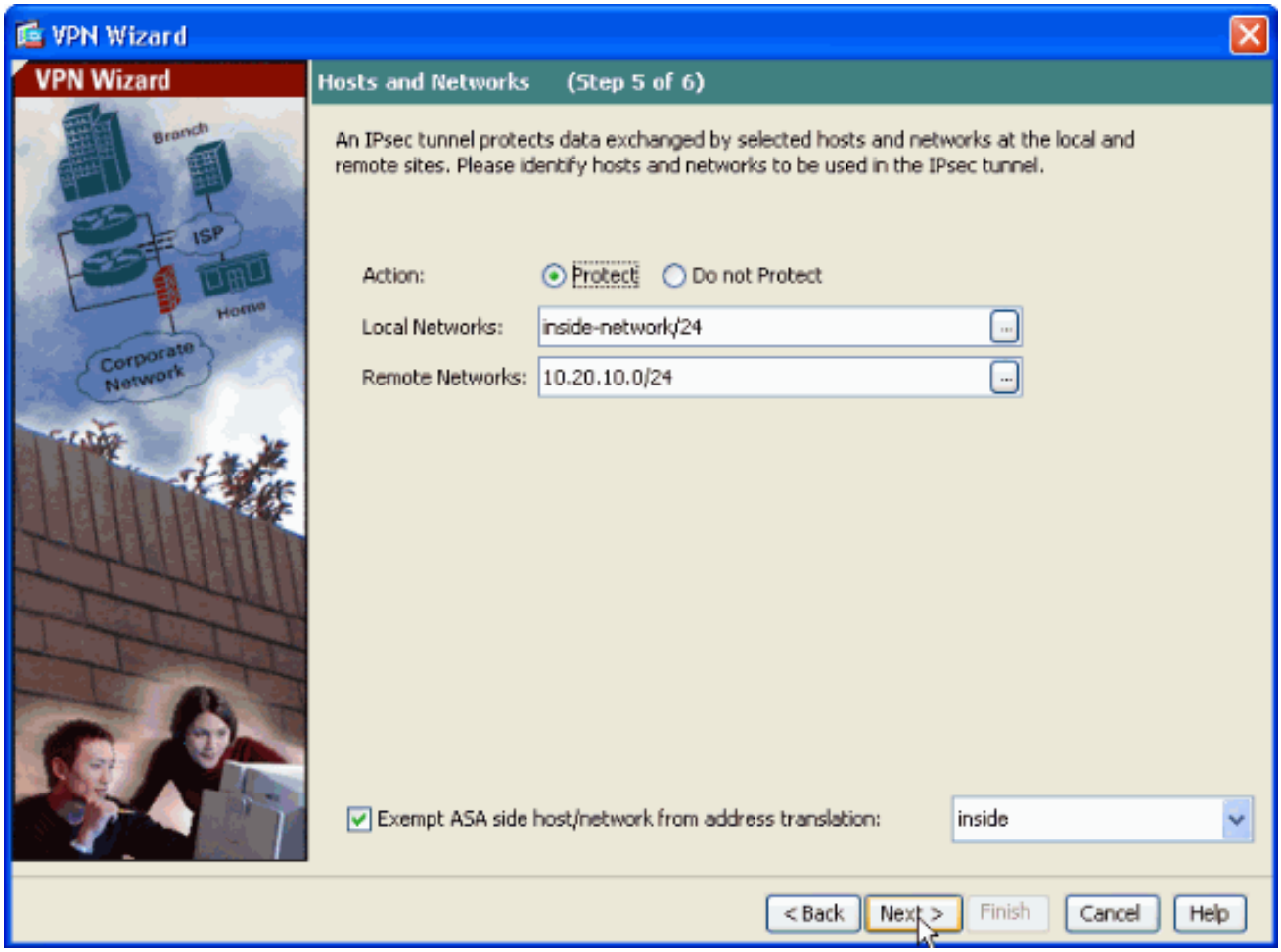
12. Нажмите на кнопку, расположенную рядом с полем Remote Networks, как показано на рисунке, чтобы выбрать адрес удаленной сети из раскрывающегося списка.



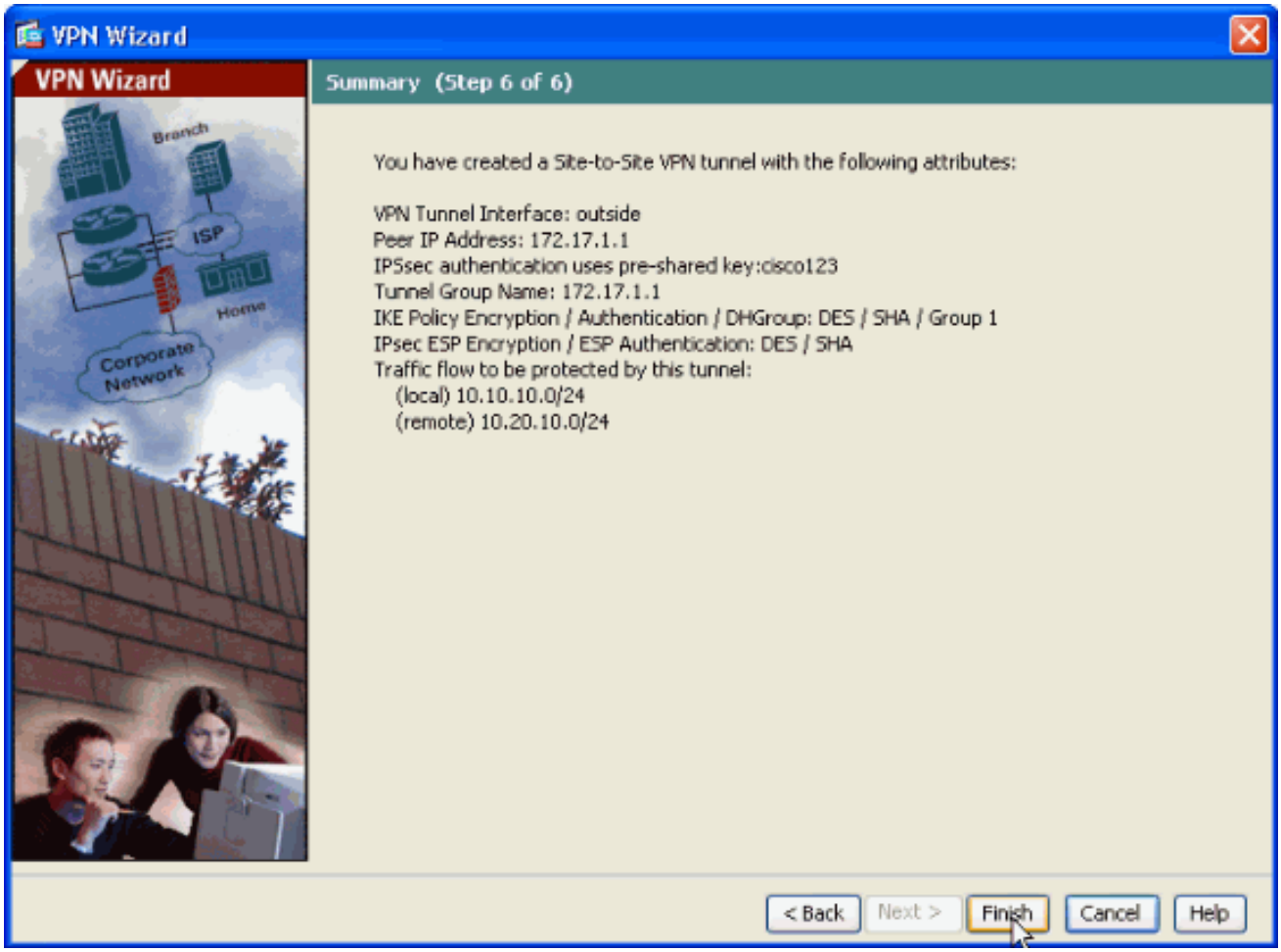
13. **Выберите адрес удаленной сети и нажмите кнопку OK, как показано на рисунке.Примечание:** Если у вас нет Удаленной сети в списке тогда, сеть должна быть добавлена к списку путем **нажмите**
Add.



14. Установите флажок Exempt ASA side host/network from address translation, чтобы исключить траффик туннеля от его обработки с помощью NAT. Нажмите кнопку Next.



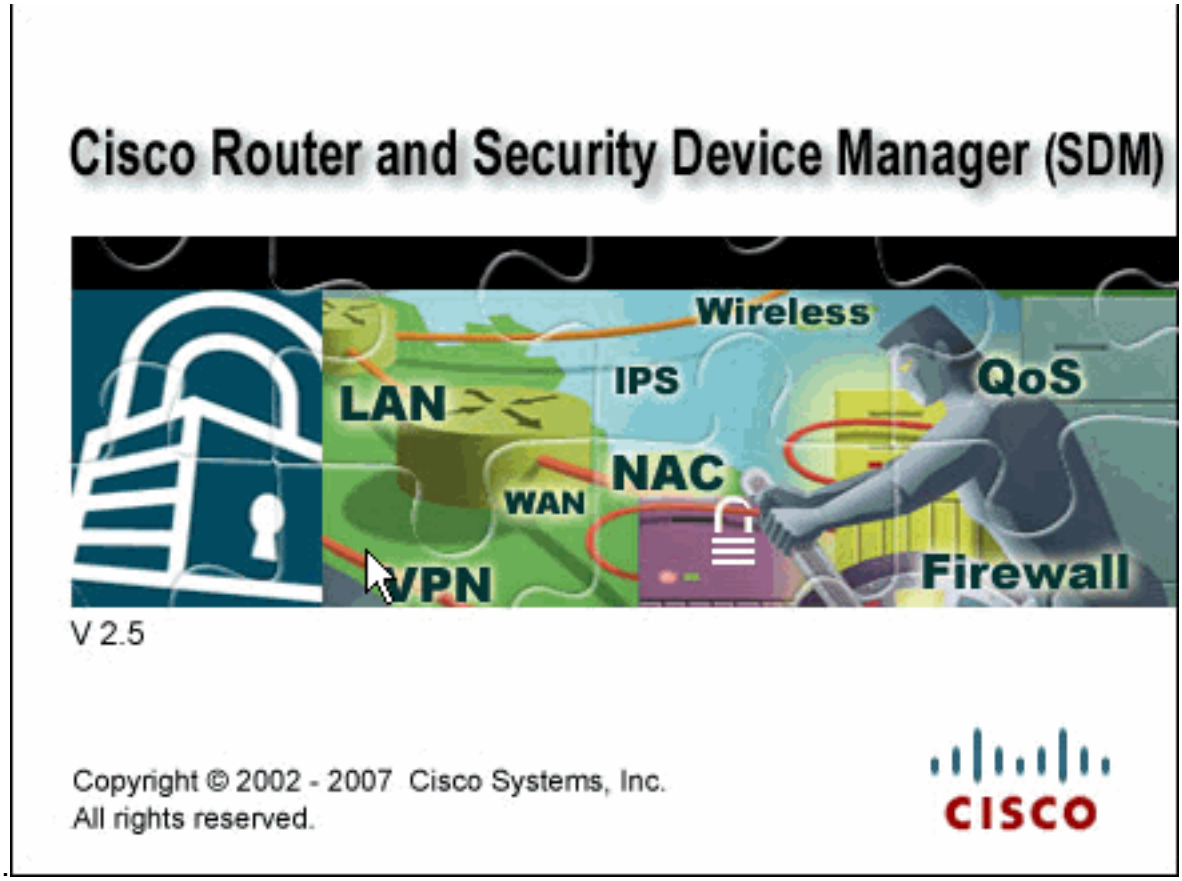
15. Все параметры, установленные с помощью мастера "VPN Wizard" отобразятся на странице "Summary". **Дважды проверьте настройки и, если они верны, нажмите кнопку Finish.**



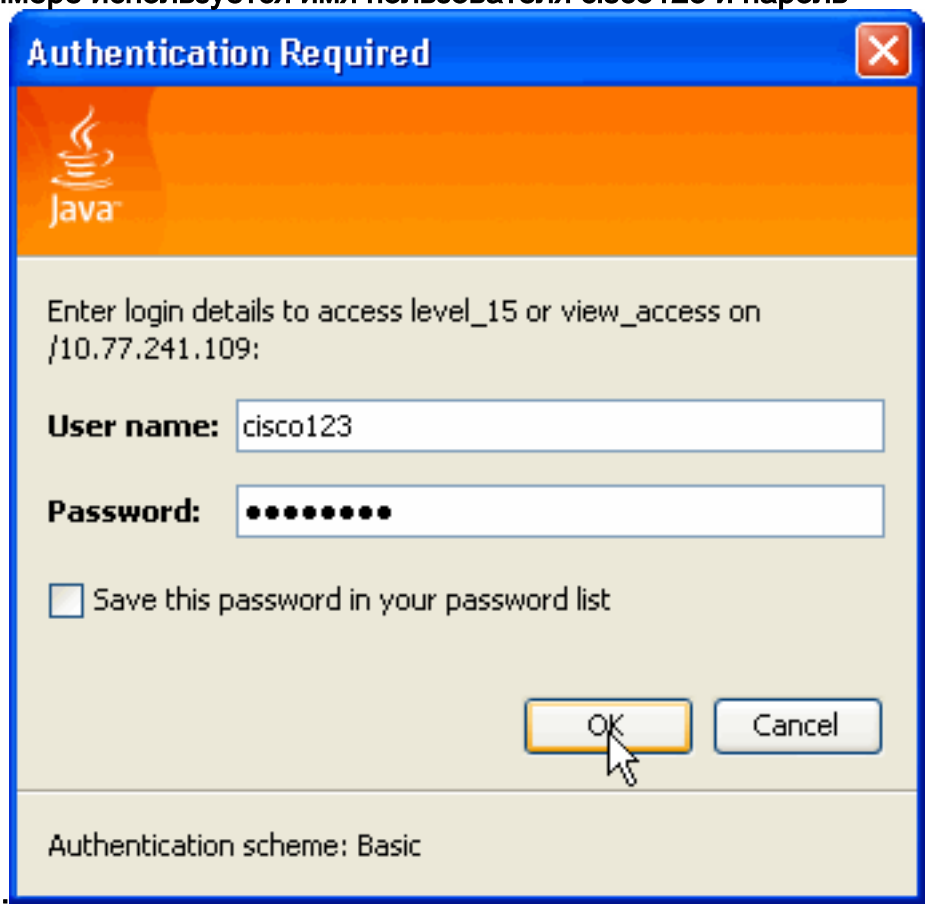
Настройка маршрутизатора с помощью SDM

Выполните эти шаги, чтобы настроить VPN-туннель "ЛВС-ЛВС" на маршрутизаторе Cisco IOS:

1. **Откройте браузер и введите адрес https://<IP_адрес интерфейса_маршрутизатора,_который_необходимо_настроить_для_доступа_SDM>, чтобы подключиться к SDM на маршрутизаторе.**Отвечайте на все предупреждения, связанные с проверкой SSL-сертификата, выдаваемые браузером. По умолчанию имя пользователя и пароль являются пустыми.Маршрутизатор отобразит следующее окно для загрузки приложения SDM. В данном примере используется приложение, загруженное на локальный компьютер, а не приложение

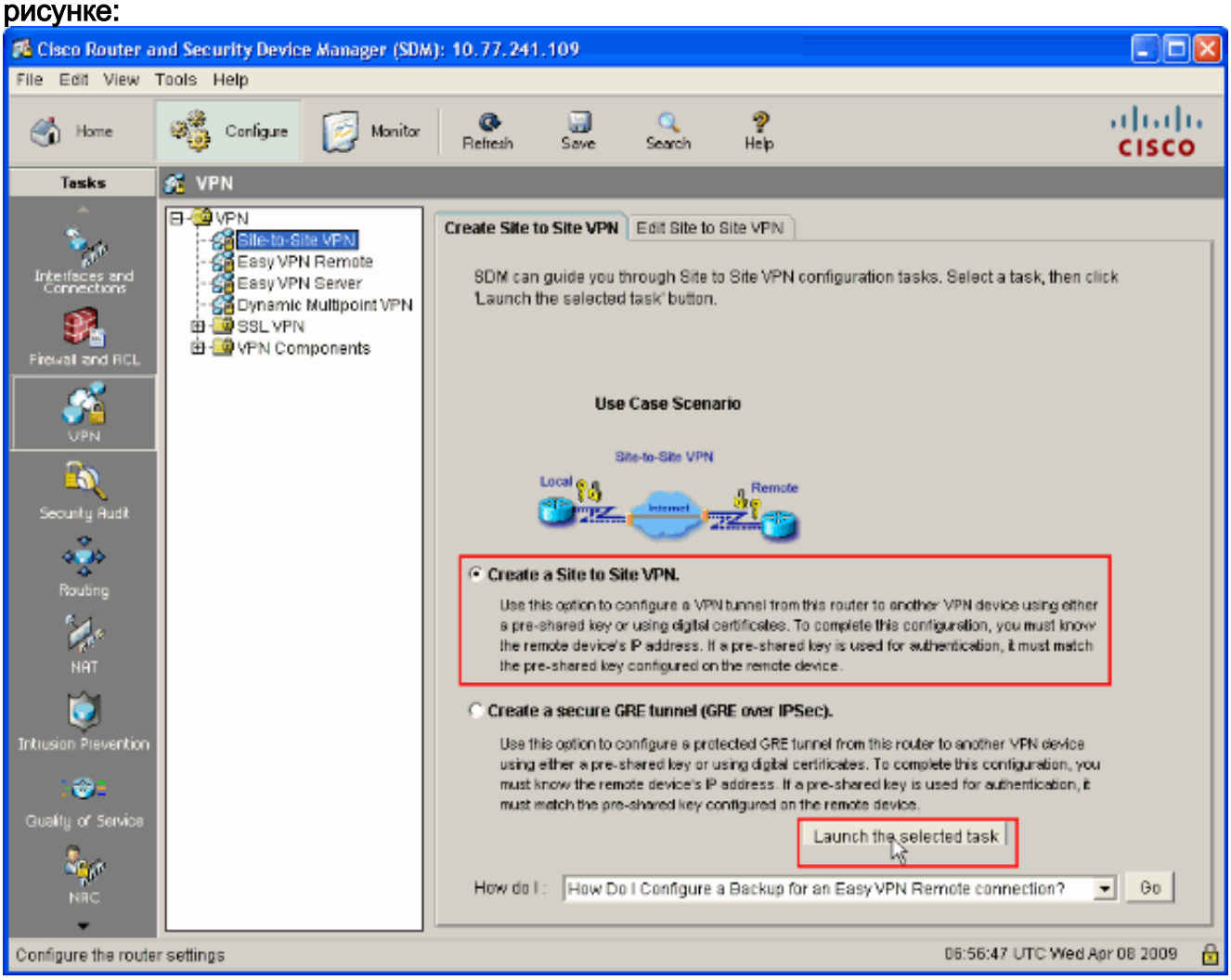
Java. 

2. Начнется загрузка SDM. После загрузки SDM Launcher выполните все шаги, сопровождаемые соответствующими подсказками, необходимые для установки приложения и запуска Cisco SDM Launcher.
3. **Введите имя пользователя и пароль (если вы их ранее указали) и нажмите кнопку OK.В этом примере используется имя пользователя cisco123 и пароль**

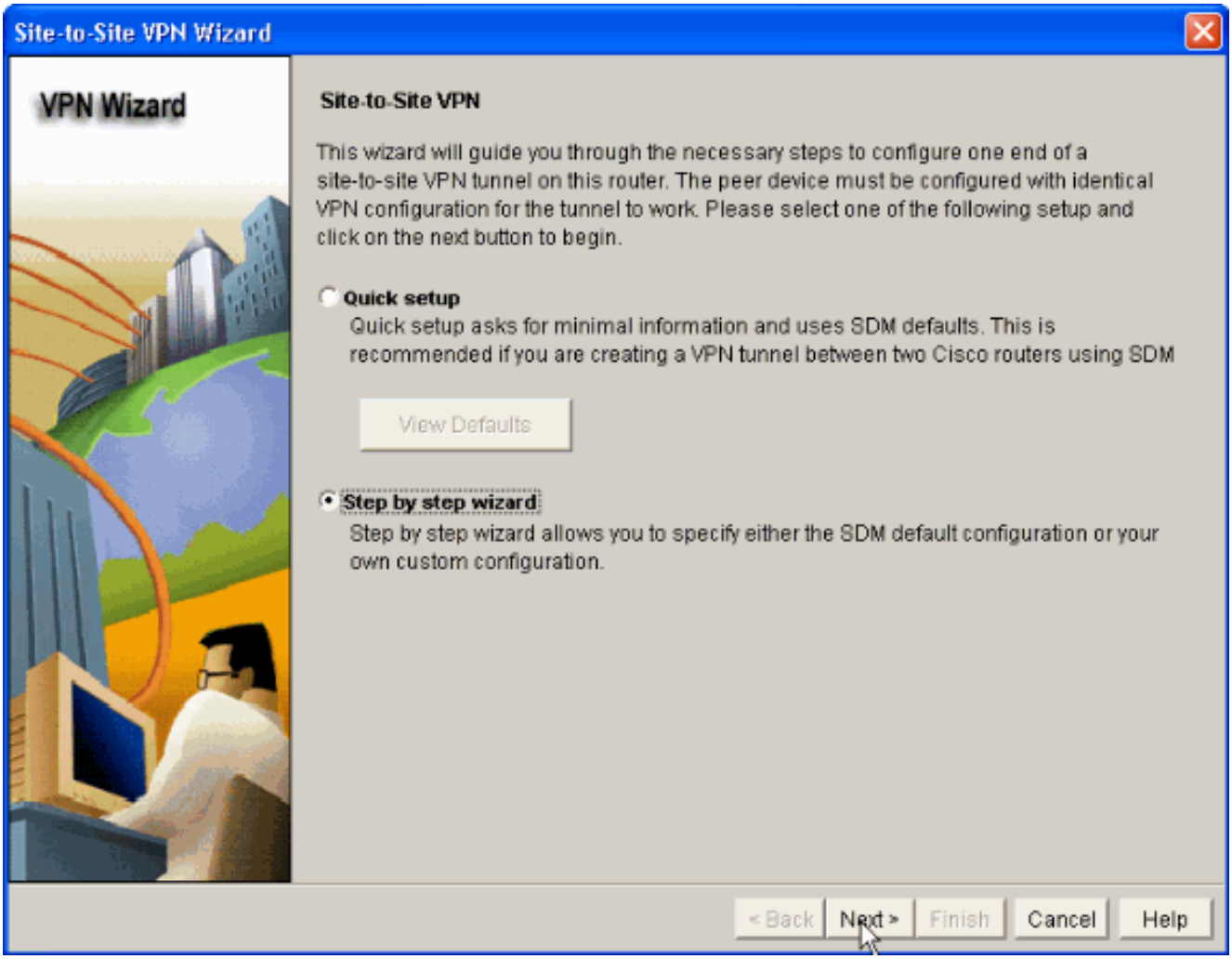


cisco123.
4. **Последовательно выберите Configuration->VPN->Site-to-Site VPN и установите**

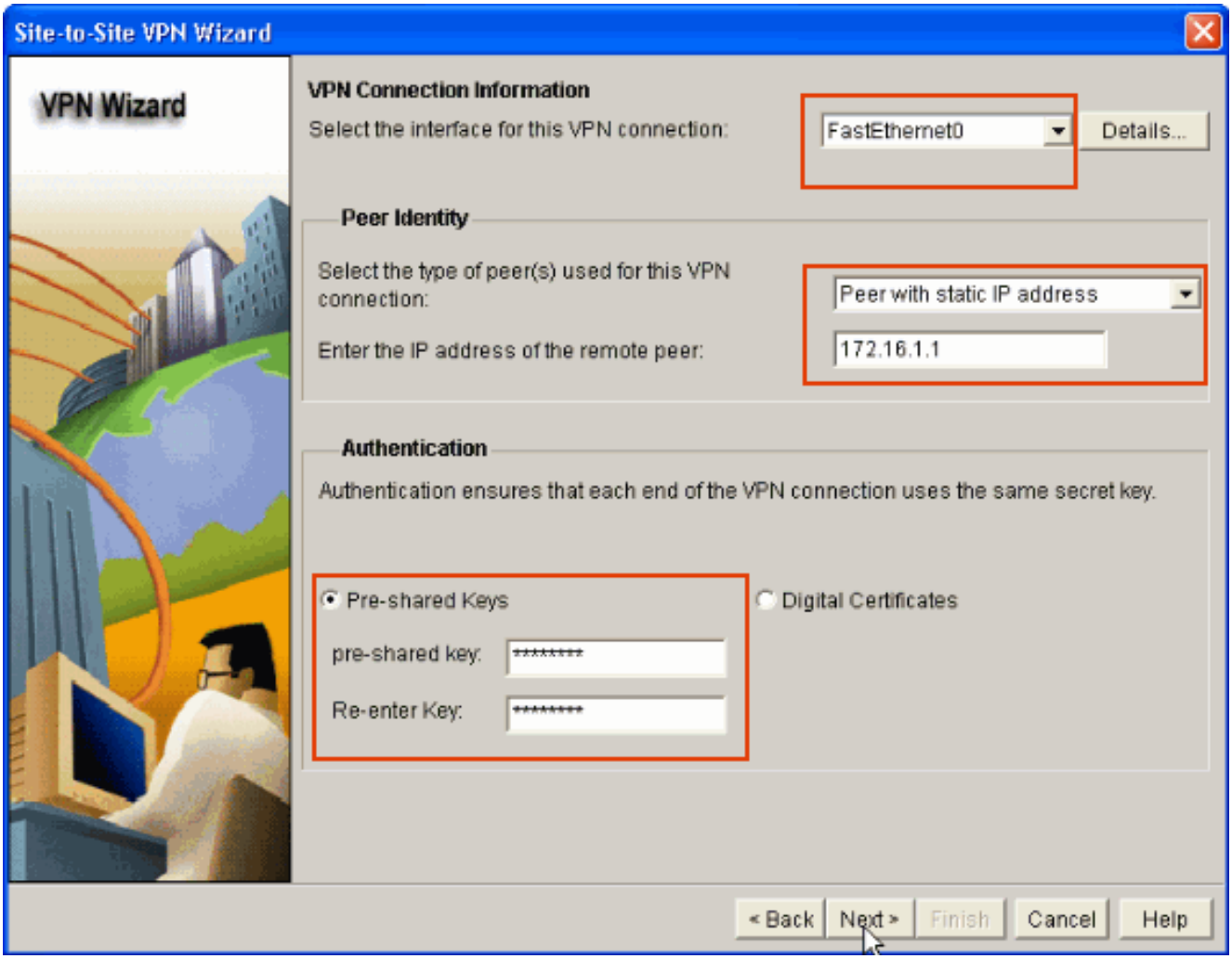
переключатель в положение Create a Site-to-Site VPN на начальной странице SDM. После этого нажмите кнопку Launch The selected Task, как показано на рисунке:



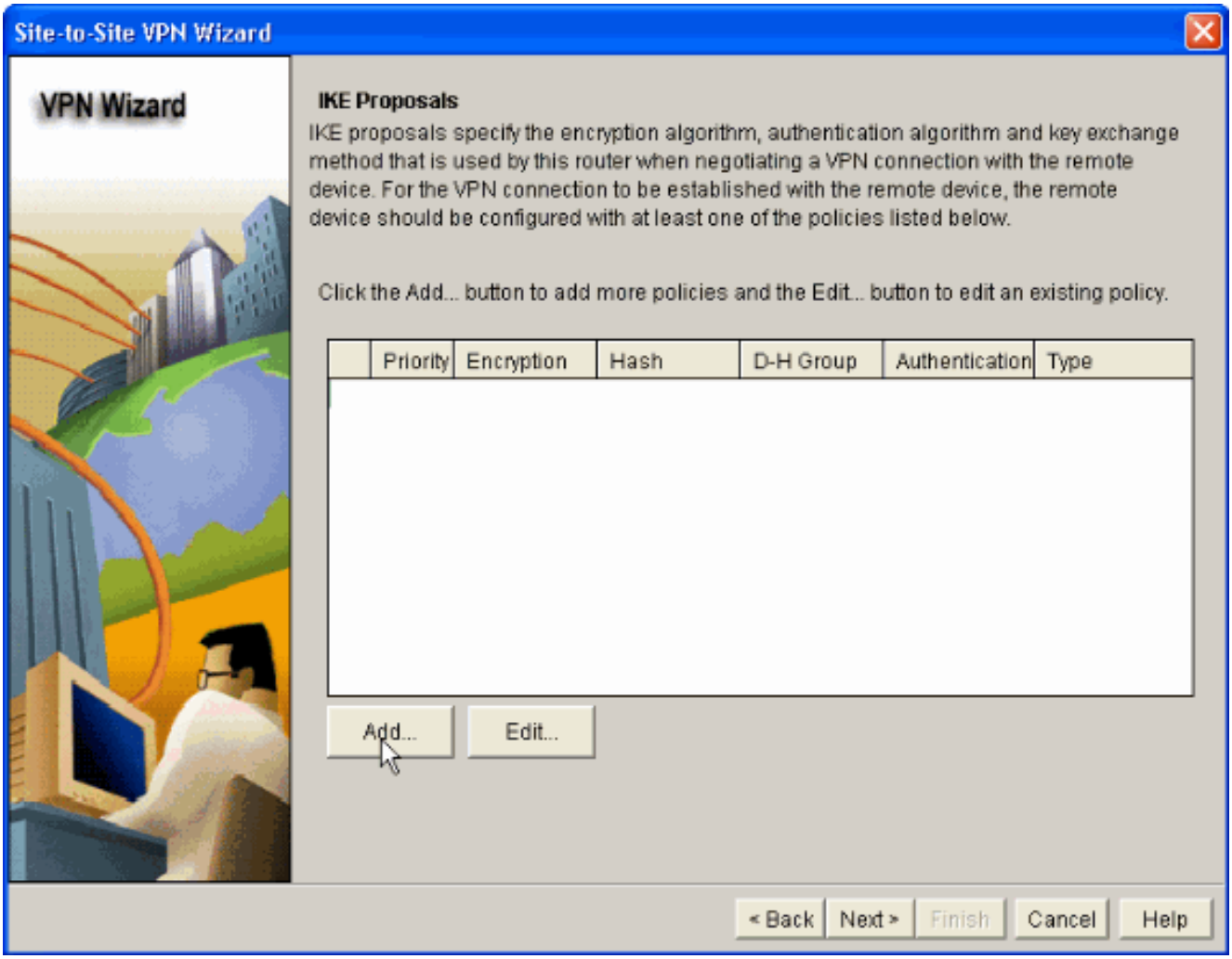
5. Установите переключатель в положение Step by step wizard для продолжения настройки:



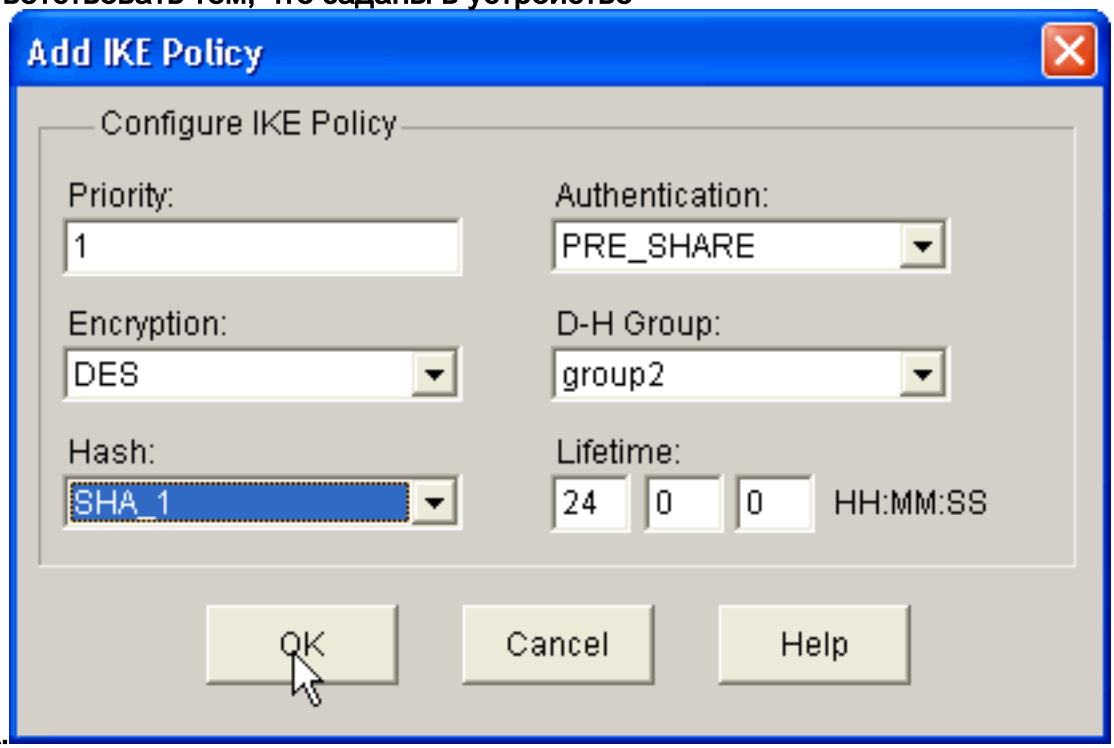
6. **В окне VPN Connection Information в соответствующих полях указывается информация о VPN-соединении.** В раскрывающемся списке выберите интерфейс VPN-туннеля. **В этом примере выбран FastEthernet0. В разделе Peer Identity выберите Peer with static IP address из списка и укажите IP-адрес удаленного узла. Затем в разделе "Authentication" установите переключатель в положение Pre-shared key и введите ключ (в этом примере используется ключ cisco123). Нажмите кнопку**
Next.



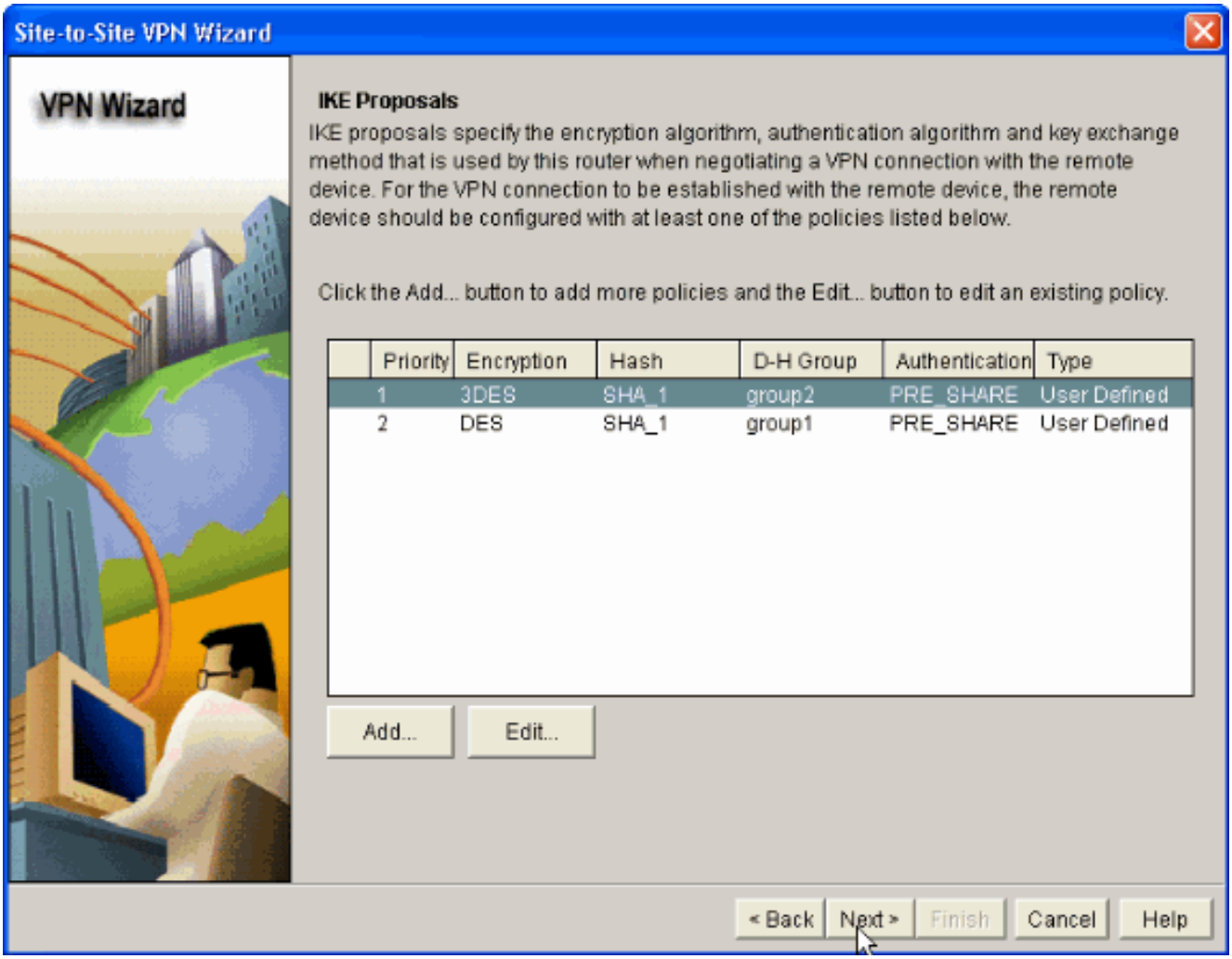
7. Нажмите кнопку Add, чтобы добавить предложения IKE, которые определяют метод шифрования, алгоритм аутентификации (Encryption Algorithm, Authentication Algorithm) и метод обмена ключами (Key Exchange
Method).



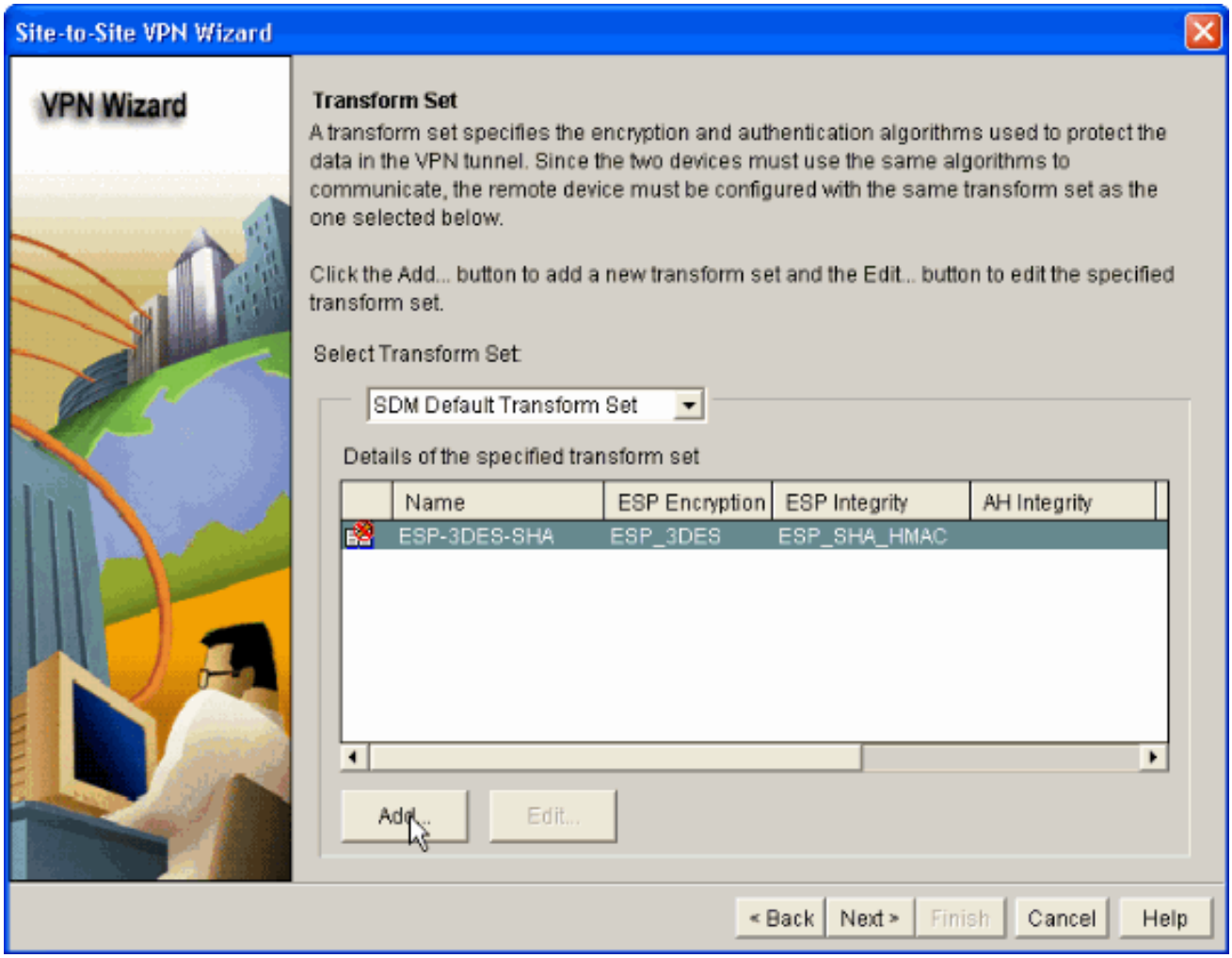
8. Укажите алгоритм шифрования, алгоритм аутентификации и метод обмена ключами, как показано на рисунке, после чего нажмите кнопку OK. Значения алгоритма шифрования, алгоритма аутентификации и метода обмена ключами должны соответствовать тем, что заданы в устройстве ASA.



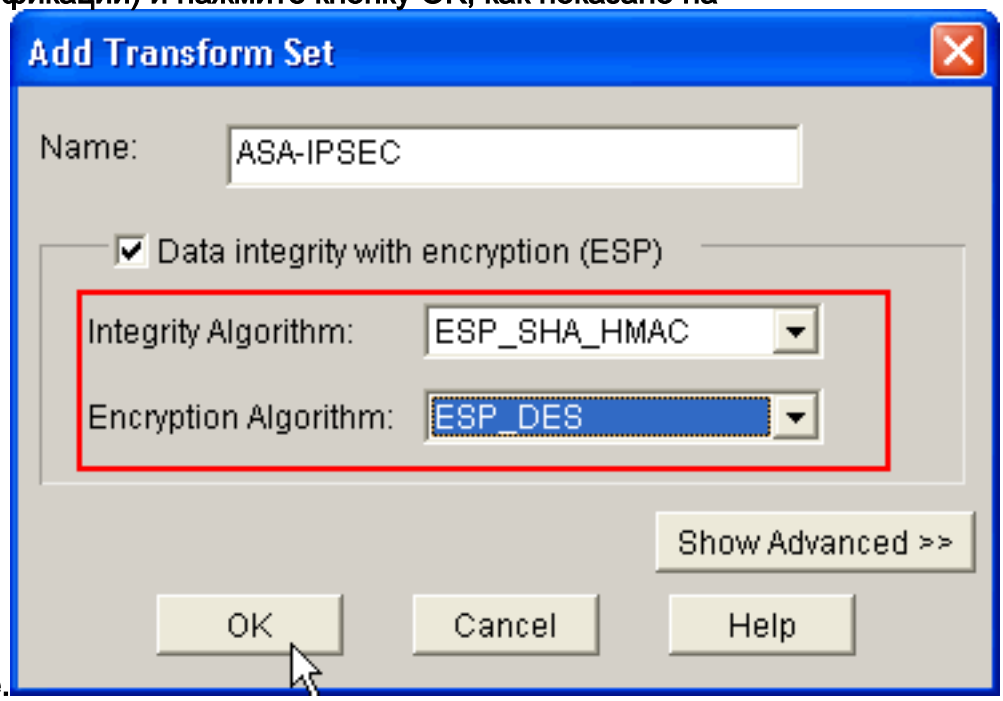
9. Нажмите кнопку Next как показано на рисунке.



10. В этом новом окне необходимо ввести дополнительные данные о наборе преобразований (Transform Set). Набор преобразований задаются алгоритмы шифрования и аутентификации, используемые для защиты данных в VPN-туннеле. Нажмите кнопку Add, чтобы указать эти дополнительные данные. Можно задать столько наборов преобразований, сколько необходимо, нажимая кнопку Add и указывая дополнительные
данные.

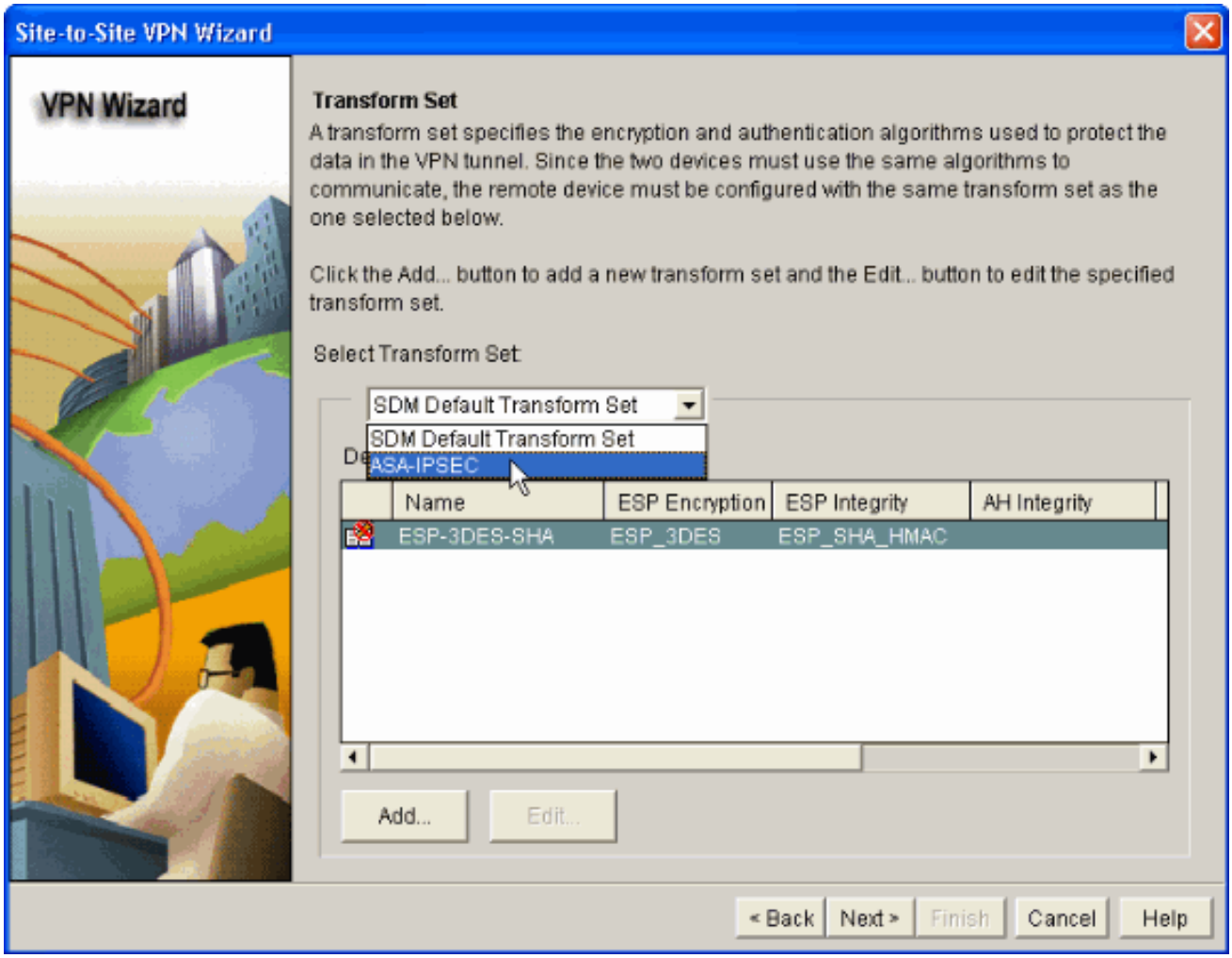


11. Укажите дополнительные данные набора преобразований (алгоритмы шифрования и аутентификации) и нажмите кнопку OK, как показано на

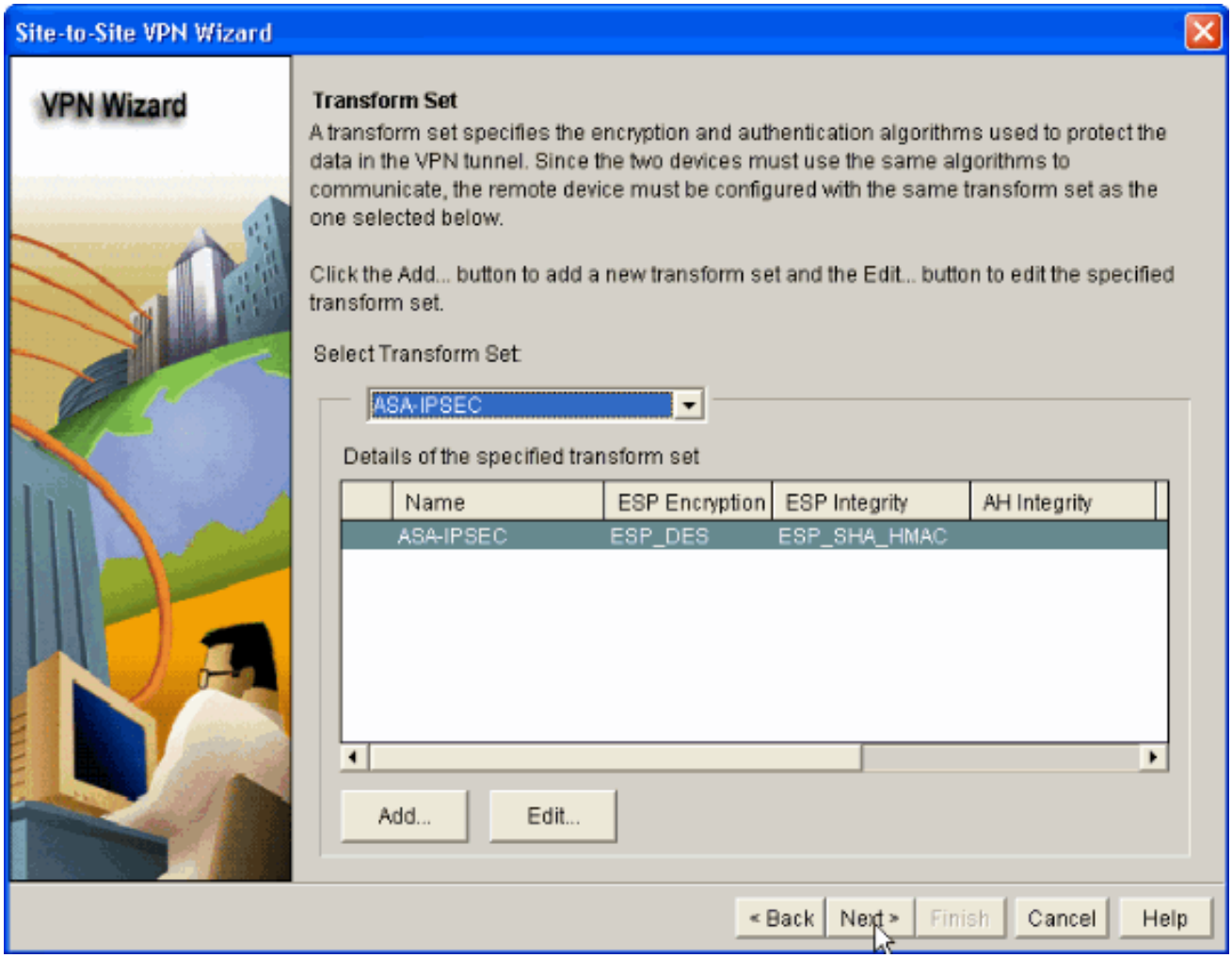


рисунке.

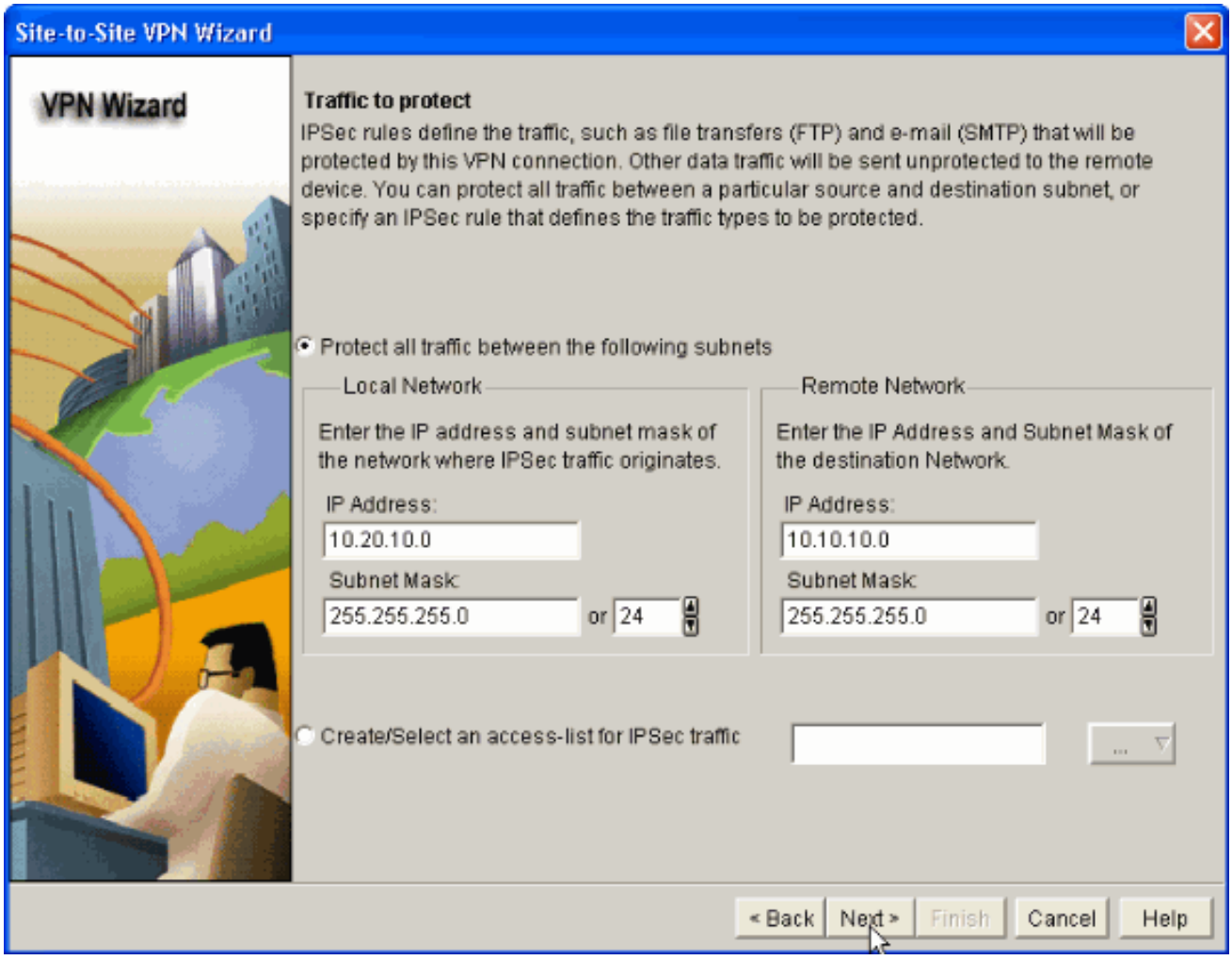
12. Выберите необходимый набор преобразований из выпадающего списка, как показано на
рисунке.



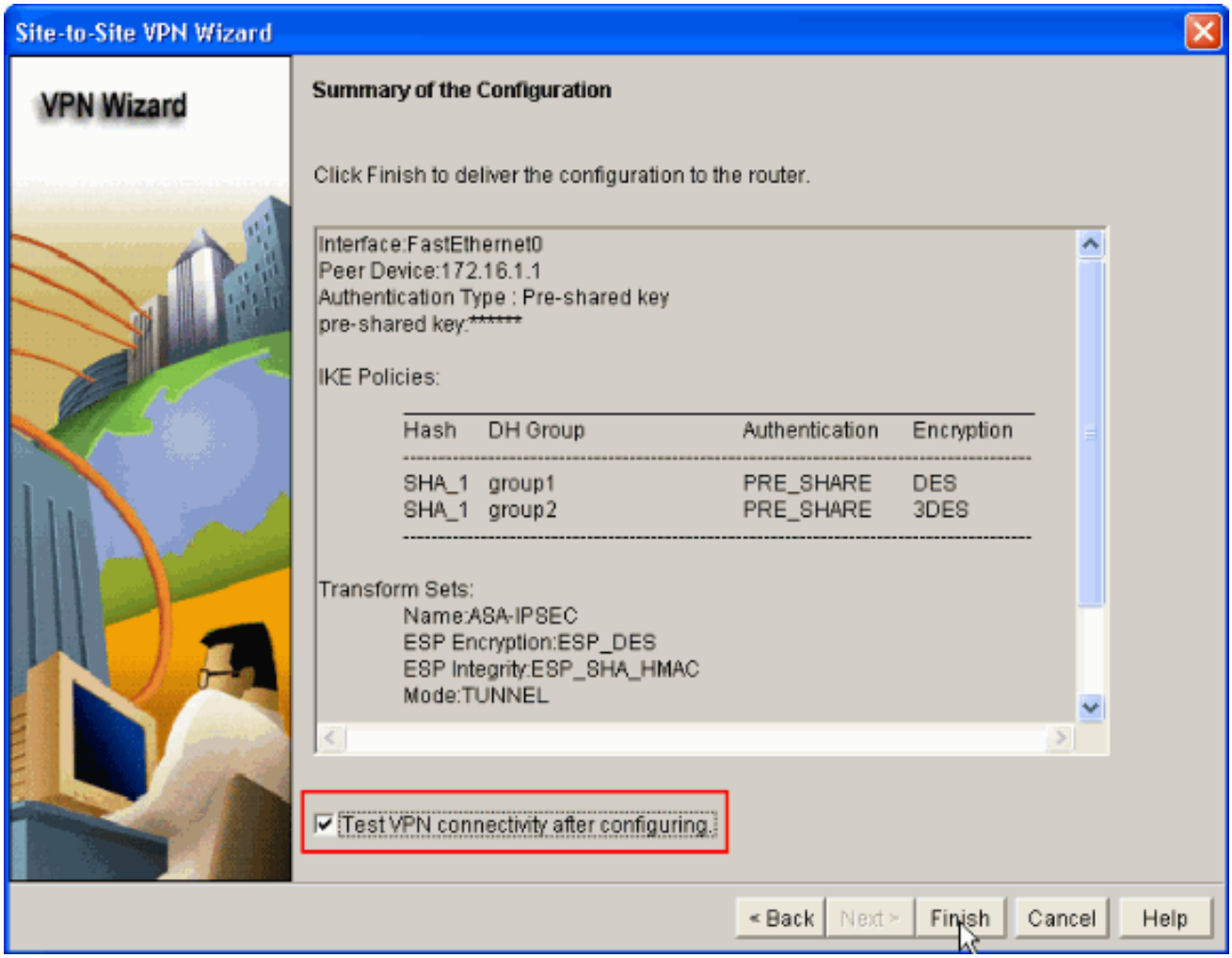
13. Нажмите кнопку **Next.**



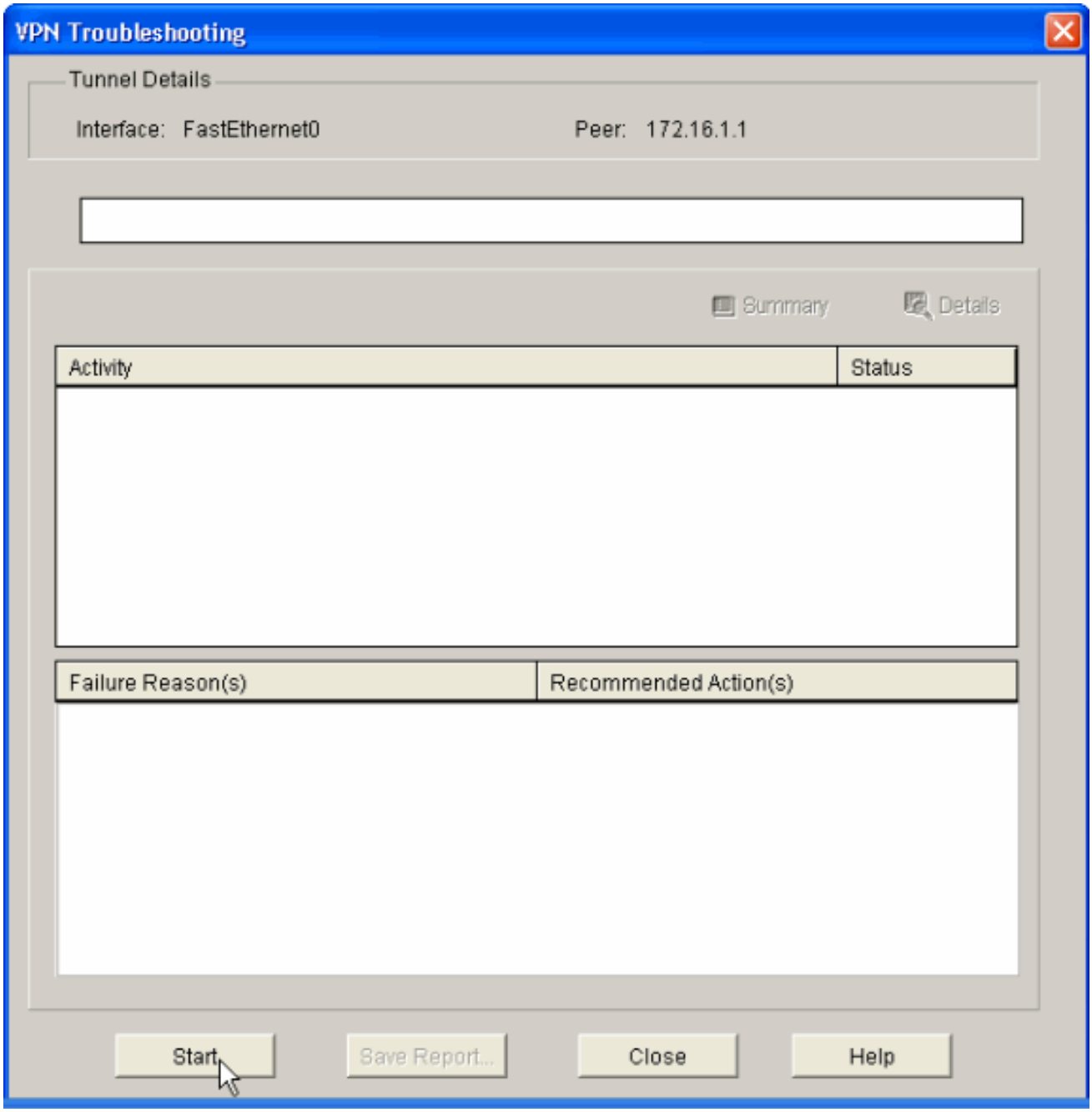
14. **В следующем окне необходимо указать трафик, подлежащий защите с помощью VPN-туннеля. Укажите исходную сеть и сеть назначения трафика, подлежащего защите, чтобы трафик между определенной исходной сетью и сетью назначения был защищен.** В этом примере в качестве исходной используется сеть с IP-адресом 10.20.10.0, а в качестве назначения - сеть с IP-адресом 10.10.10.0. **Нажмите кнопку Next.**



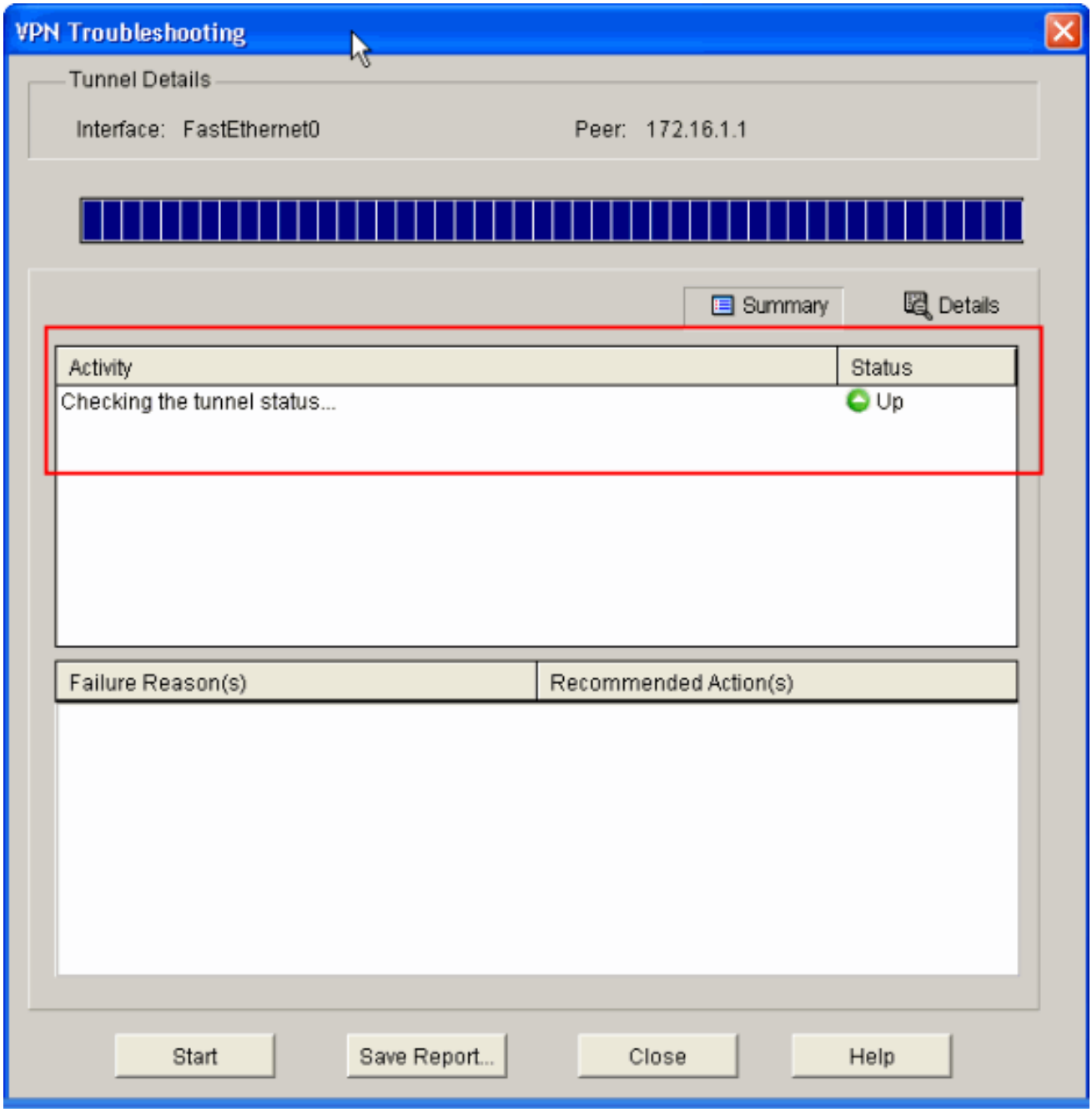
15. В этом окне отображается сводная информация о выполненной настройке VPN-соединения "ЛВС-ЛВС". **Установите флажок Test VPN Connectivity after configuring, если необходимо протестировать VPN-подключение.** В рисунке флажок отмечен, т. к. необходимо проверить подключение. **После этого нажмите кнопку Finish.**



16. Нажмите кнопку Start, как показано на рисунке, чтобы проверить VPN-соединение.



17. В следующем окне представлен результат проверки VPN-подключения. В нем можно увидеть состояние туннеля: Up (установлен) или Down (отключен). В этом примере конфигурации состояние туннеля указано как "Up" рядом с зеленым индикатором (т.е. установлен).



На этом процедура настройки маршрутизатора Cisco IOS завершена.

Конфигурация ASA в интерфейсе командной строки

ASA

```
ASA#show run : Saved ASA Version 8.0(2) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted names ! !---
Configure the outside interface. ! interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 !--- Configure the inside interface. !
interface Ethernet0/2 nameif inside security-level 100
ip address 10.10.10.1 255.255.255.0 !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any access-list inside_nat0_outbound extended
permit ip 10.10.10.0 255.255.255.0 10.20.10.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used !--- with the nat zero
command. This prevents traffic which !--- matches the
```

```
access list from undergoing network address translation
(NAT). !--- The traffic specified by this ACL is traffic
that is to be encrypted and !--- sent across the VPN
tunnel. This ACL is intentionally !--- the same as
(outside_1_cryptomap). !--- Two separate access lists
should always be used in this configuration. access-list
outside_1_cryptomap extended permit ip 10.10.10.0
255.255.255.0 10.20.10.0 255.255.255.0 !--- This access
list (outside_cryptomap) is used !--- with the crypto
map outside_map !--- to determine which traffic should
be encrypted and sent !--- across the tunnel. !--- This
ACL is intentionally the same as (inside_nat0_outbound).
!--- Two separate access lists should always be used in
this configuration. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image disk0:/asdm-613.bin
asdm history enable arp timeout 14400 global (outside) 1
interface nat (inside) 1 10.10.10.0 255.255.255.0 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in !--- the ACL
inside_nat0_outbound. access-group 100 in interface
outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 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 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0
dmz no snmp-server location no snmp-server contact !---
PHASE 2 CONFIGURATION ---! !--- The encryption types for
Phase 2 are defined here. crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 1
match address outside_1_cryptomap !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec
peer crypto map outside_map 1 set transform-set ESP-DES-
SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside !--- Specifies
the interface to be used with !--- the settings defined
in this configuration. !--- PHASE 1 CONFIGURATION ---!
!--- This configuration uses isakmp policy 10. !--- The
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 1 lifetime 86400 telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! tunnel-group 172.17.1.1 type ipsec-l2l !--
- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l–IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer. tunnel-group 172.17.1.1 ipsec-
attributes pre-shared-key * !--- Enter the pre-shared-
key in order to configure the !--- authentication
method. 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 ! ! !-- Output
suppressed! username cisco123 password ffIRPGpDSOJh9YLq
encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

Настройка маршрутизатора с помощью интерфейса командной строки

Маршрутизатор

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- 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 2 authentication pre-share !---
Specifies the pre-shared key "cisco123" which should !--
- be identical at both peers. This is a global !---
configuration mode command. crypto isakmp key cisco123
address 172.16.1.1 ! ! !--- 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 ASA-IPSEC esp-
des esp-sha-hmac ! !--- !--- Indicates that IKE is used
to establish !--- the IPsec Security Association for
protecting the !--- traffic specified by this crypto map
entry. crypto map SDM_CMAP_1 1 ipsec-isakmp description
Tunnel to172.16.1.1 !--- !--- Sets the IP address of the
remote end. set peer 172.16.1.1 !--- !--- Configures
IPsec to use the transform-set !--- "ASA-IPSEC" defined
earlier in this configuration. set transform-set ASA-
IPSEC !--- !--- Specifies the interesting traffic to be
encrypted. match address 100 ! ! ! !--- Configures the
interface to use the !--- crypto map "SDM_CMAP_1" for
IPsec. interface FastEthernet0 ip address 172.17.1.1
255.255.255.0 duplex auto speed auto crypto map
SDM_CMAP_1 ! interface FastEthernet1 ip address
10.20.10.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet2 no ip address ! interface Vlan1
```

```
ip address 10.77.241.109 255.255.255.192 ! ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2 ip route
10.77.233.0 255.255.255.0 10.77.241.65 ip route
172.16.1.0 255.255.255.0 172.17.1.2 ! ! ip nat inside
source route-map nonat interface FastEthernet0 overload
! ip http server ip http authentication local ip http
secure-server ! !--- Configure the access-lists and map
them to the Crypto map configured. access-list 100
remark SDM_ACL Category=4 access-list 100 remark IPSec
Rule access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255 ! ! ! !--- This ACL 110 identifies
the traffic flows using route map access-list 110 deny
ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255 access-list
110 permit ip 10.20.10.0 0.0.0.255 any route-map nonat
permit 10 match ip address 110 ! control-plane ! ! line
con 0 login local line aux 0 line vty 0 4 privilege
level 15 login local transport input telnet ssh ! end
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

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

- Команды show устройства защиты PIX
- Команды show удаленного маршрутизатора IOS

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: 172.17.1.1 Type : L2L Role : initiator
Rekey : no State : MM_ACTIVE
```
- **show crypto ipsec sa — отображает все текущие ассоциации безопасности (SA) IPsec узла.**
```
ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1,
local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) current_peer: 172.17.1.1
#pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts
verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #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.: 172.16.1.1, remote crypto endpt.: 172.17.1.1
path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp
sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings
={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing:
remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y
outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use
settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa
timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection
support: Y
```

Команды show удаленного маршрутизатора IOS

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE**

узла.`Router#show crypto isakmp sa dst src state conn-id slot status 172.17.1.1 172.16.1.1 QM_IDLE 3 0 ACTIVE`

- **show crypto ipsec sa — отображает все текущие ассоциации безопасности (SA) IPsec**

  узла.`Router#show crypto ipsec sa interface: FastEthernet0 Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1 protected vrf: (none) local ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) current_peer 172.16.1.1 port 500 PERMIT, flags={origin_is_acl,} #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68 #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1 path mtu 1500, ip mtu 1500 current outbound spi: 0xB7C1948E(3082917006) inbound esp sas: spi: 0x434C4A7F(1129073279) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3004) IV size: 8 bytes replay detection support: Y Status: ACTIVE inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0xB7C1948E(3082917006) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1 sa timing: remaining key lifetime (k/sec): (4578719/3002) IV size: 8 bytes replay detection support: Y Status: ACTIVE outbound ah sas: outbound pcp sas:`

- **show crypto engine connections active — показывает текущие соединения и информацию относительно зашифрованных и расшифрованных пакетов (только на маршрутизаторе).**`Router#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 3 FastEthernet0 172.17.1.1 set HMAC_SHA+DES_56_CB 0 0 2001 FastEthernet0 172.17.1.1 set DES+SHA 0 59 2002 FastEthernet0 172.17.1.1 set DES+SHA 59 0`

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.**

Примечание: См. раздел Важные сведения о командах отладки и Устранение проблем системы безопасности IP - Понимание и Использование команд отладки перед использованием **команд отладки**.

- **debug crypto ipsec 7 – отображает связь IPsec этапа 2.debug crypto isakmp 7 — отображает процесс установления связи по протоколу ISAKMP на этапе 1.**
- **debug crypto ipsec – отображает согласования IPSec на Этапе 2.debug crypto isakmp – отображает согласования ISAKMP на 1-м этапе.**

Для получения дополнительной информации об устранении неполадок VPN-соединений "ЛВС-ЛВС" обратитесь к документу Устранение наиболее распространенных неполадок удаленных VPN-соединений и VPN-туннелей "ЛВС-ЛВС" на базе протокола IPSec.

Дополнительные сведения

- Cisco PIX Firewall Software
- Диспетчер адаптивных устройств защиты Cisco (Cisco Adaptive Security Device Manager)
- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Configuration Professional: VPN Защищенного взаимодействия между сетями Site-to-Site

IPsec Между ASA/PIX и Примером конфигурации Маршрутизатора IOS
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Диспетчер маршрутизаторов и устройств защиты Cisco (Cisco Router and Security Device Manager – SDM)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация