Configuration Professional: VPN защищенного взаимодействия между сетями Site-to-Site IPsec между двумя примерами конфигурации маршрутизаторов IOS

Содержание

Введение

Этот документ предоставляет пример конфигурации для LAN-LAN (От узла к узлу) Туннель IPSec между двумя Cisco IOS® Routers с помощью Cisco Configuration Professional (CP Cisco). Для упрощения используются статические маршруты.

Предварительные условия

Требования

Удостоверьтесь, что вы удовлетворяете это требование перед попыткой этой конфигурации:

- Перед выполнением шагов по настройке согласно данному документу необходимо установить IP-подключение между конечными узлами.

Используемые компоненты

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

- Маршрутизатор Cisco 1841 с Cisco IOS Software Release 12.4 (15T)
- Версия 2.5 CP Cisco

Примечание: См. Базовую настройку маршрутизатора Использование Cisco Configuration Professional, чтобы позволить маршрутизатору быть настроенным CP Cisco.

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

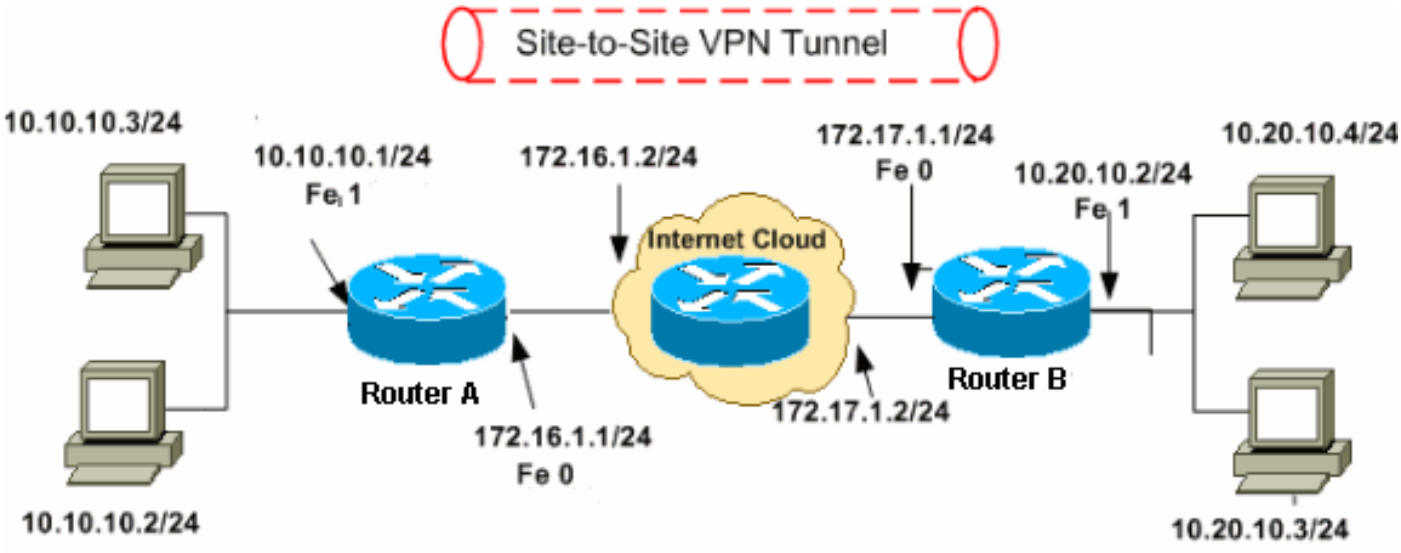
Условные обозначения

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

!--- конфигурацию

Схема сети

В настоящем документе используется следующая схема сети:



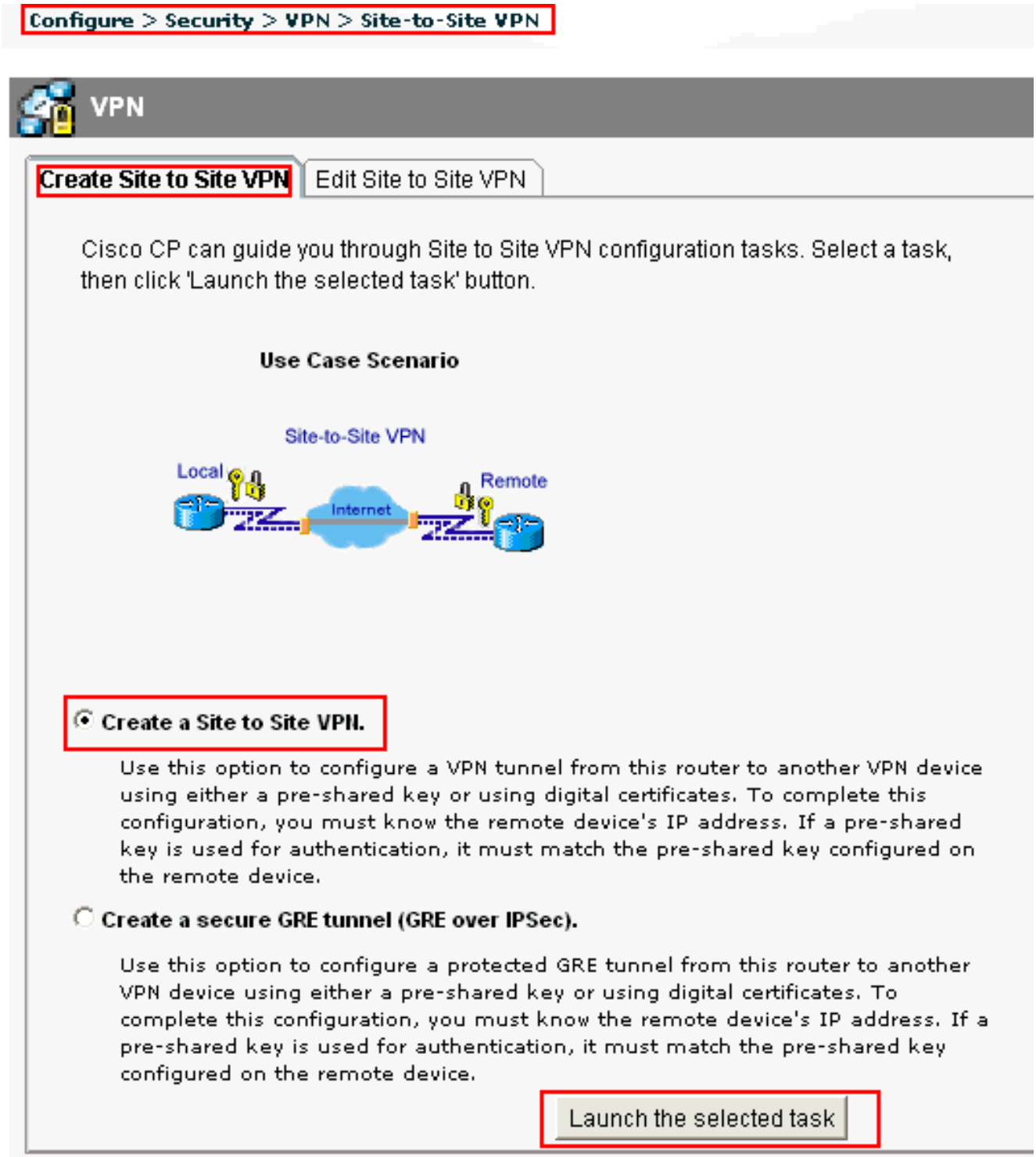
Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

- Маршрутизатор конфигурация Cisco CP
- Конфигурация Cisco CP маршрутизатора B
- Конфигурация интерфейса командой строки маршрутизатора B

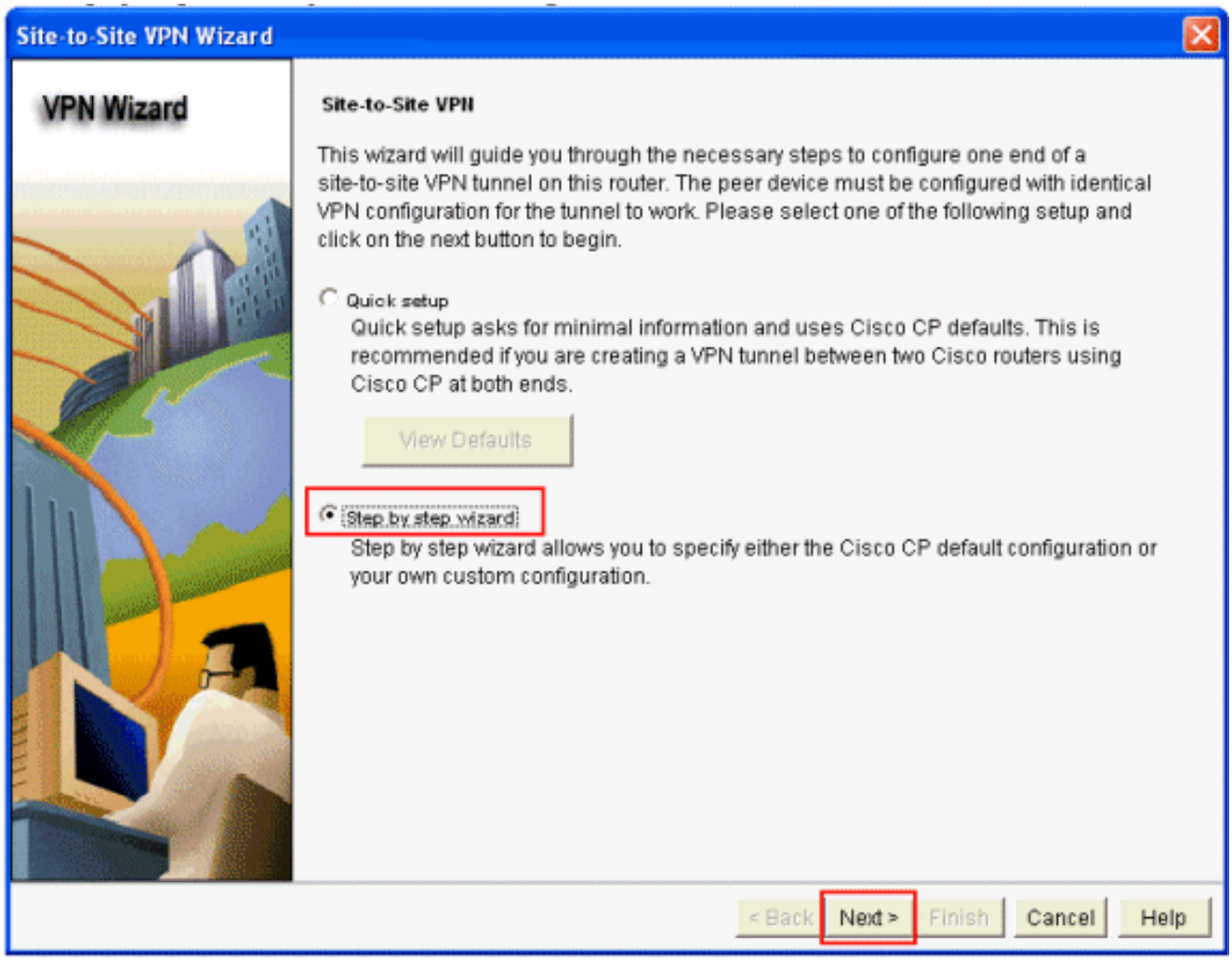
Маршрутизатор конфигурация Cisco CP

Выполните эти шаги для настройки Туннеля VPN типа «узел-узел» на маршрутизаторе Cisco IOS:

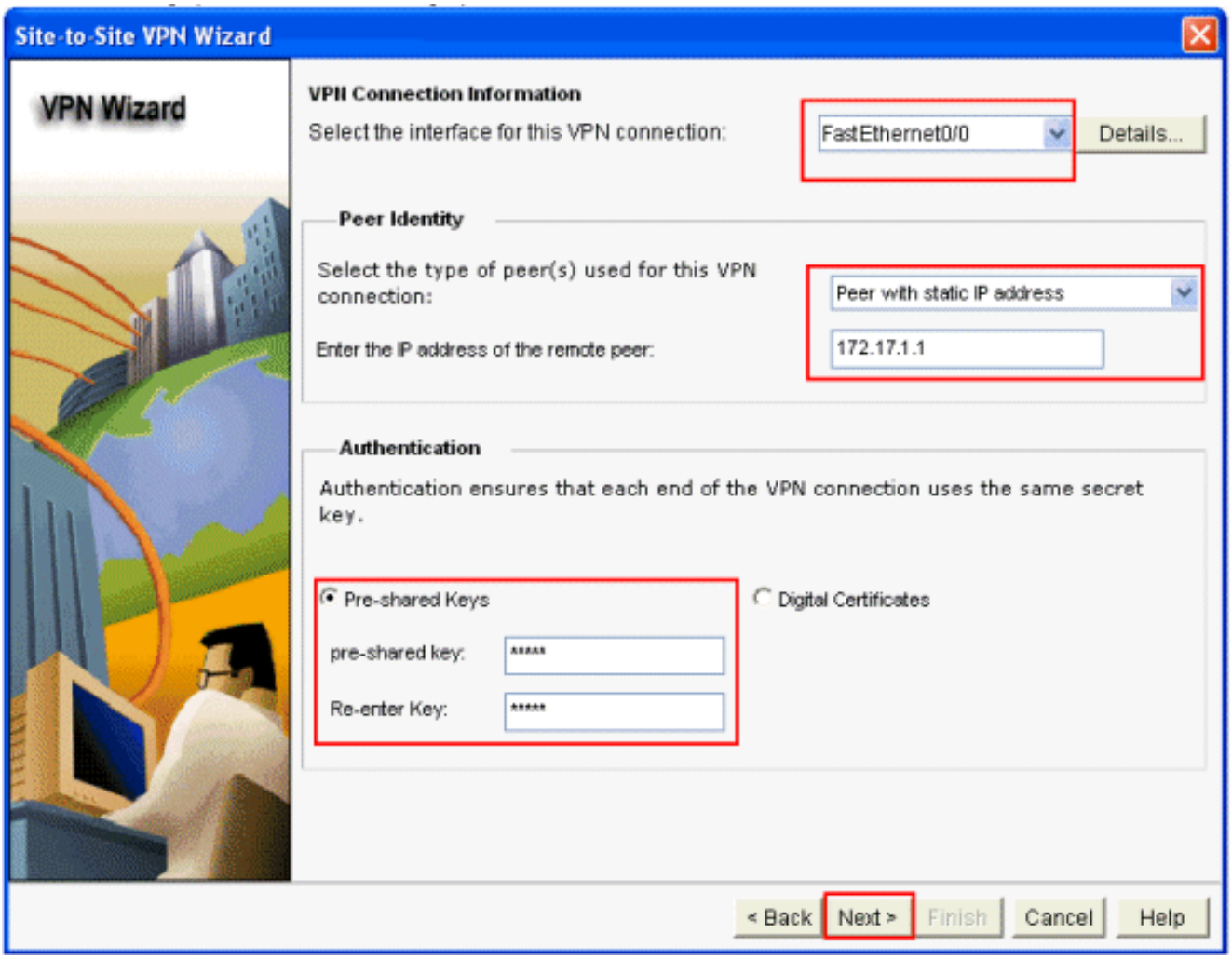
1. Выберите**> Security Configure> VPN> Сквозной VPN-соединение**, и нажмите, кнопка с зависимой фиксацией рядом с **Создают Сквозное VPN-соединение**. **Выберите Launch the selected**
task.



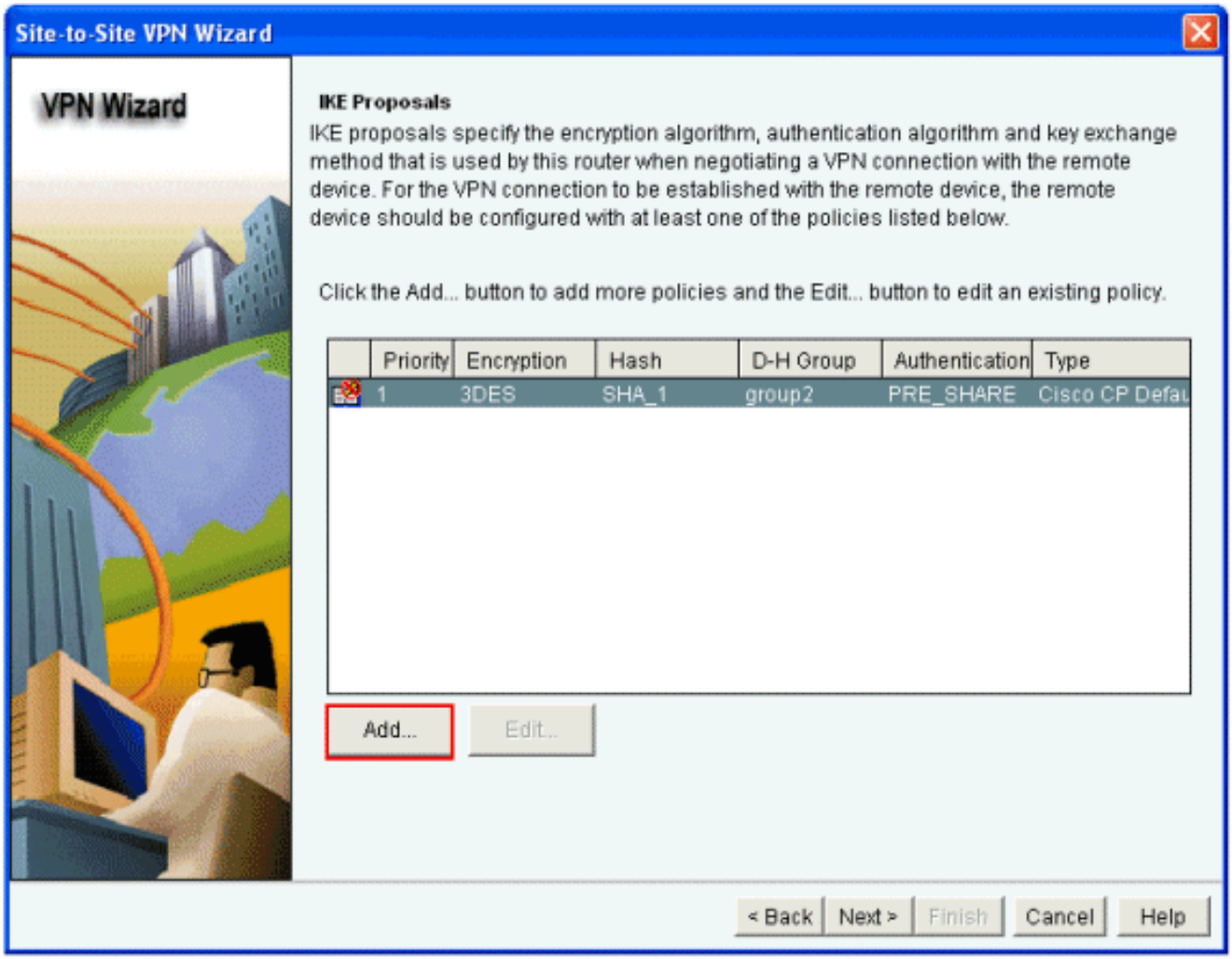
2. Выберите **мастера Step by step**, чтобы продолжить конфигурацию и нажать **Next**.



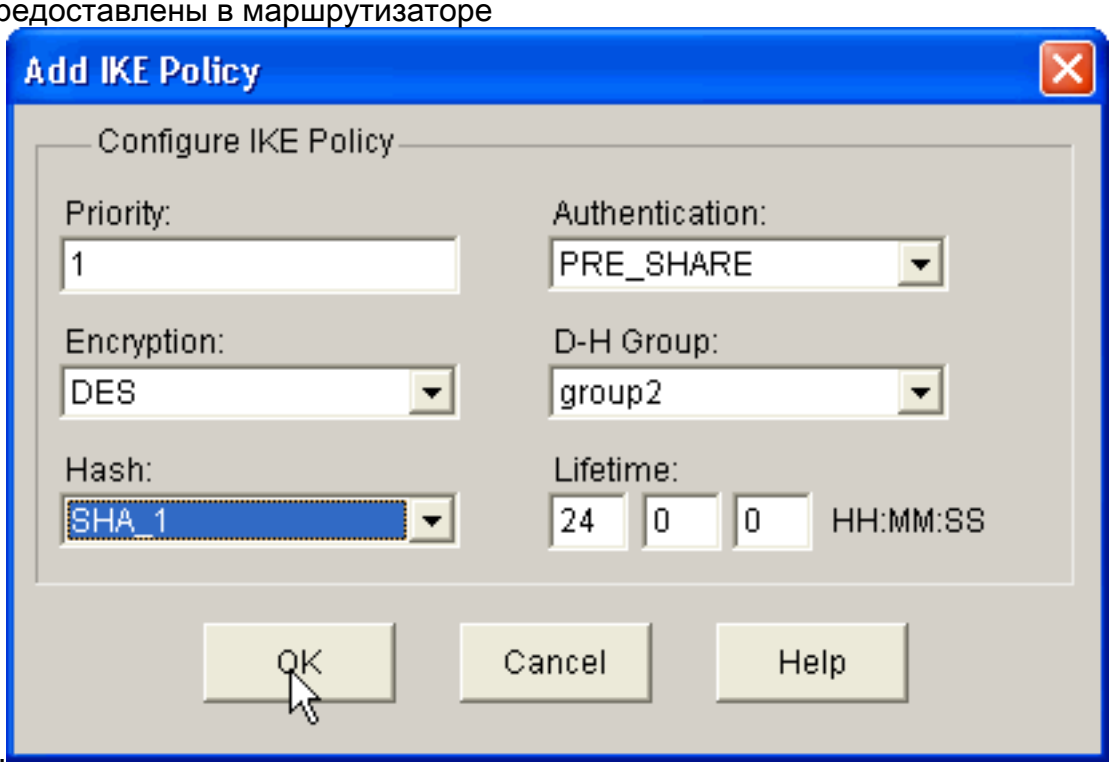
3. В окне VPN Connection Information в соответствующих полях указывается информация о VPN-соединении. Выберите интерфейс VPN-туннеля от раскрывающегося меню. **В этом примере выбран FastEthernet0. В разделе Peer Identity выберите Peer with static IP address из списка и укажите IP-адрес удаленного узла.** Затем предоставьте Предварительные общие ключи (*cisco123* в данном примере) в Опознавательном разделе. Наконец, нажмите
Next.



4. **Нажмите Add** для добавления Предложений ike, которые задают Алгоритм шифрования, Алгоритм аутентификации и Метод обмена ключами.

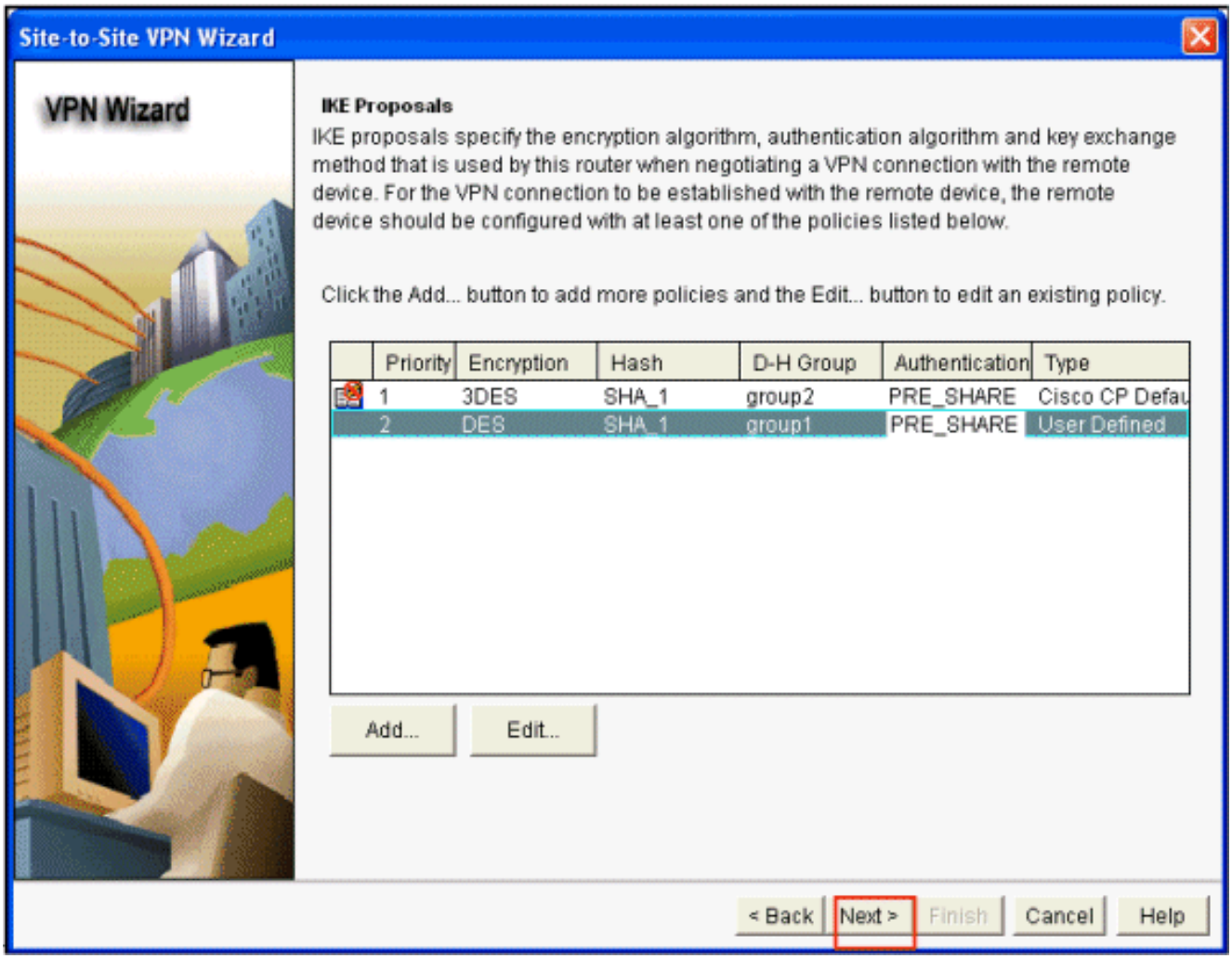


5. Предоставьте Алгоритм шифрования, Алгоритм аутентификации и Метод обмена ключами, и затем нажмите **OK**. Алгоритм шифрования, Алгоритм аутентификации и значения Метода обмена ключами должны совпасть с данными, которые будут предоставлены в маршрутизаторе

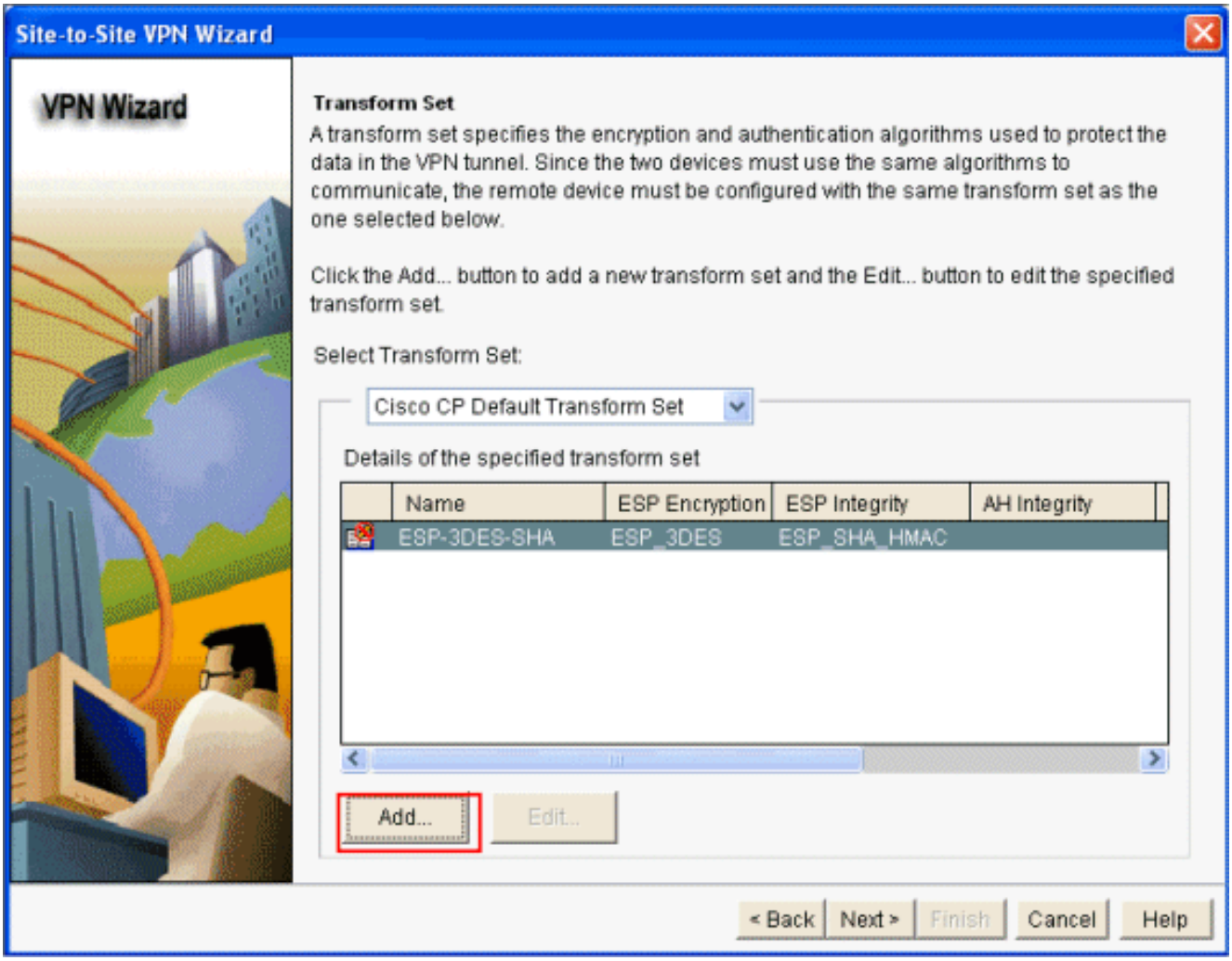


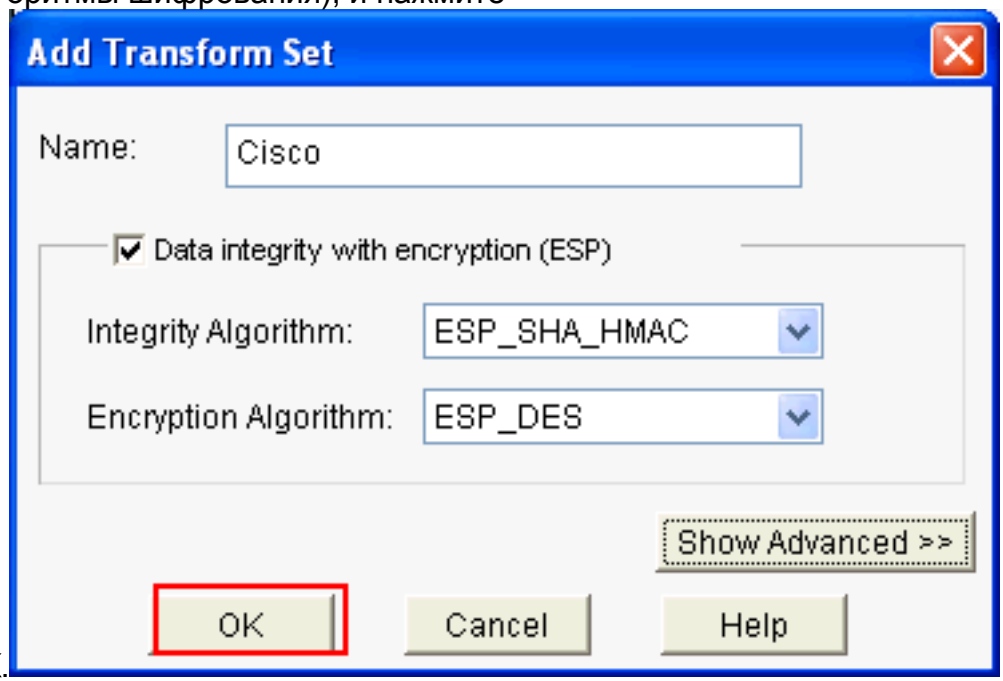
B.

6. **Нажмите кнопку Next.**

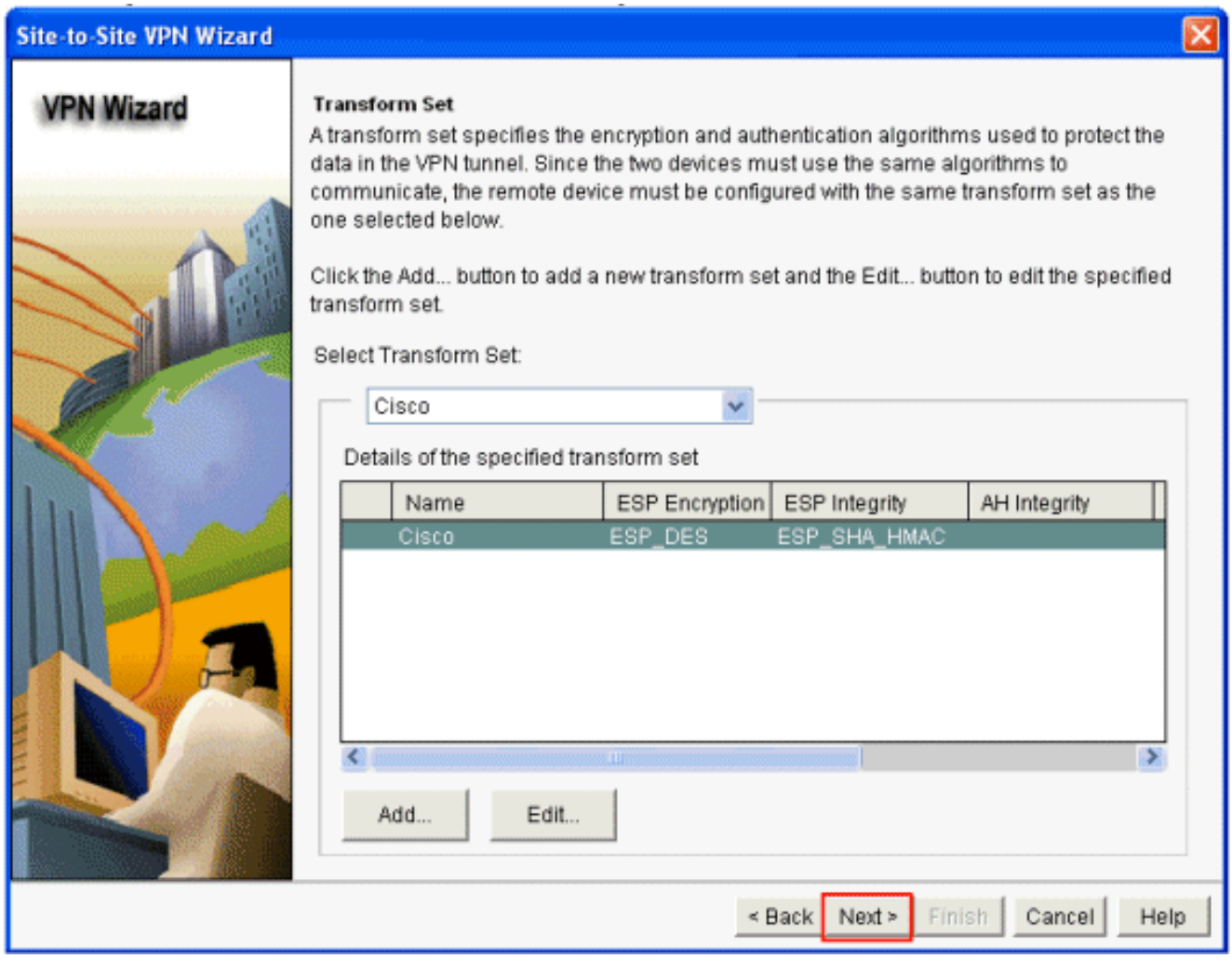


7. В этом новом окне предоставлена подробная информация Набора преобразований. Набор преобразований задаются алгоритмы шифрования и аутентификации, используемые для защиты данных в VPN-туннеле. **Нажмите Add** для предоставления этой подробной информации. Можно добавить любое количество Наборов преобразований по мере необходимости при помощи этого метода.

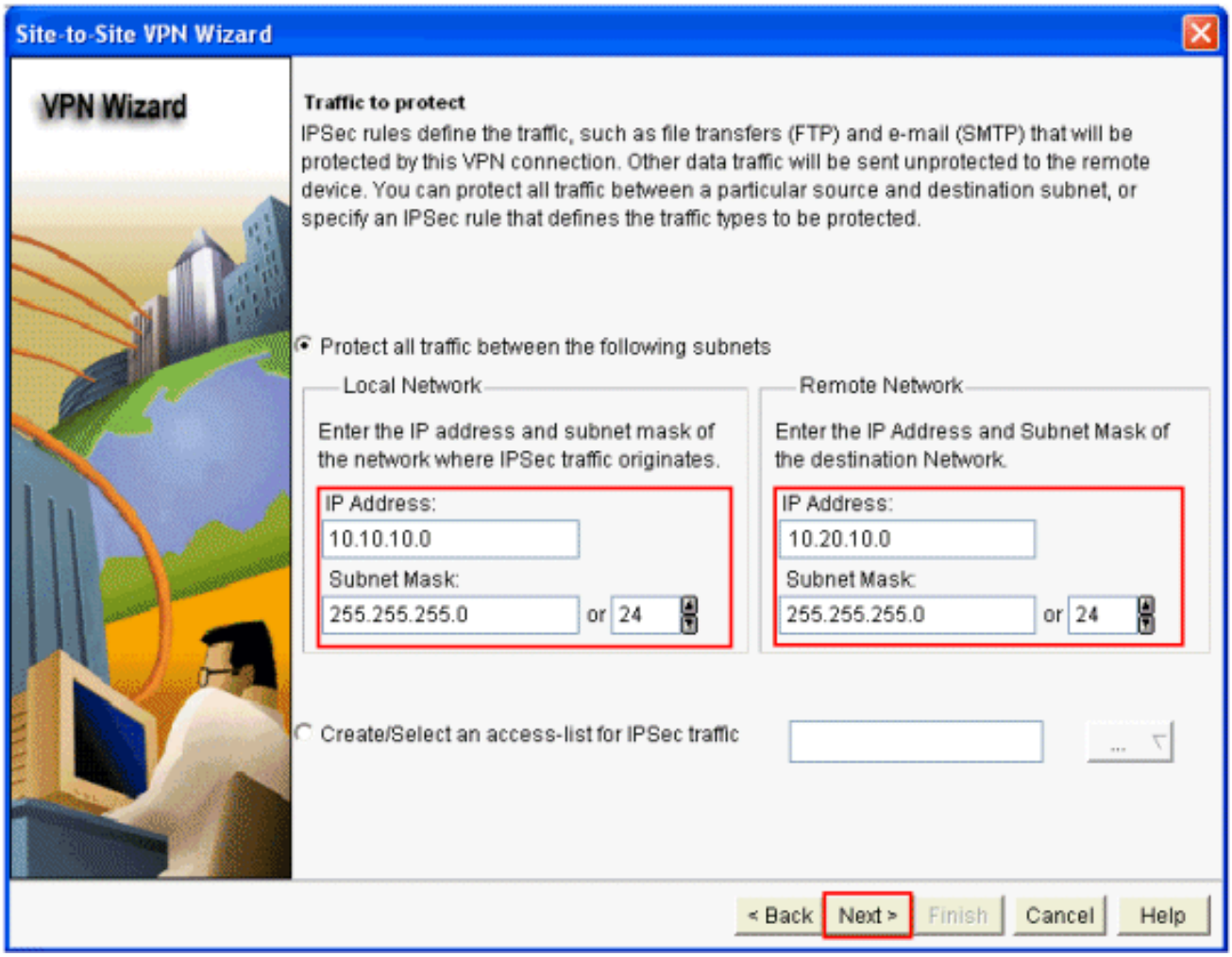


8. Предоставьте подробную информацию Набора преобразований (Целостность и Алгоритмы шифрования), и нажмите


OK.
9. Выберите требуемый **Набор преобразований**, который будет использоваться от раскрывающегося меню и нажмет **Next**.



10. 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 данном примере Исходная сеть *10.10.10.0*, и Сеть назначения *10.20.10.0*. **Нажмите кнопку Next.**

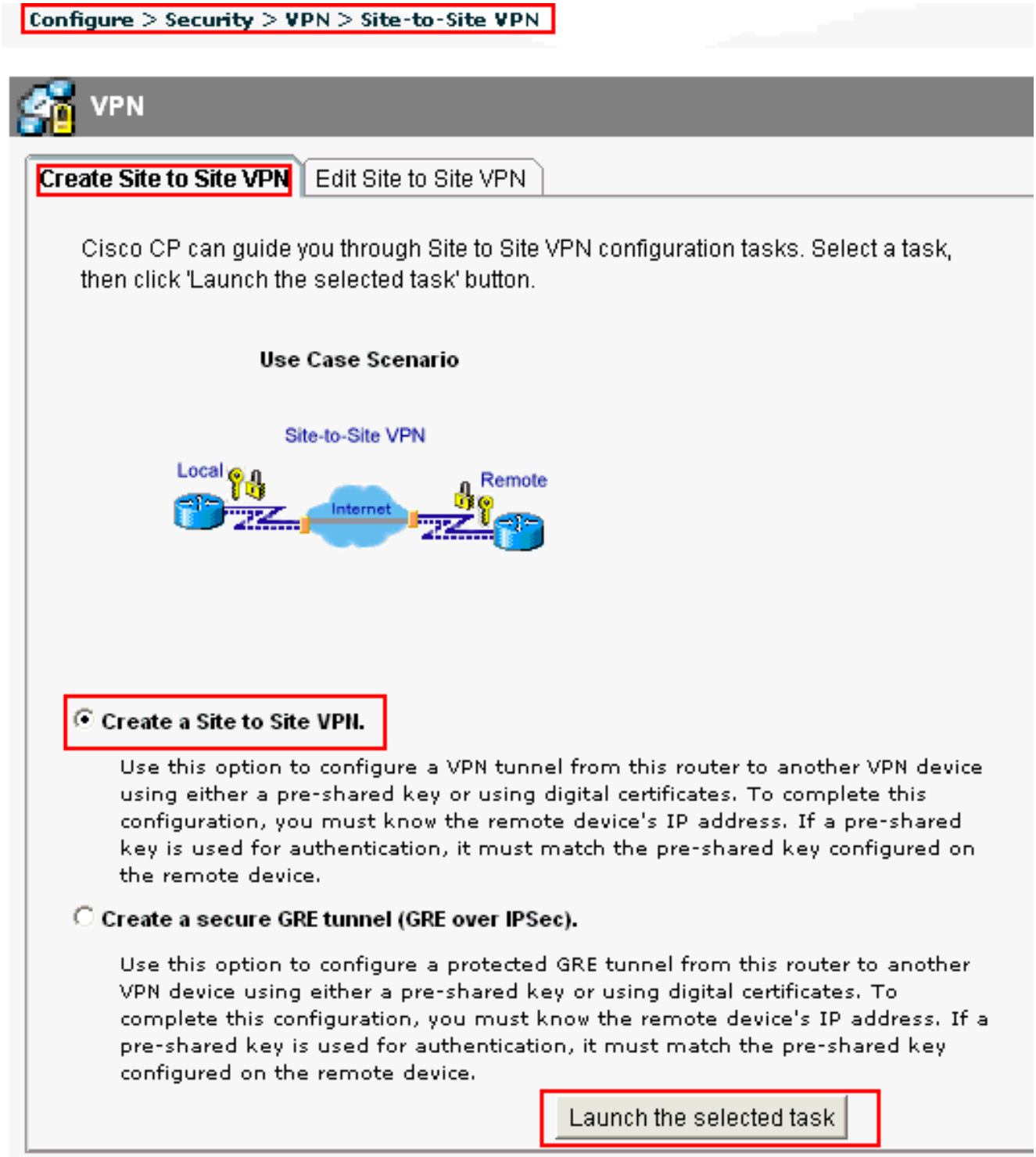


11. Нажмите **Finish** в следующем окне для завершения конфигурации на маршрутизаторе A..

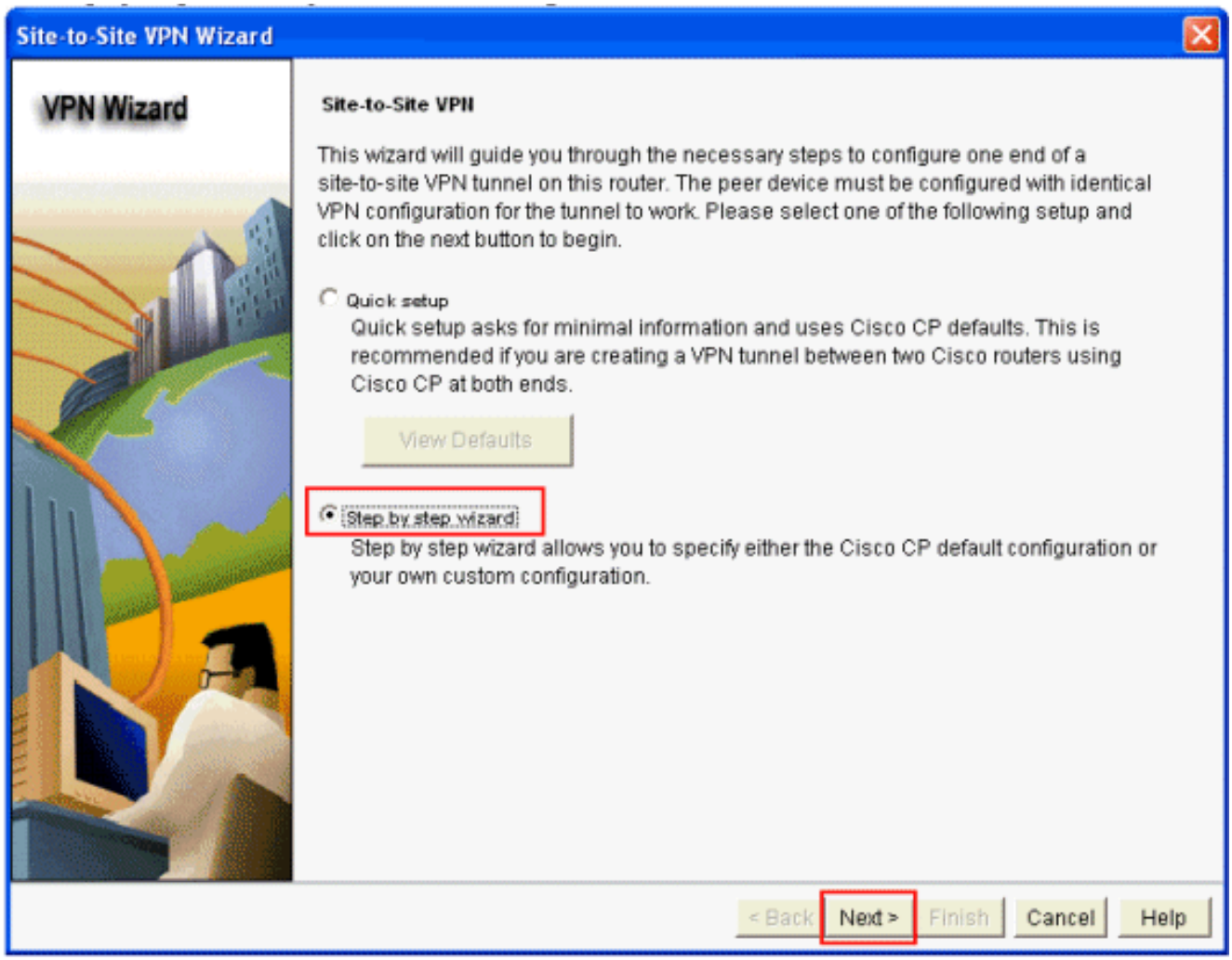
Конфигурация Cisco CP маршрутизатора B

Выполните эти шаги для настройки Туннеля VPN типа «узел-узел» на маршрутизаторе Cisco IOS (маршрутизатор B):

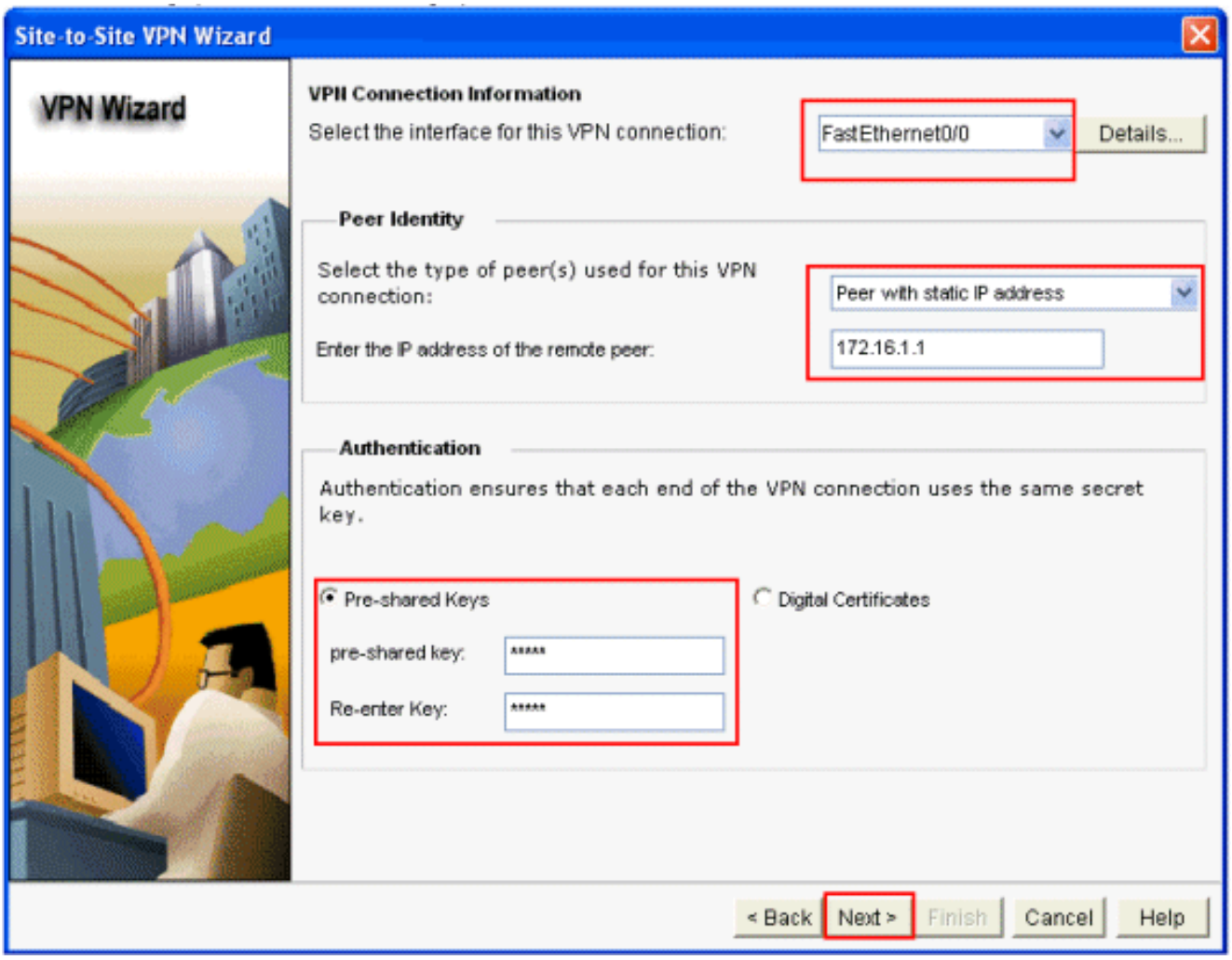
1. Выберите**> Security Configure> VPN> Сквозной VPN-соединение**, и нажмите, кнопка с зависимой фиксацией рядом с **Создают Сквозное VPN-соединение**. **Выберите Launch the selected**
   task.



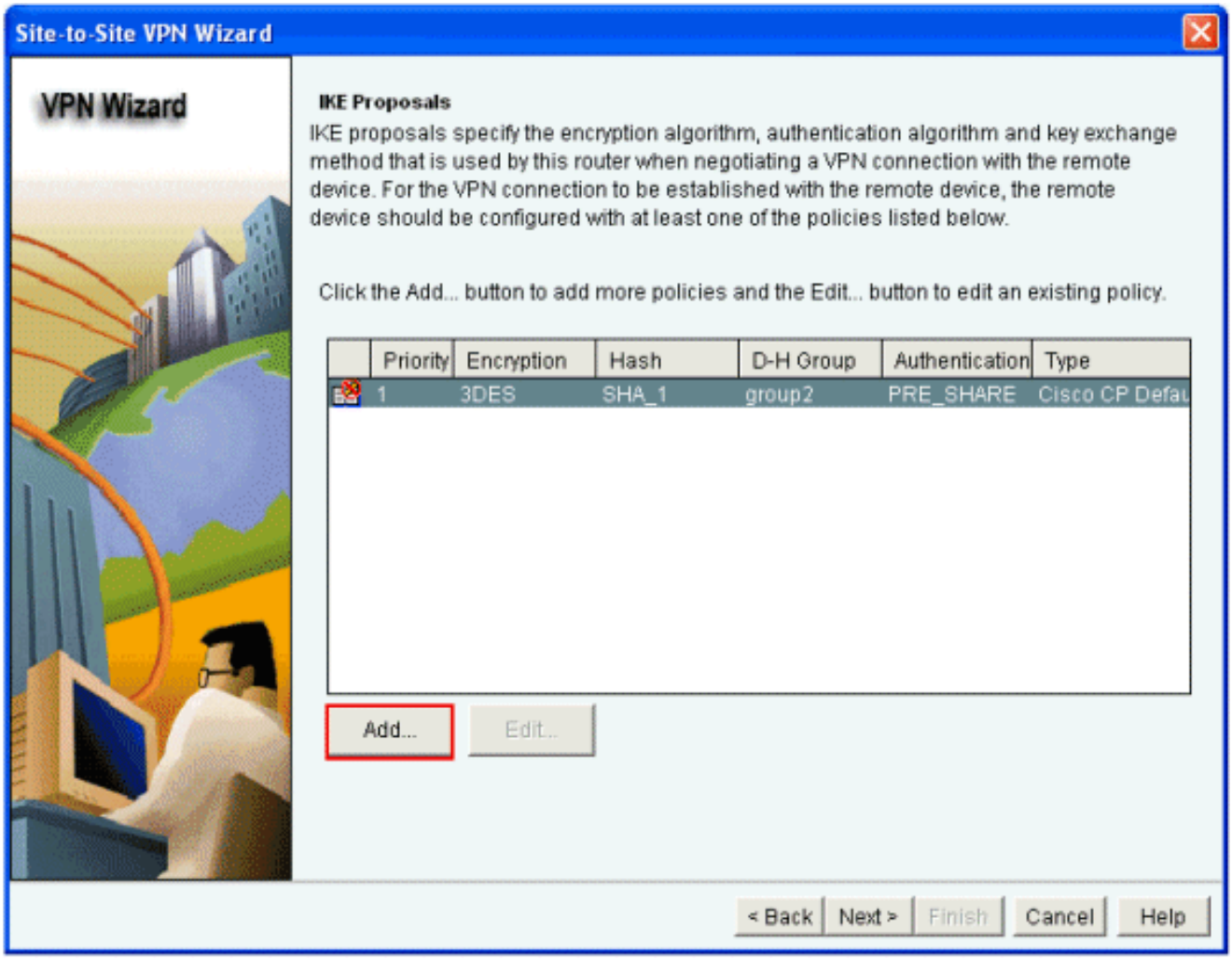
2. Выберите **мастера Step by step**, чтобы продолжить конфигурацию и нажать **Next**.



3. В окне VPN Connection Information в соответствующих полях указывается информация о VPN-соединении. Выберите интерфейс VPN-туннеля от раскрывающегося меню. **В этом примере выбран FastEthernet0. В разделе Peer Identity выберите Peer with static IP address из списка и укажите IP-адрес удаленного узла.** Затем предоставьте Предварительные общие ключи (*cisco123* в данном примере) в Опознавательном разделе. Наконец, нажмите
Next.

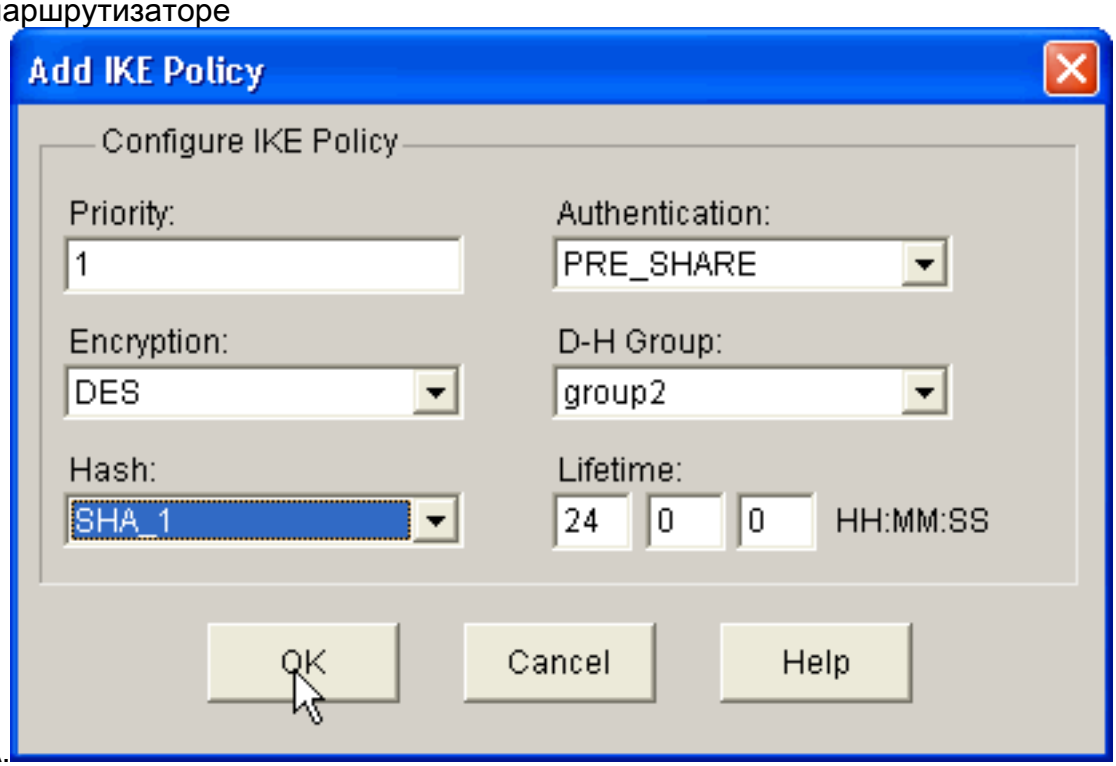


4. **Нажмите Add** для добавления Предложений ike, которые задают Алгоритм шифрования, Алгоритм аутентификации и Метод обмена ключами.

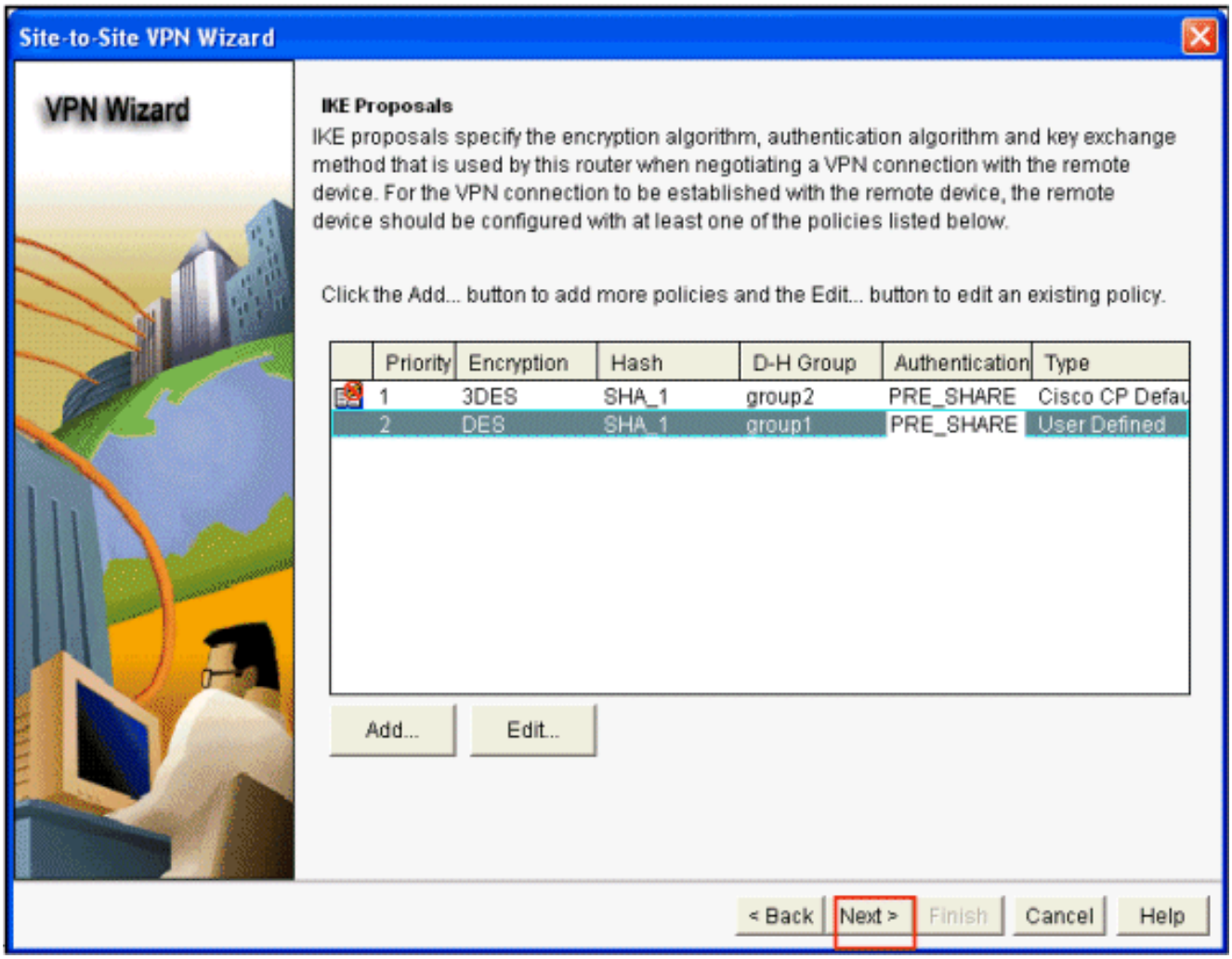


5. Предоставьте Алгоритм шифрования, Алгоритм аутентификации и Метод обмена ключами, и затем нажмите **OK**. Алгоритм шифрования, Алгоритм аутентификации и значения Метода обмена ключами должны совпасть с данными, предоставленными в маршрутизаторе

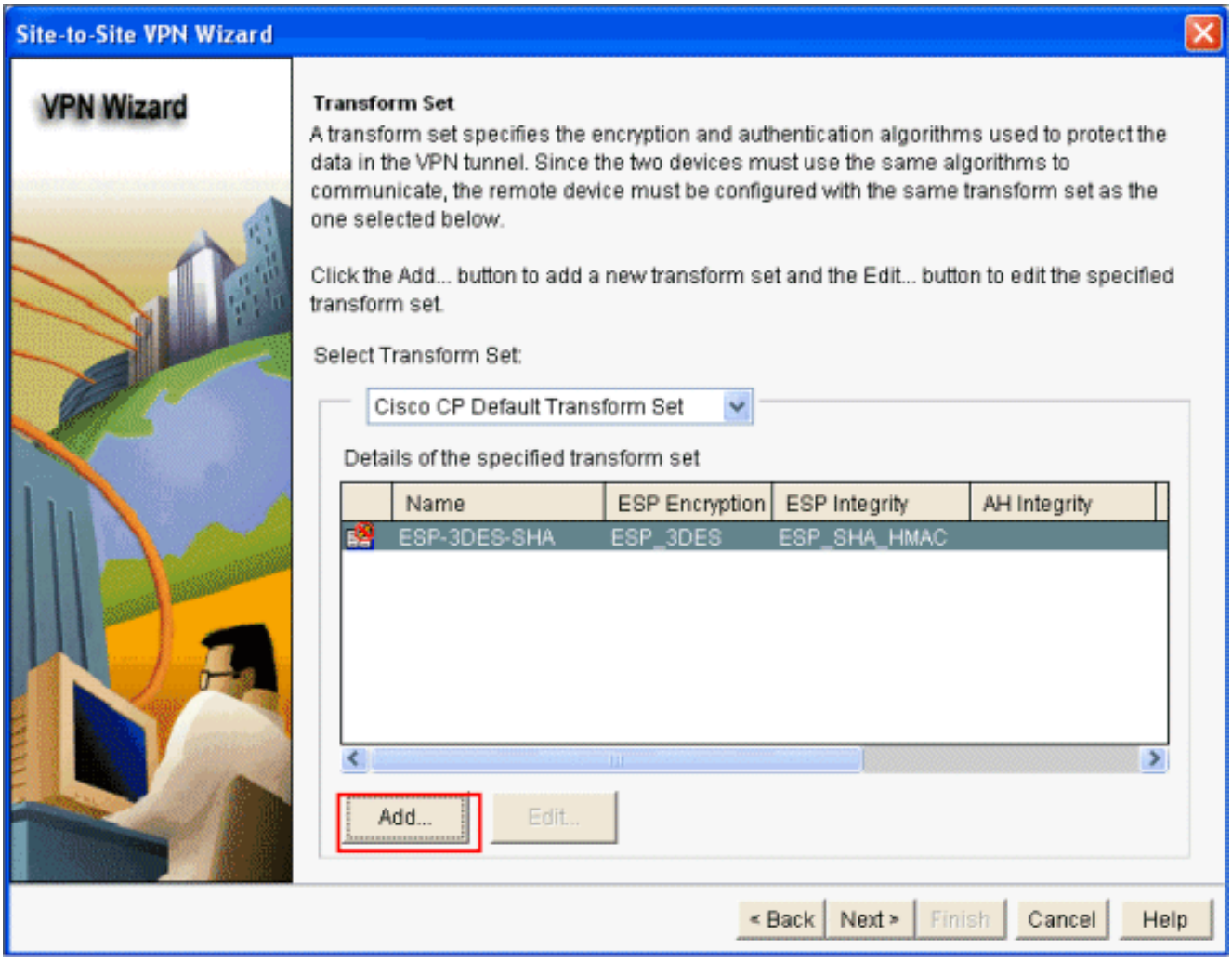
A.

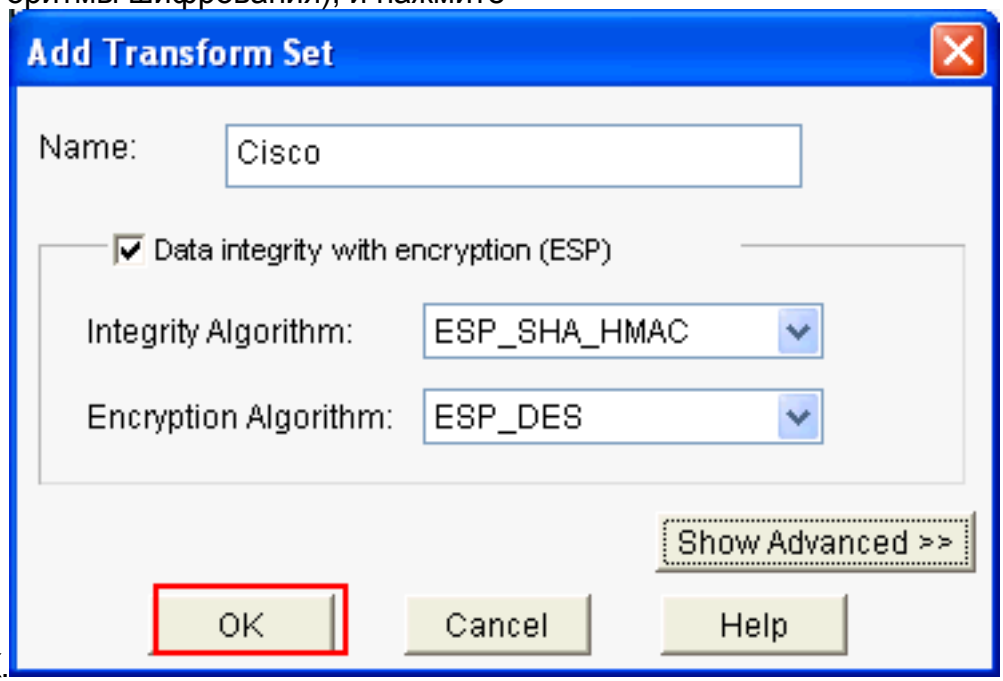


6. **Нажмите кнопку Next.**

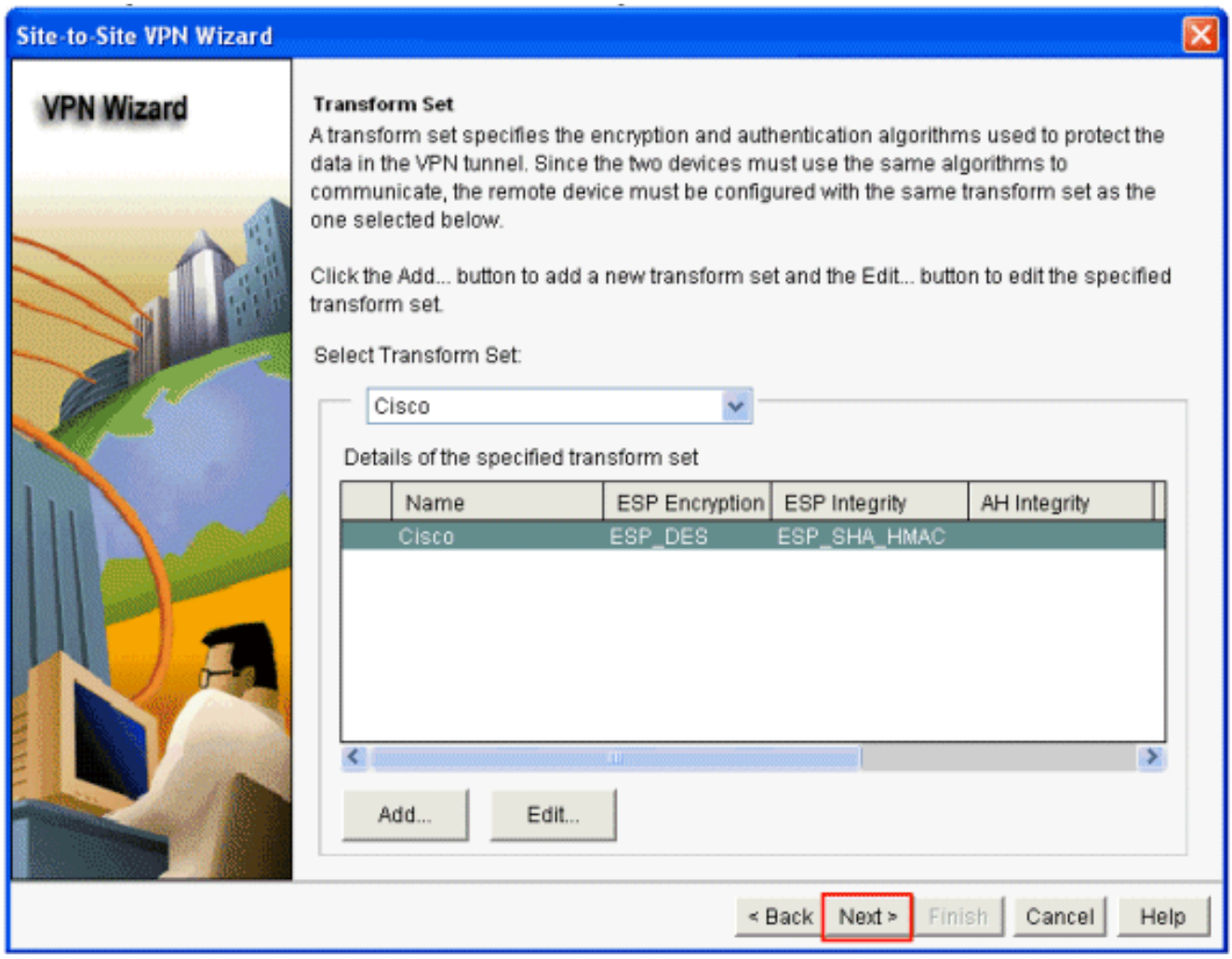


7. В этом новом окне предоставлена подробная информация Набора преобразований. Набор преобразований задаются алгоритмы шифрования и аутентификации, используемые для защиты данных в VPN-туннеле. **Нажмите Add** для предоставления этой подробной информации. Можно добавить любое количество Наборов преобразований по мере необходимости при помощи этого метода.

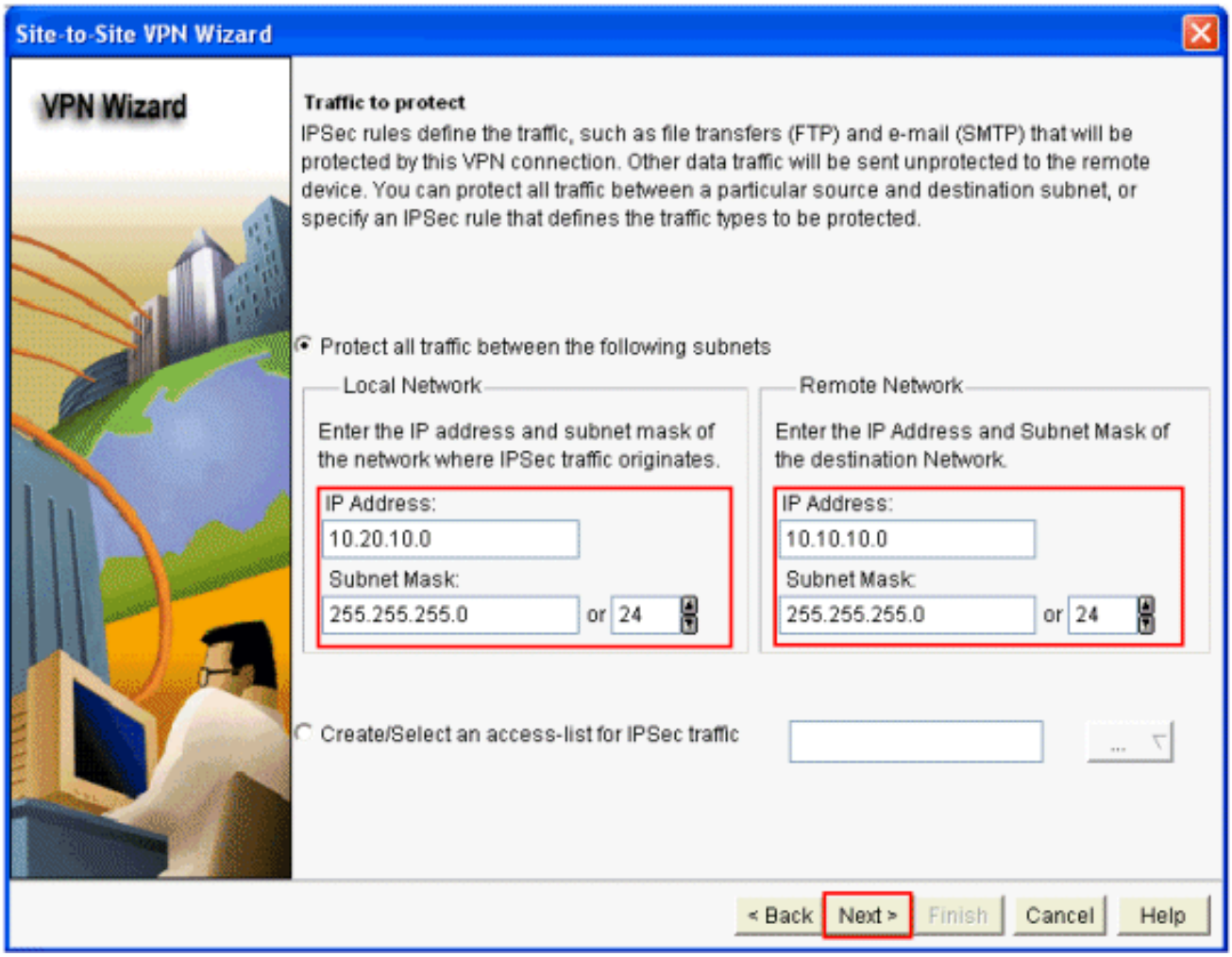


8. Предоставьте подробную информацию Набора преобразований (Целостность и Алгоритмы шифрования), и нажмите


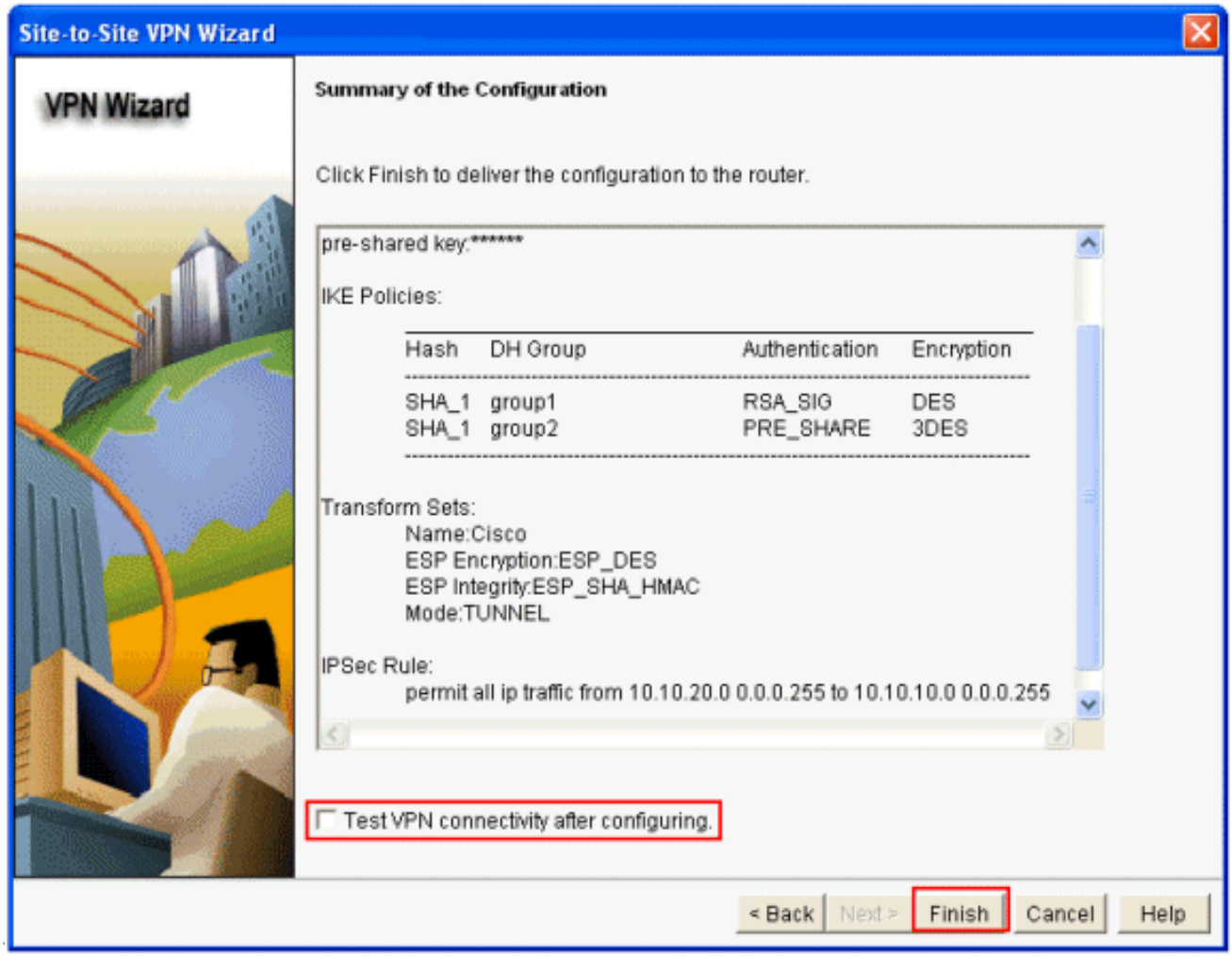
OK.
9. Выберите требуемый **Набор преобразований**, который будет использоваться от раскрывающегося меню и нажмет **Next**.



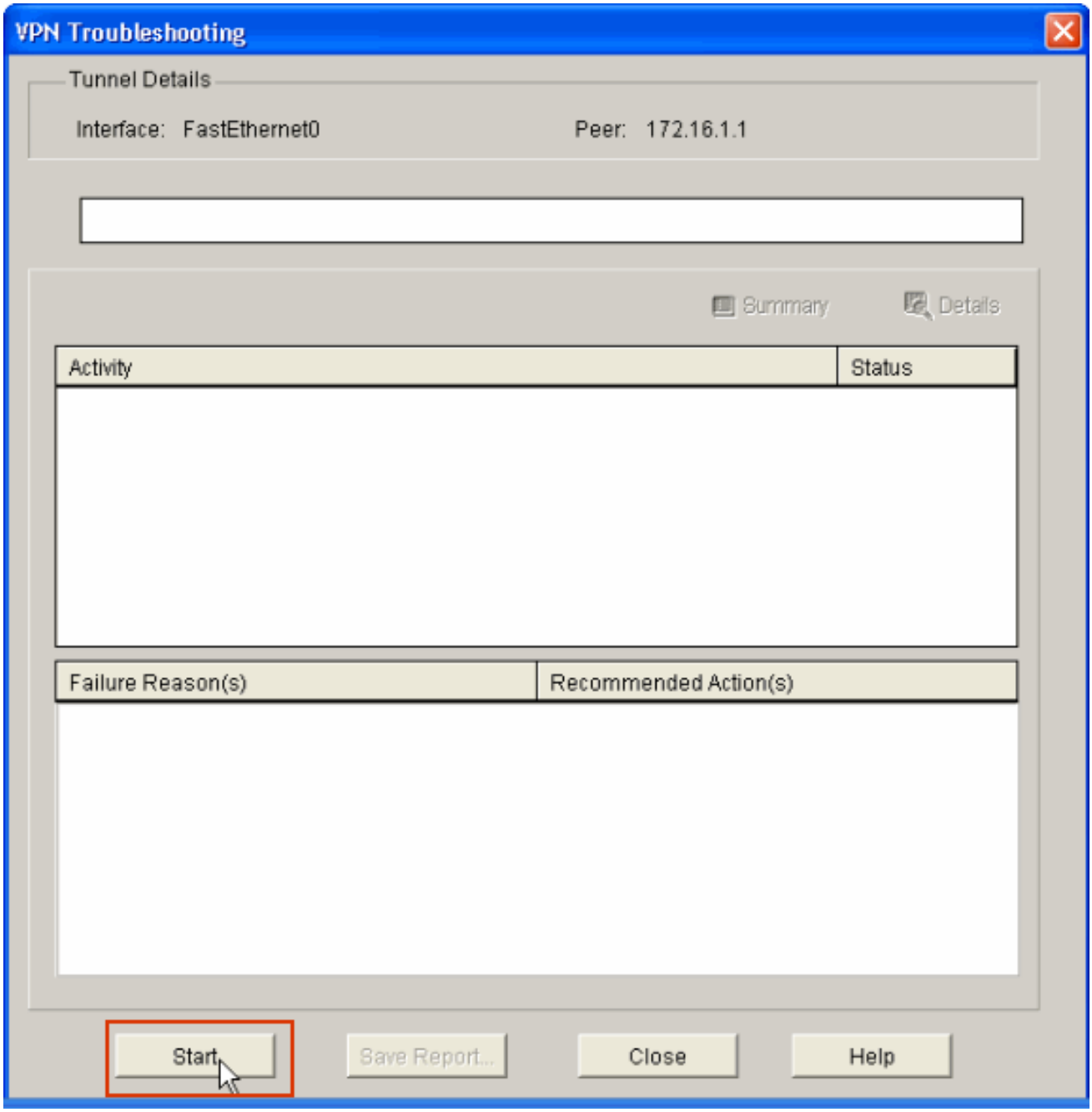
10. В следующем окне необходимо указать трафик, подлежащий защите с помощью VPN-туннеля. Укажите исходную сеть и сеть назначения трафика, подлежащего защите, чтобы трафик между определенной исходной сетью и сетью назначения был защищен. *В этом примере в качестве исходной используется сеть с IP-адресом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



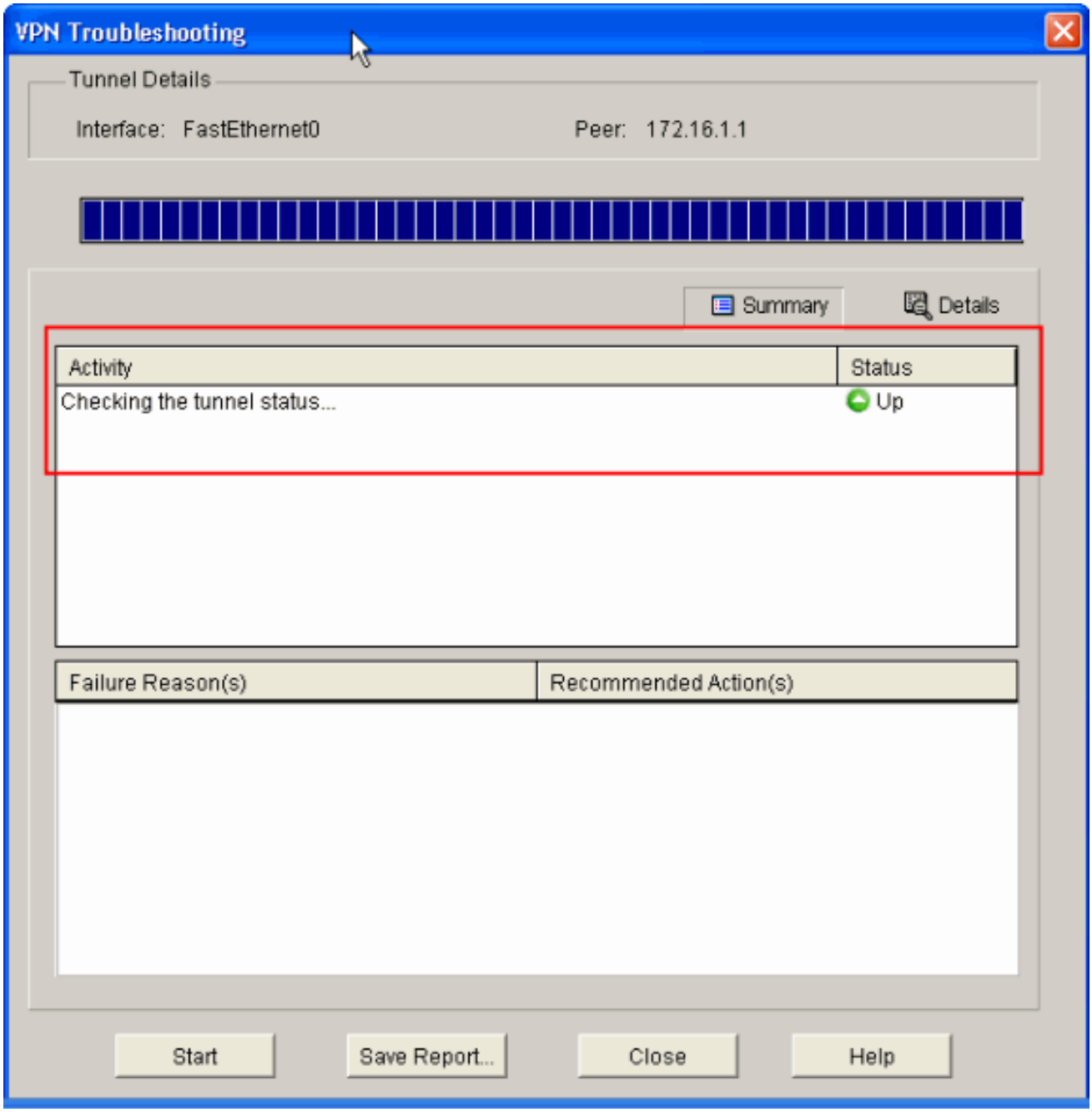
11. Это окно показывает сводку Сквозной VPN-соединение конфигурации. **Установите флажок Test VPN Connectivity after configuring, если необходимо протестировать VPN-подключение**. В рисунке флажок отмечен, т. к. необходимо проверить подключение. **Нажмите кнопку Finish.**



12. Нажмите **Start** для проверки возможности VPN - подключения.



13. 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).



Это завершает конфигурацию на Cisco IOS RouterB и показывает, что туннель подключен.

Конфигурация интерфейса командой строки маршрутизатора B

Маршрутизатор B

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
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 Router-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 !--- "Router-IPSEC" defined
earlier in this configuration. set transform-set Router-
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.**

- Маршрутизатор IOS - команды показа

Маршрутизатор IOS - команды показа

- **show crypto isakmp sa — отображает все текущие ассоциации безопасности (SA) IKE узла.**`RouterB# 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.**`RouterB# 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 connection active** — Показывают текущие соединения и информацию о зашифрованных и расшифрованных пакетах.`RouterB#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.

Дополнительные сведения

- Краткое руководство по началу работы Cisco Configuration Professional
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация