Пример конфигурации IPsec между двумя маршрутизаторами IOS с накладывающимися частными сетями

Содержание

Введение

Этот документ описывает способ настройки маршрутизатора Cisco IOS в IPsec VPN для защищенного взаимодействия между сетями двух объектов с пересекающимися адресами частной сети за шлюзами VPN.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на Cisco IOS 3640 маршрутизаторов, которые работают под управлением ПО версии 12.4.

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.

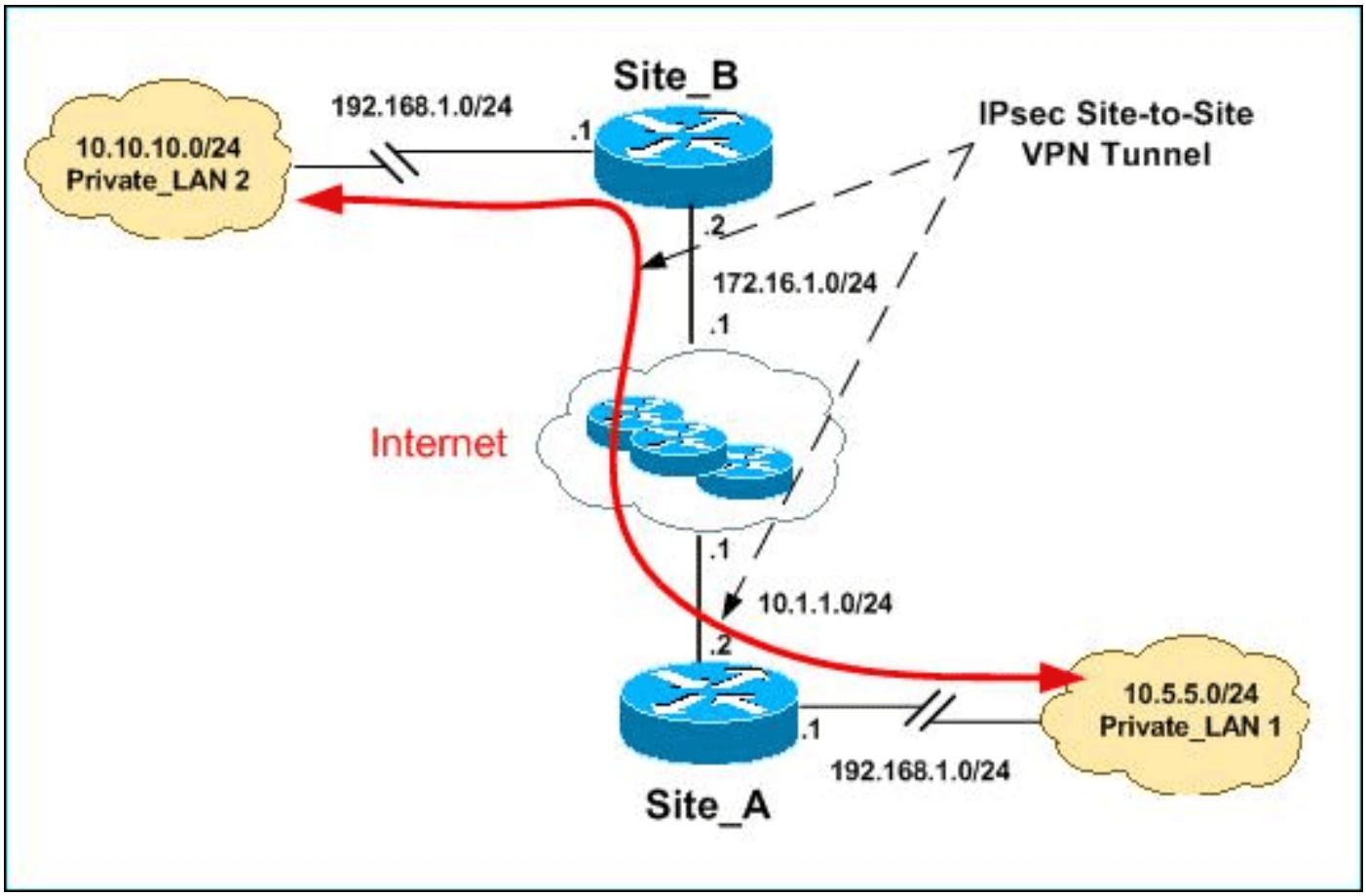
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

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.

И Private_LAN1 и Private_LAN2 имеют IP-подсеть 192.168.1.0/24. Это моделирует адресное пространство с перекрытием позади каждой стороны Туннеля IPSec.

В данном примере маршрутизатор Site_A выполняет двунаправленную трансляцию так, чтобы эти две частных локальных сети (LAN) могли связаться по Туннелю IPSec. Трансляция означает, что Private_LAN1 "рассматривает" Private_LAN2 как 10.10.10.0/24 через Туннель IPSec, и Private_LAN2 "рассматривает" Private_LAN1 как 10.5.5.0/24 через Туннель IPSec.

Конфигурации

Эти конфигурации используются в данном документе:

- SDM-конфигурация маршрутизатора Site_A
- Конфигурация интерфейса командой строки маршрутизатора Site_A
- Конфигурация маршрутизатора Site_B

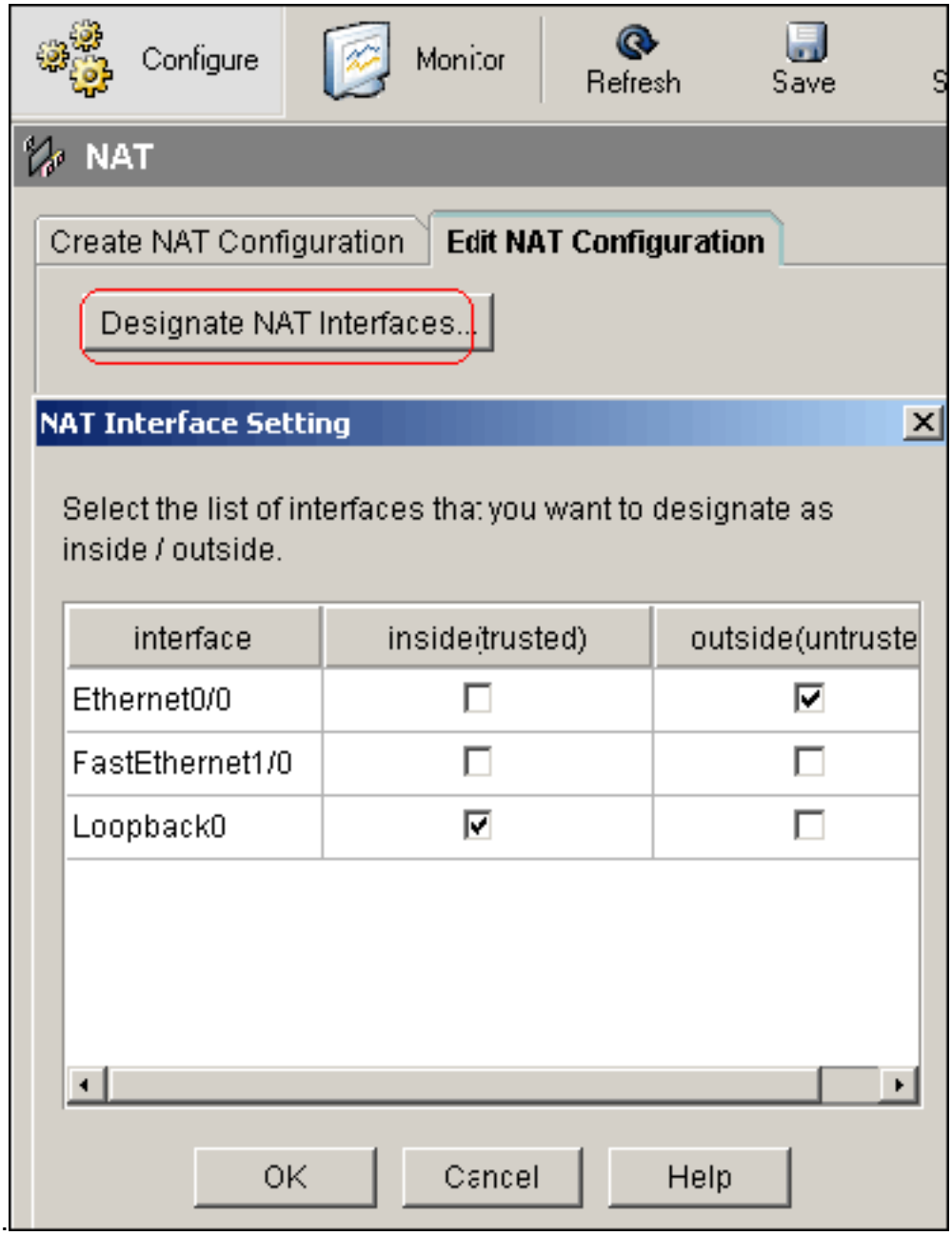
SDM-конфигурация маршрутизатора Site_A

Примечание: Этот документ предполагает, что маршрутизатор настроен с базовыми параметрами как конфигурация интерфейса и т.д. См. Базовую настройку маршрутизатора с помощью SDM для получения дополнительной информации.

Конфигурация статического преобразования сетевых адресов (NAT)

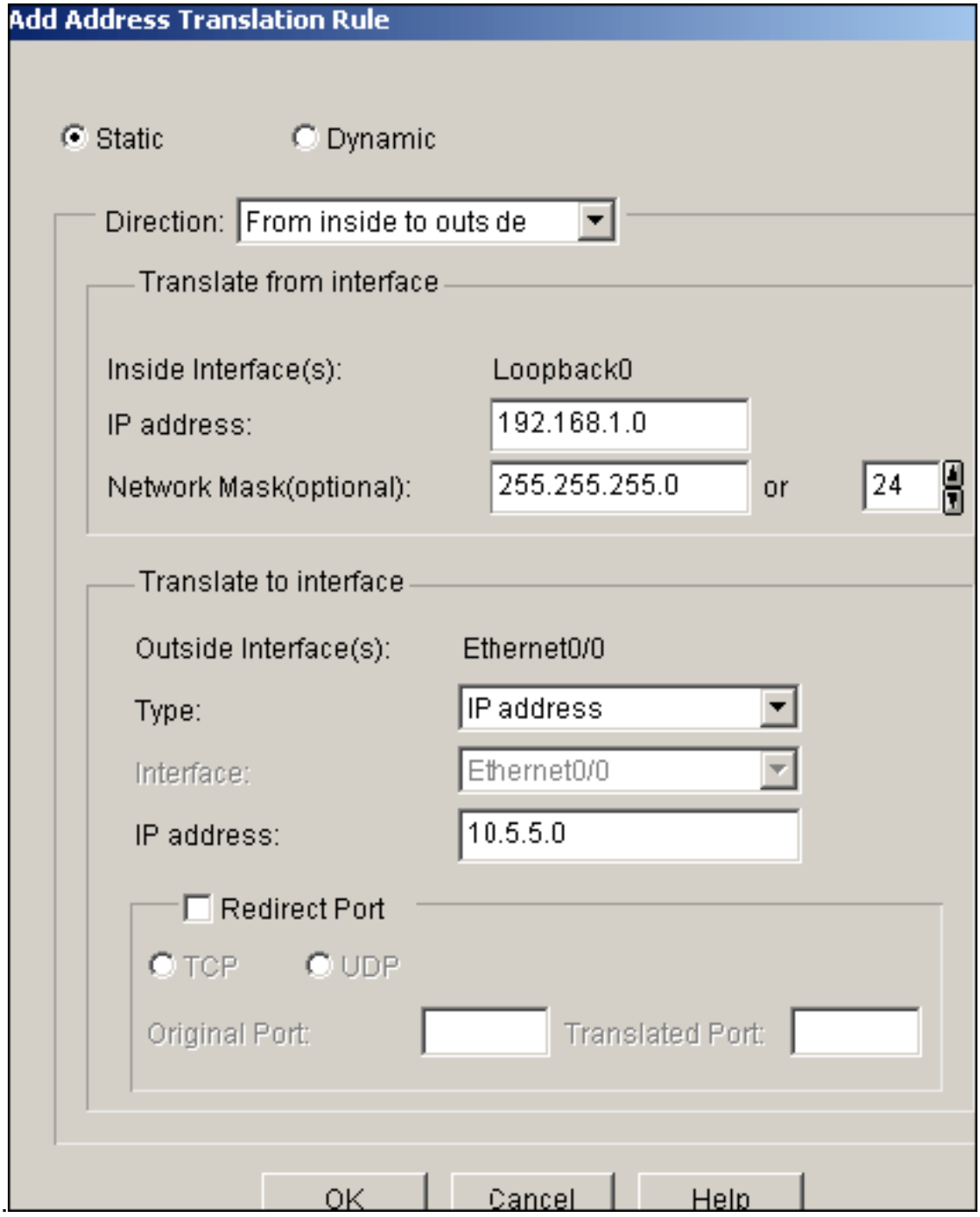
Выполните эти шаги для использования NAT для настройки SDM на маршрутизаторе Site_A:

1. Выберите **Configure> NAT> Edit NAT Configuration** и нажмите **Designate NAT Interfaces** для определения доверяемый и ненадежные интерфейсы как



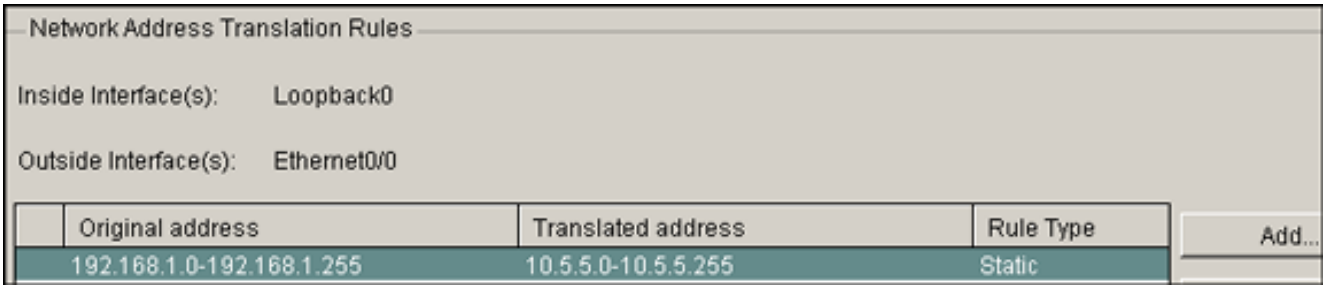
показано.

2. **Нажмите кнопку OK.**
3. **Нажмите Add** для настройки преобразования NAT изнутри к внешнему направлению

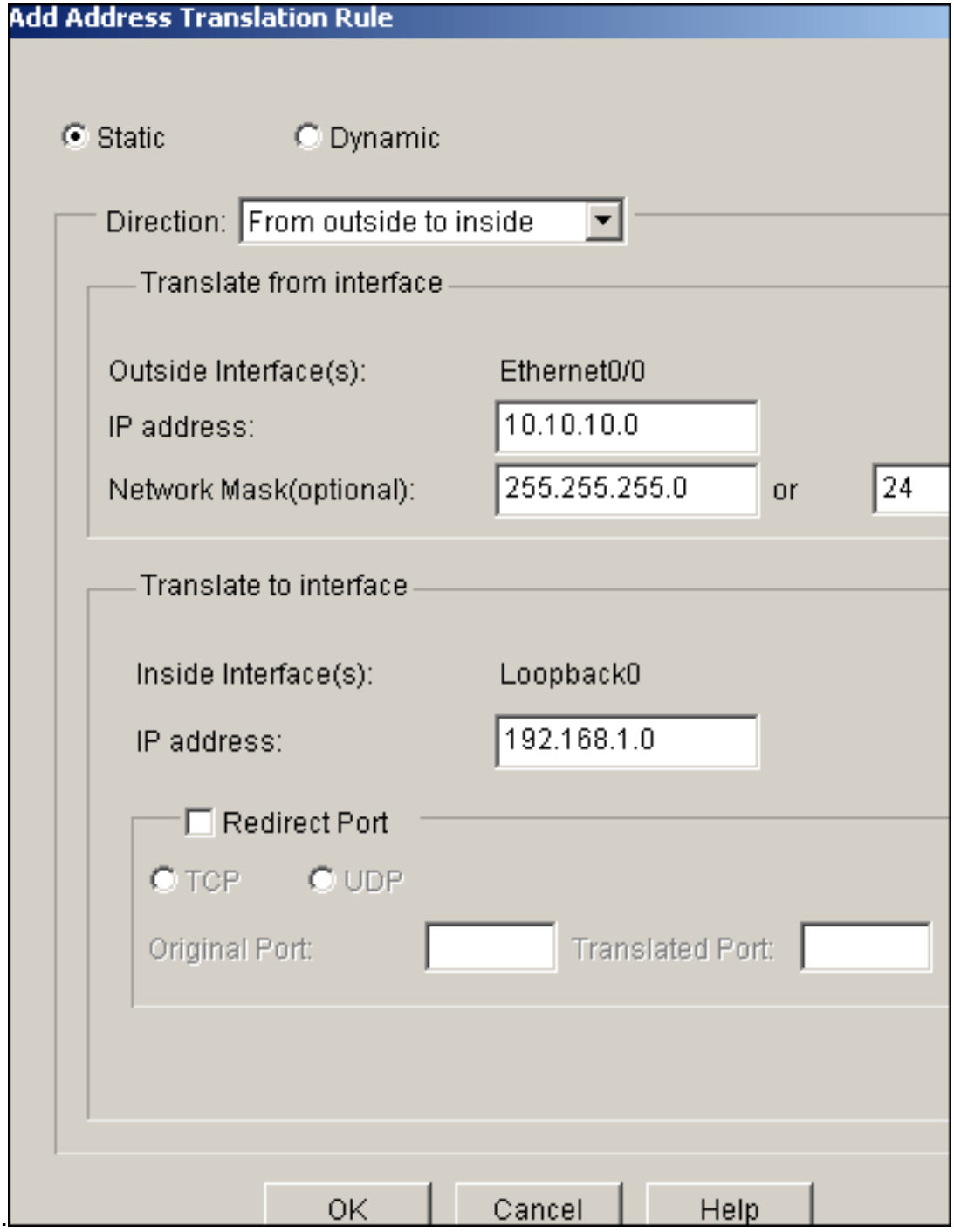


как показано.

4. **Нажмите кнопку ОК.**

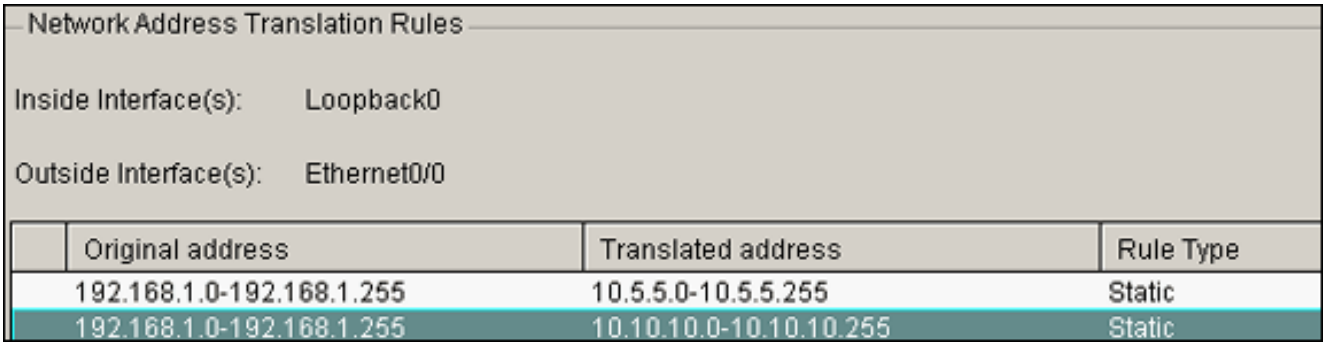


5. Еще раз **нажмите Add** для настройки преобразования NAT снаружи к внутреннему направлению как



показано.

6. **Нажмите кнопку ОК.**

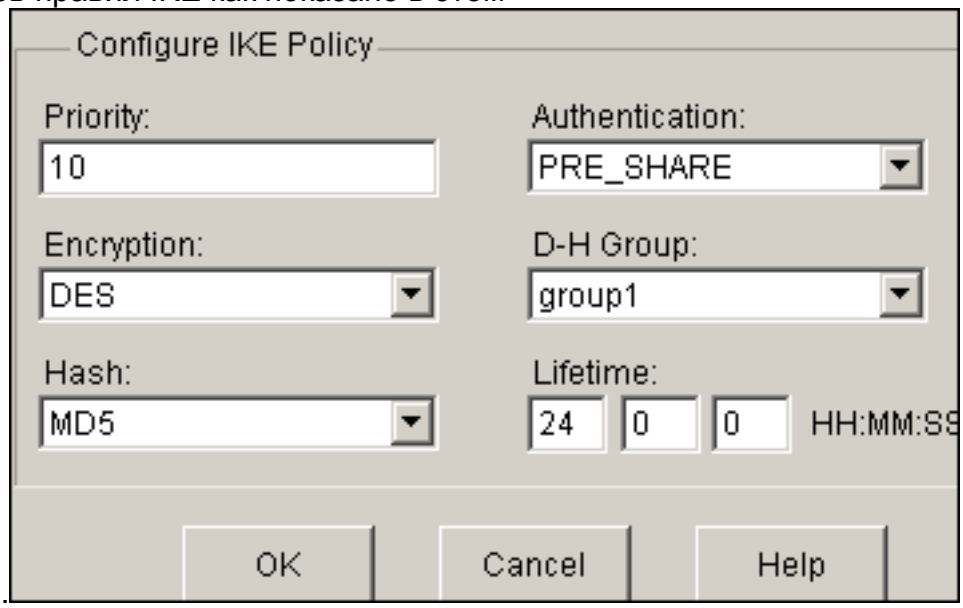


Примечание: Вот эквивалентная конфигурация CLI:

Конфигурация VPN

Выполните эти шаги для использования VPN для настройки SDM на маршрутизаторе Site_A:

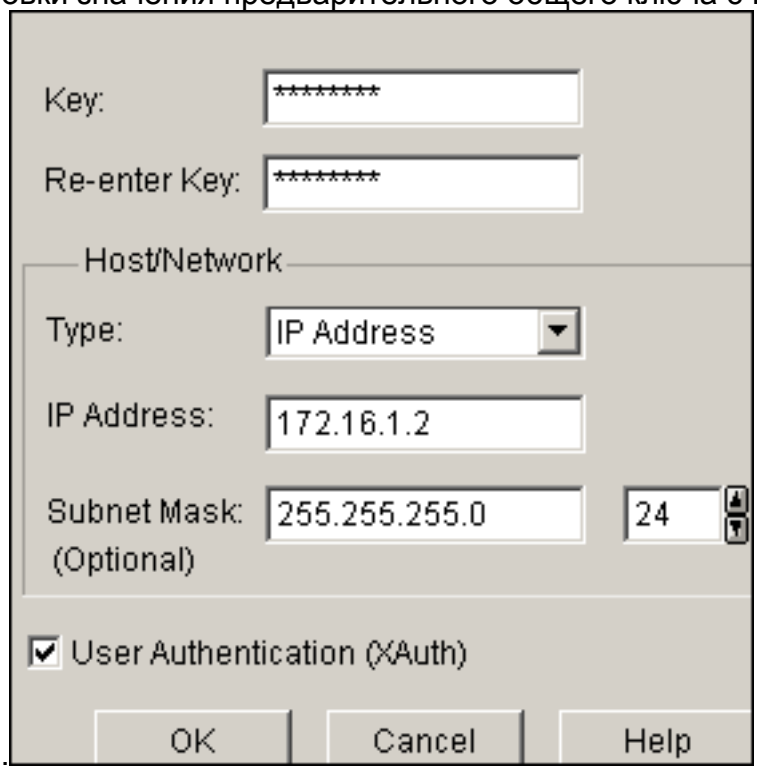
1. Выберите **Configure> VPN> VPN Components> IKE> IKE Policies> Add** для определения Наборов правил IKE как показано в этом образе.



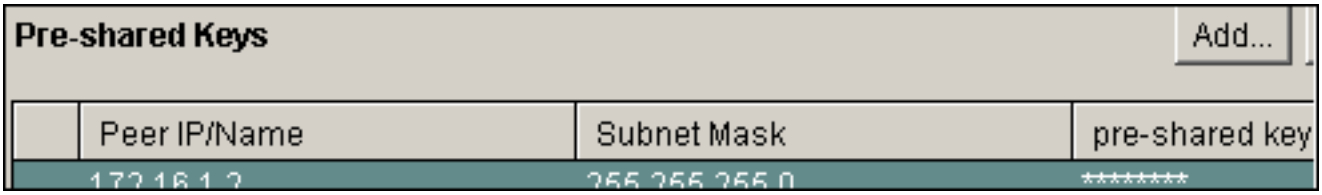
2. **Нажмите кнопку ОК.**

Примечание: Вот эквивалентная конфигурация CLI:

3. Выберите **Configure> VPN> VPN Components> IKE> Pre-shared Keys> Add** для установки значения предварительного общего ключа с IP - адресом адресуемым точки.

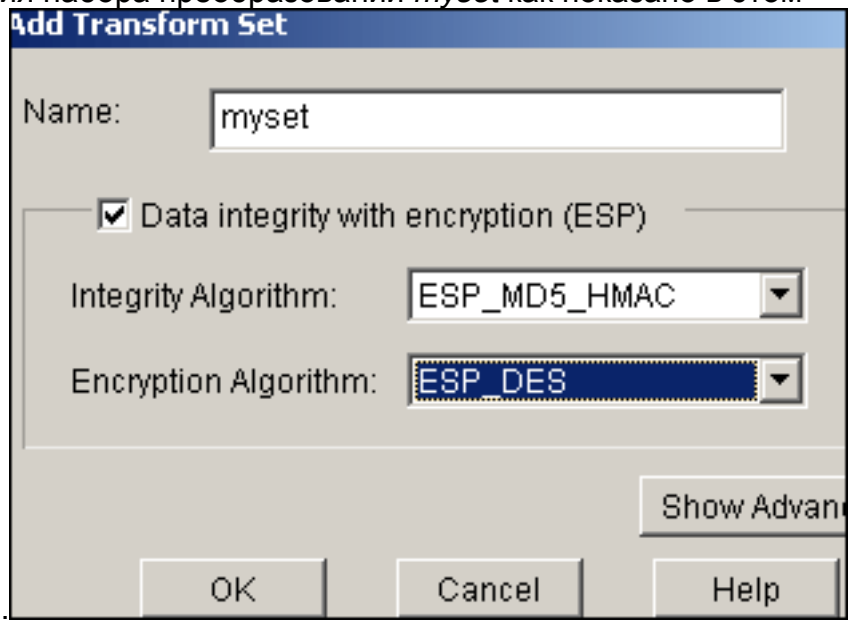


4. **Нажмите кнопку ОК.**



Примечание: Вот эквивалентная конфигурация CLI:

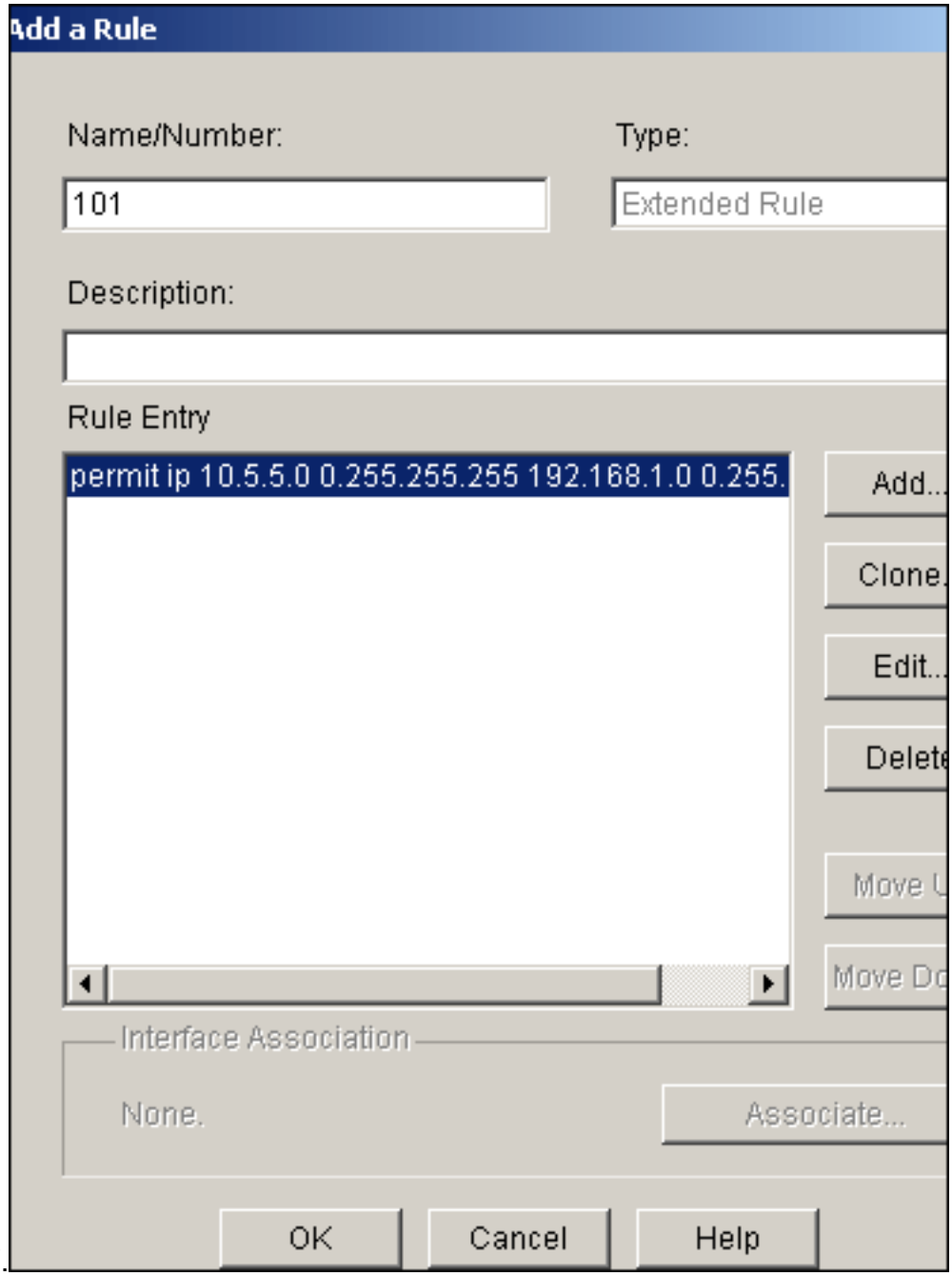
5. Выберите **Configure> VPN> VPN Components> IPSec> Transform Sets> Add** для создания набора преобразований *myset* как показано в этом образе.



6. **Нажмите кнопку ОК.**

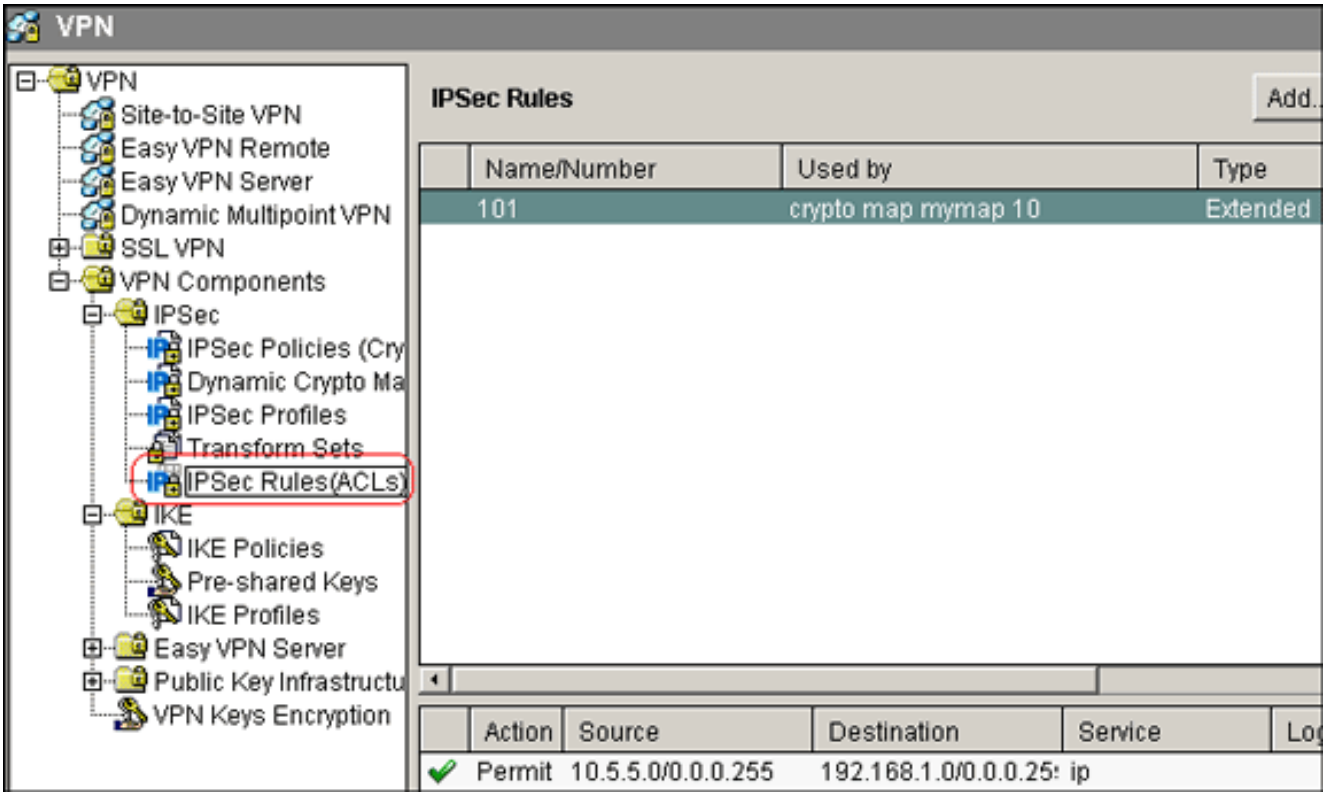
Примечание: Вот эквивалентная конфигурация CLI:

7. Выберите **Configure> VPN> VPN Components> IPSec> IPSec Rules (ACLs)> Add** для создания крипто-Списка контроля доступа (ACL)



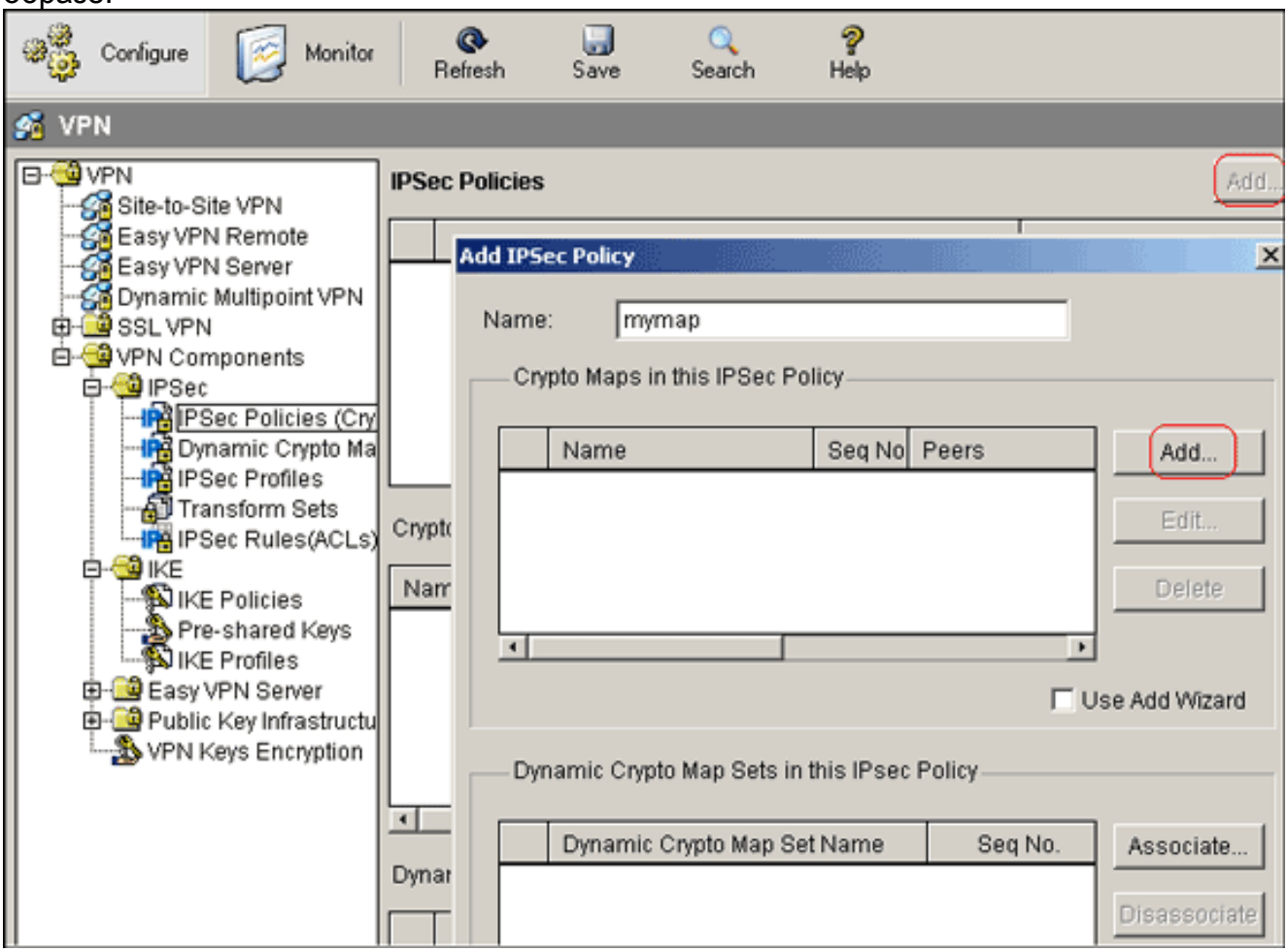
101.

8. **Нажмите кнопку ОК.**

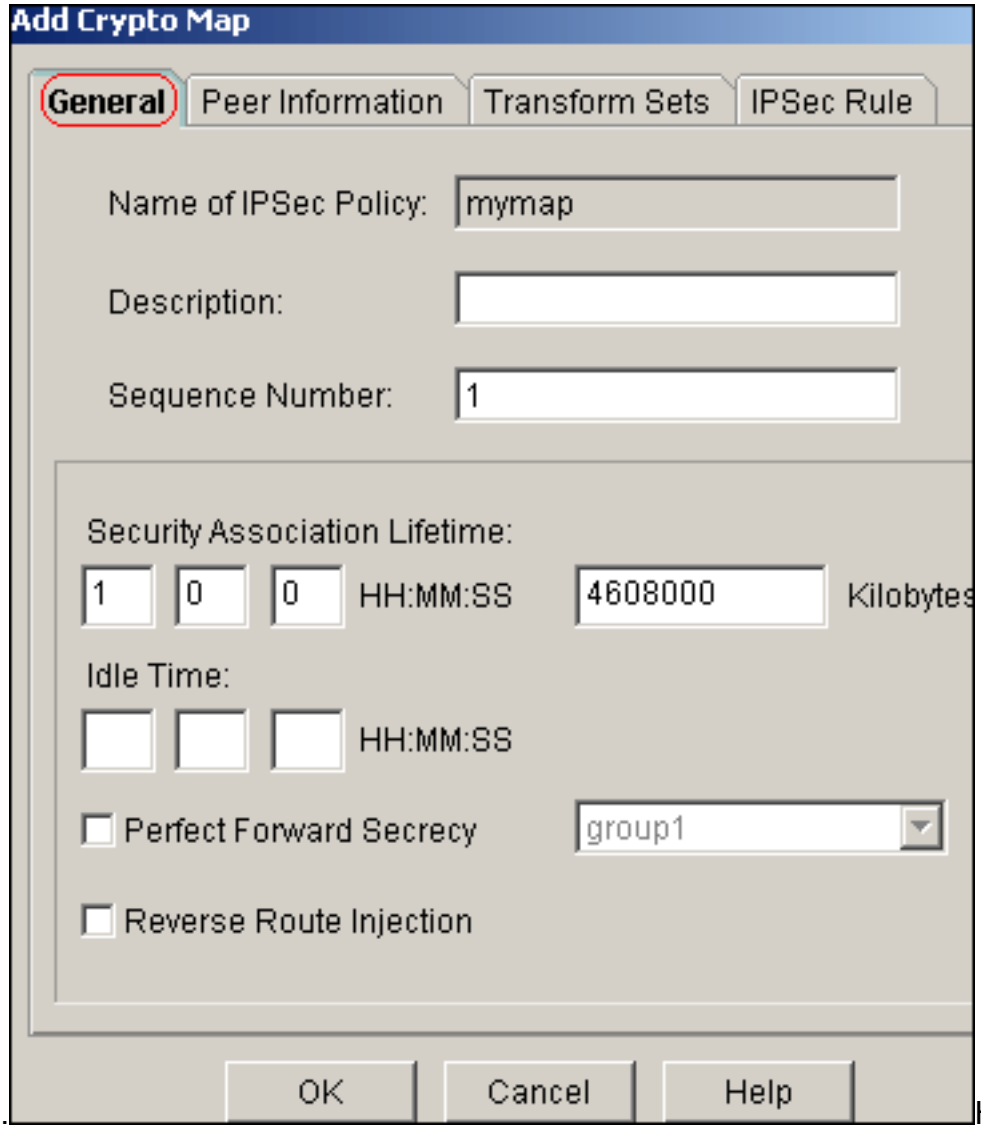


Примечание: Вот эквивалентная конфигурация CLI:

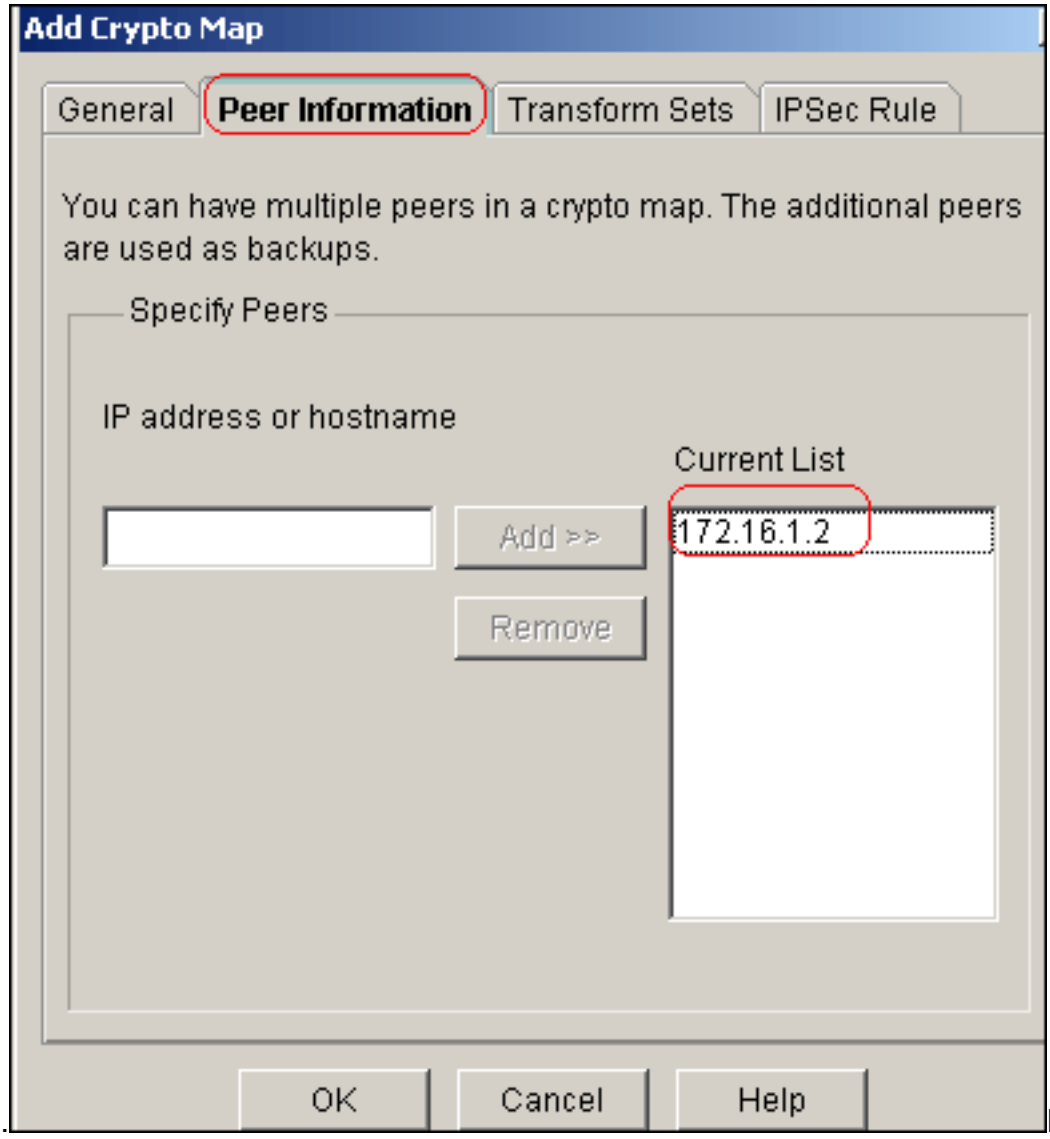
9. Выберите **Configure> VPN> VPN Components> IPSec> IPSec Policies> Add** для создания карты cryto *mymap* как показано в этом образе.



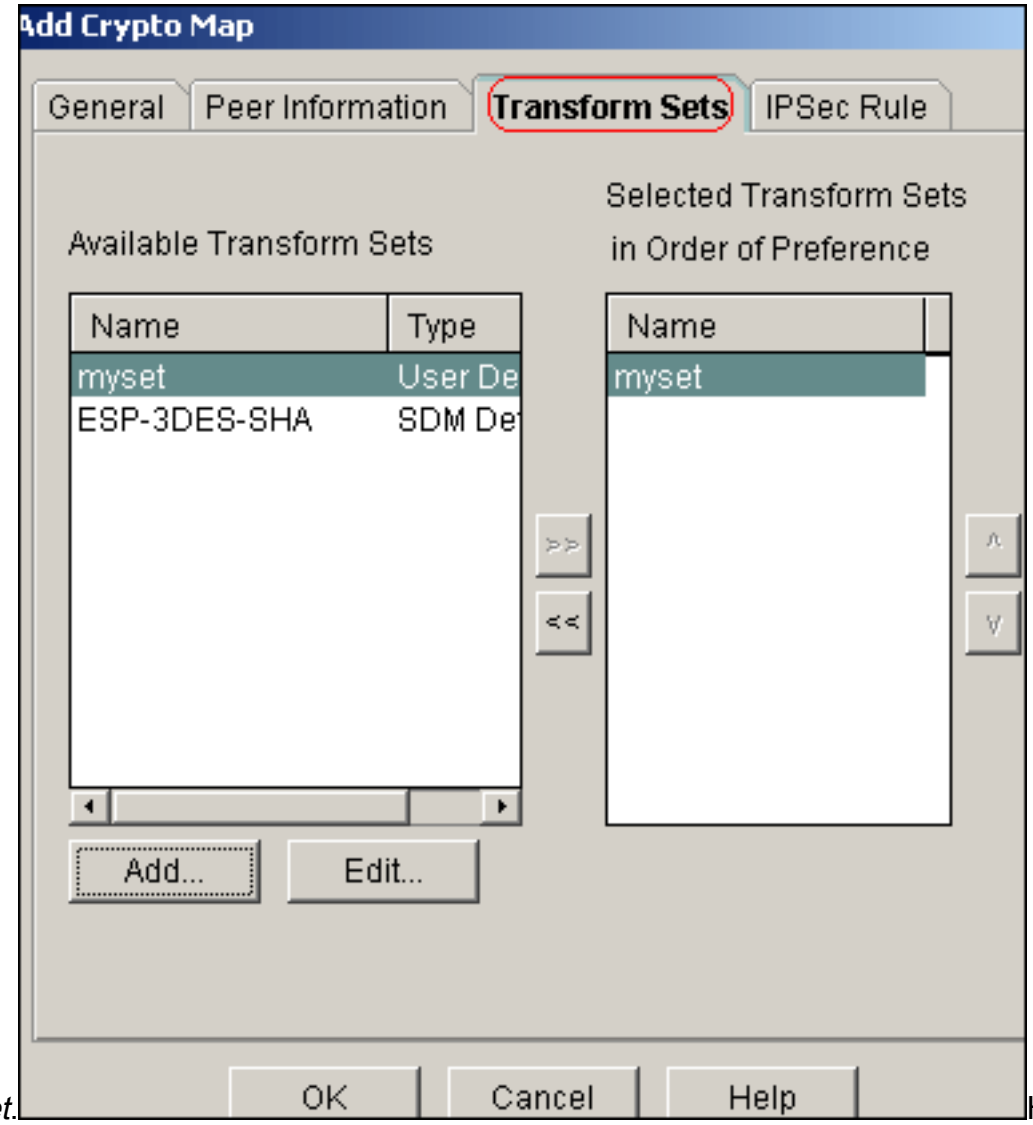
10. **Нажмите Add.**Нажмите **Вкладку Общие** и сохраните настройки по



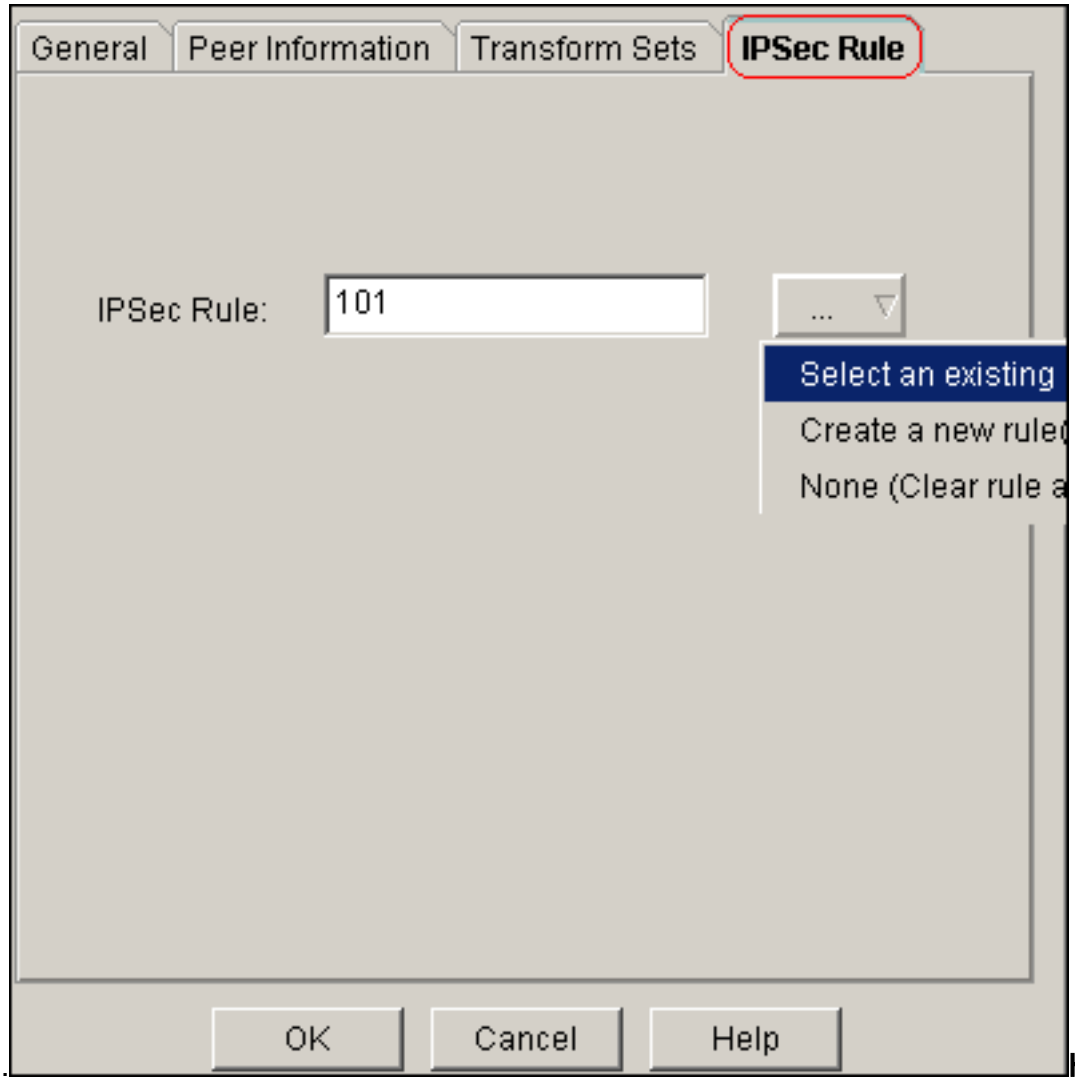
умолчанию. Нажмите вкладку **Peer Information** для добавления IP - адреса адресуемого точки



172.16.1.2. Нажмите вкладку **Transform Sets** для выбора желаемого набора преобразований

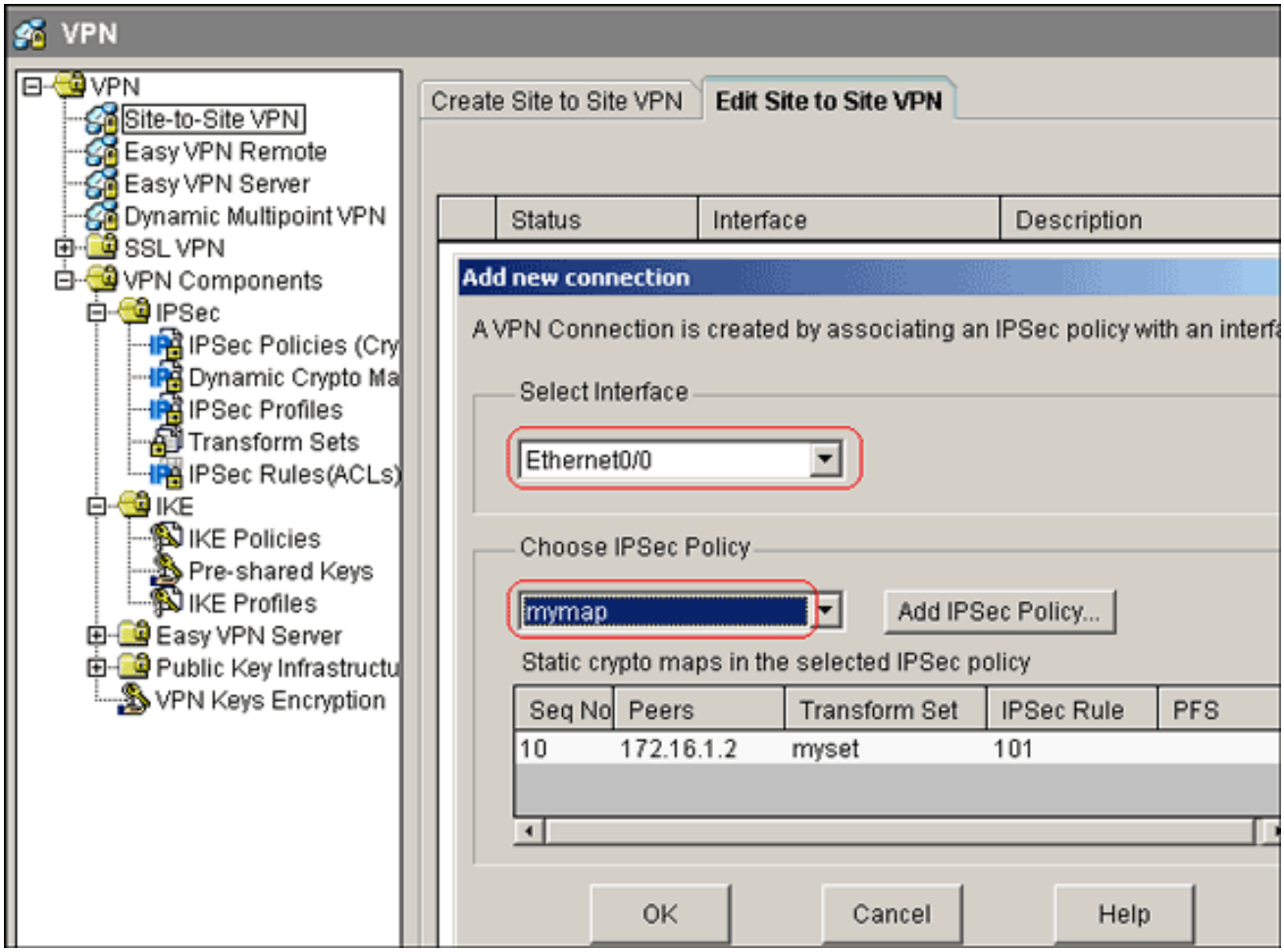


myset. Нажмите вкладку **IPSec Rule** для выбора существующего крипто-ACL

101. 

Нажмите кнопку OK.Примечание: Вот эквивалентная конфигурация CLI:

11. Выберите **Configure> VPN> Site-to-Site VPN> Edit Site-to-Site VPN> Add** для применения криптокарты *mymap* к интерфейсному Ethernet0/0.



12. **Нажмите кнопку OK.Примечание:** Вот эквивалентная конфигурация CLI:

[Конфигурация интерфейса командой строки маршрутизатора Site_A]

Маршрутизатор Site_A

```
Site_A#show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from
console by console
Building configuration...

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
!
```

```
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE
authentication ! ! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set myset
 match address 101
!--- Defines crypto map. ! ! ! ! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 half-duplex
 crypto map mymap
!--- Apply crypto map on the outside interface. ! ! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. ! ! control-plane ! ! line con 0 line aux 0 line
vty 0 4 ! ! end Site_A#
```

Конфигурация интерфейса командой строки маршрутизатора Site_B

Маршрутизатор Site_B

```
Site_B#show running_config
Building configuration...

Current configuration : 939 bytes
!
```

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set myset
 match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
 crypto map mymap
!
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

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

- show crypto isakmp sa — показывает все текущие ассоциации безопасности протокола

IKE (Internet Key Exchange, обмен ключами в Интернете) на одноранговом узле.Site_A#**show crypto isakmp sa**

```
dst             src             state          conn-id slot status
172.16.1.2      10.1.1.2        QM_IDLE              1    0 ACTIVE
```

- show crypto isakmp sa detail — Отображает подробные данные всех текущих SA IKE в узле.Site_A#**show cryto isakmp sa detail**

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime
 Cap.
1     10.1.1.2        172.16.1.2               ACTIVE des  md5  psk  1  23:59:42

       Connection-id:Engine-id =  1:1(software)
```

- show crypto ipsec sa — отображает настройки, используемые текущими SA.Site_A#**show crypto ipsec sa**

```
interface: Ethernet0/0
    Crypto map tag: mymap, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.16.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 3, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x1A9CDC0A(446487562)

     inbound esp sas:
      spi: 0x99C7BA58(2580003416)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3336)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A9CDC0A(446487562)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3335)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

```
     outbound ah sas:

     outbound pcp sas:
Site_A#
```

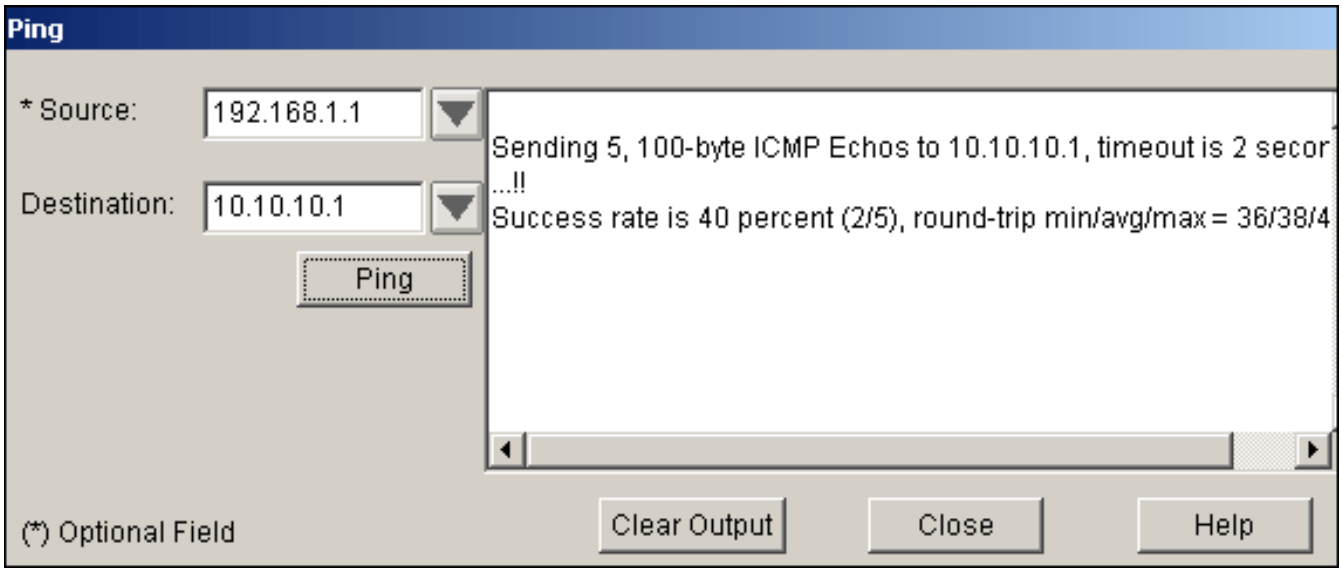
- **show ip nat translations** Информация о слоте преобразования Показов.`Site_A#`**`show ip nat translations`**

```
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.10.10.1         192.168.1.1
--- ---                ---                10.10.10.0         192.168.1.0
--- 10.5.5.1           192.168.1.1        ---                ---
--- 10.5.5.0           192.168.1.0        ---                ---
```

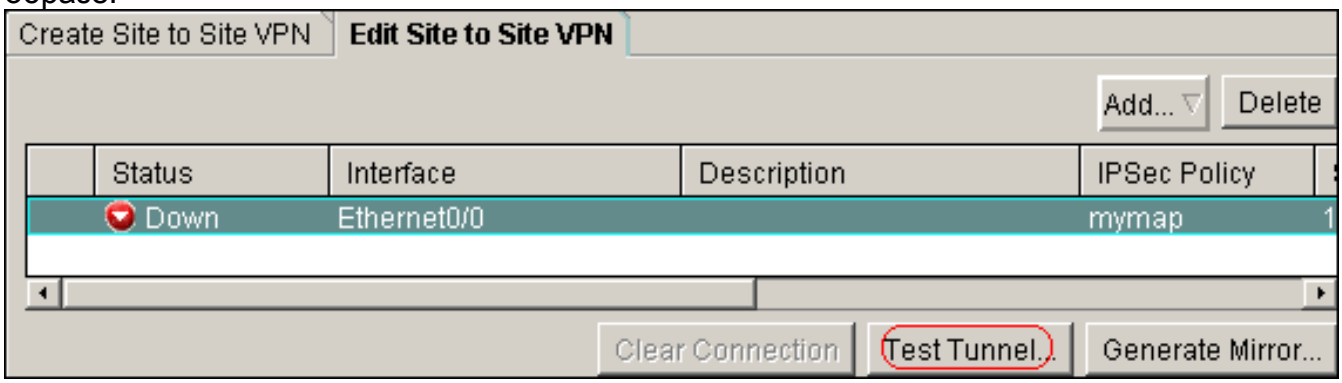
- **show ip nat statistics** статическую информацию о трансляции.`Site_A#`**`show ip nat statistics`**

```
Total active translations: 4 (2 static, 2 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
Hits: 42  Misses: 2
CEF Translated packets: 13, CEF Punted packets: 0
Expired translations: 7
Dynamic mappings:
Queued Packets: 0
Site_A#
```

- Выполните эти шаги для проверки соединения:В SDM выберите **Tools> Ping** для установления VPN-туннеля IPSec с source IP как 192.168.1.1 и IP - адрес назначения как 10.10.10.1.

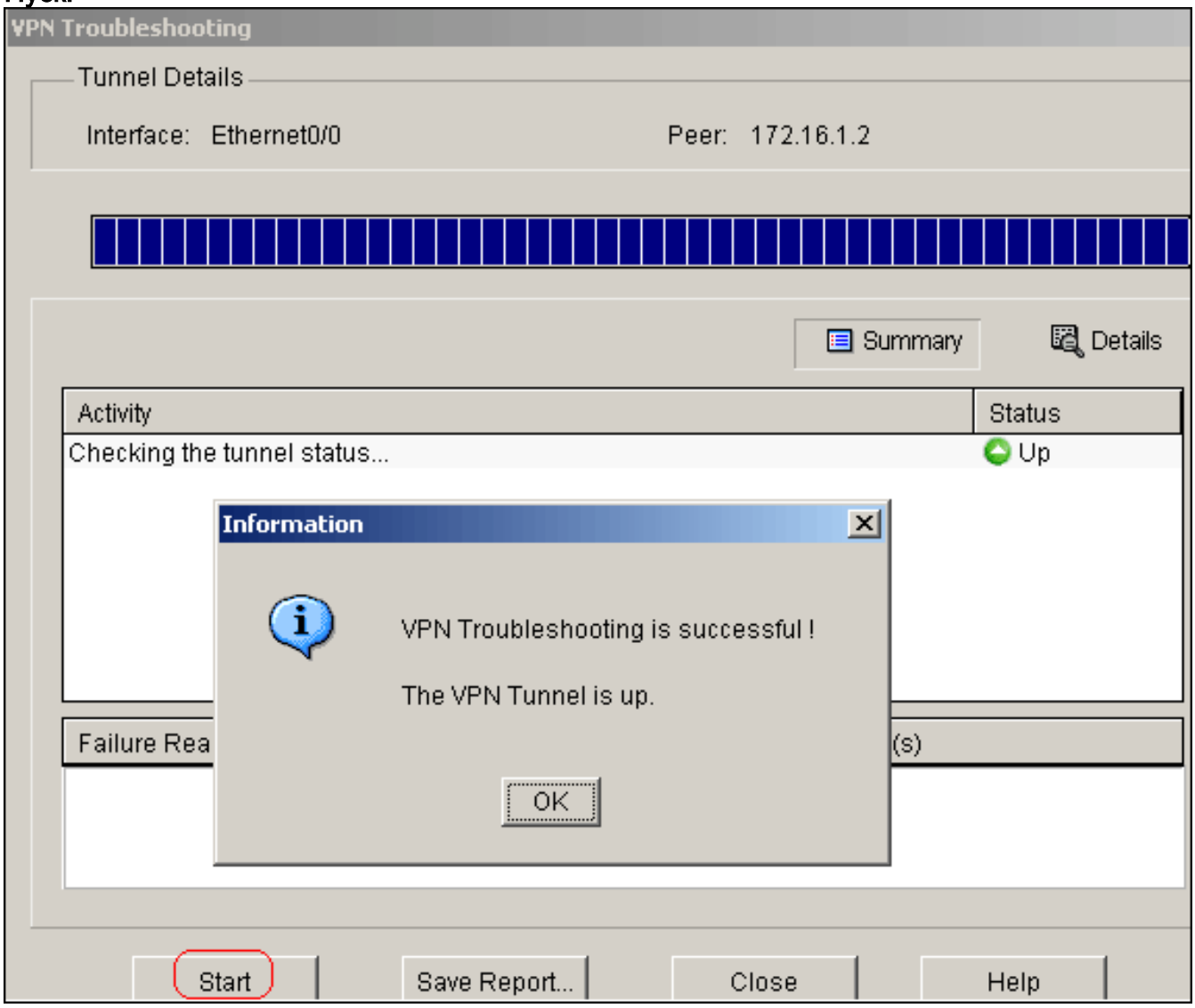


Нажмите **Test Tunnel**, чтобы проверить, что VPN-туннель IPSec установлен как показано в этом
образе.



Нажмите кнопку

Пуск.



Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

```
Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
```

Дополнительные сведения

- Устранение наиболее распространенных проблем удаленных VPN-подключений и VPN-туннелей LAN — LAN на базе протокола IPSec
- IPSec между ASA/PIX и Cisco VPN 3000 Concentrator с Примером конфигурации Наложений частной сети
- Cisco Systems – техническая поддержка и документация