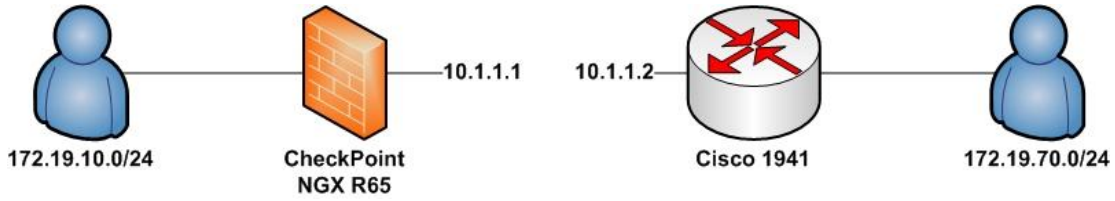
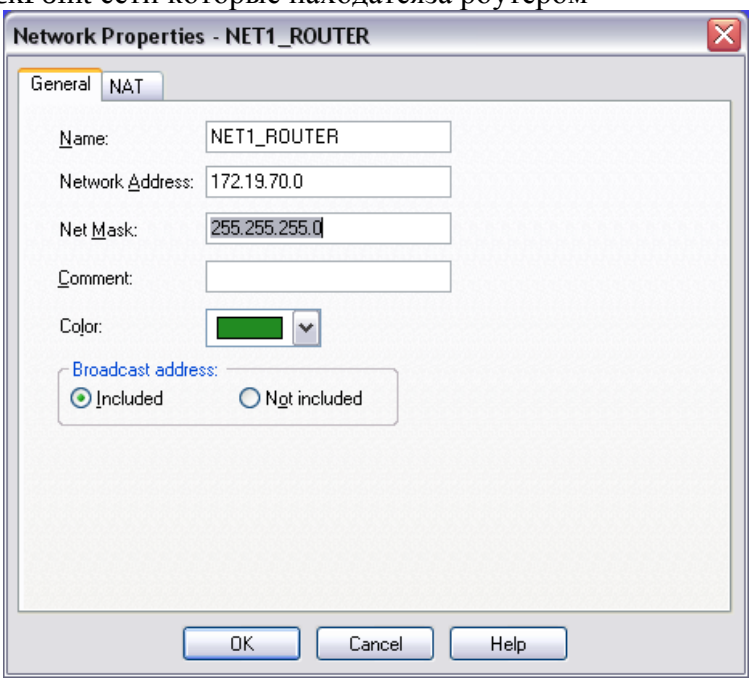
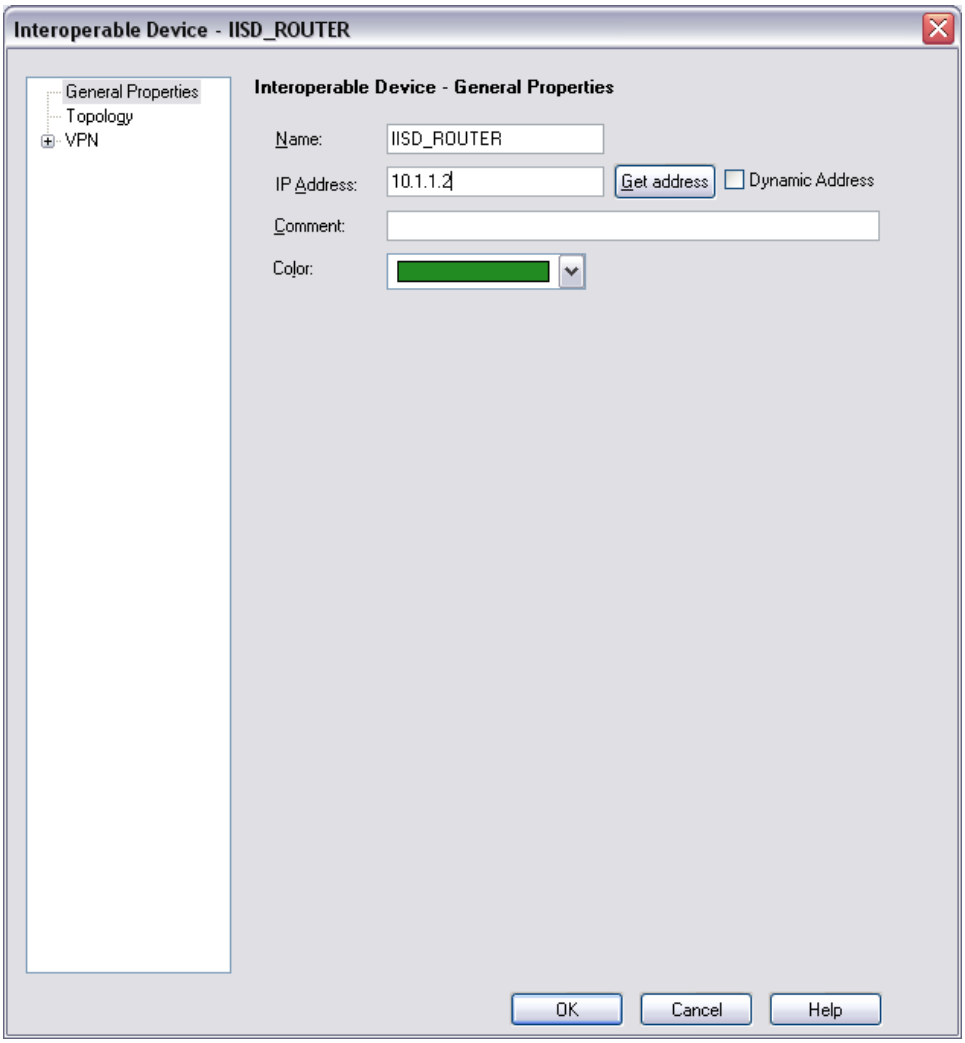
топология:



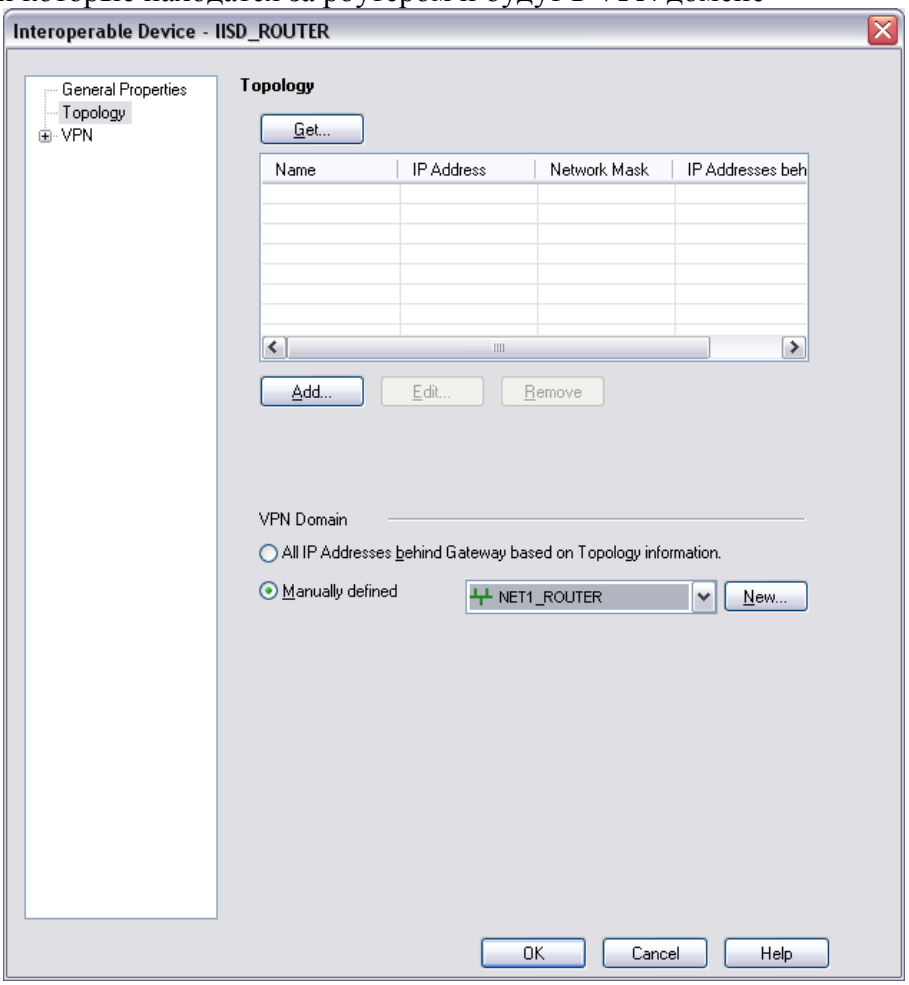
1. добавляем на CheckPoint сети которые находатсяза роутером



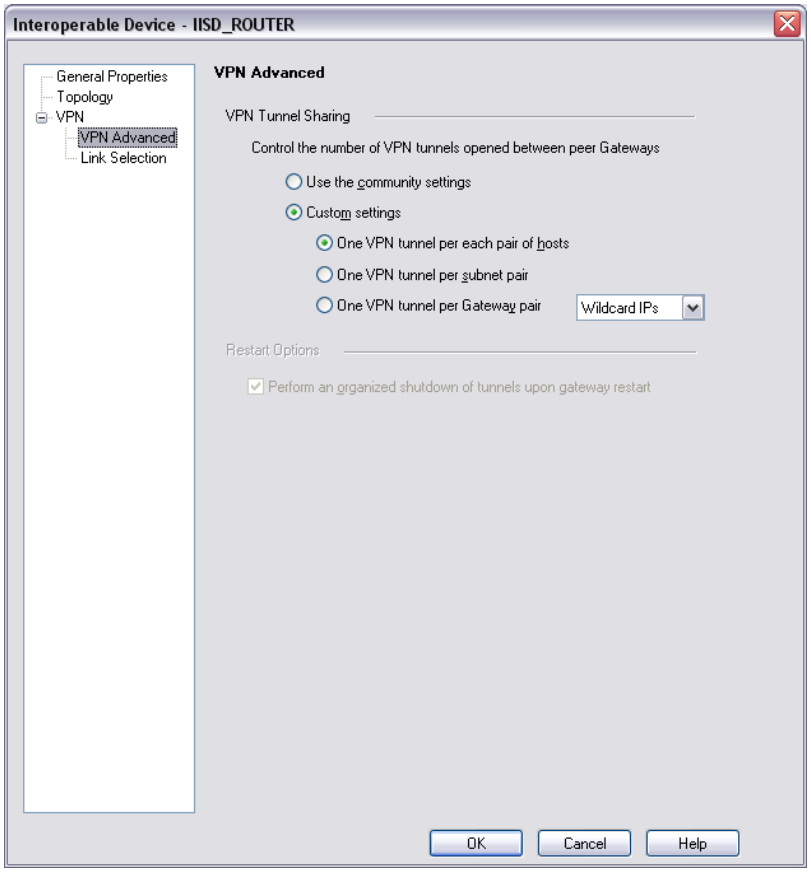
2. Добавляем interoperable device

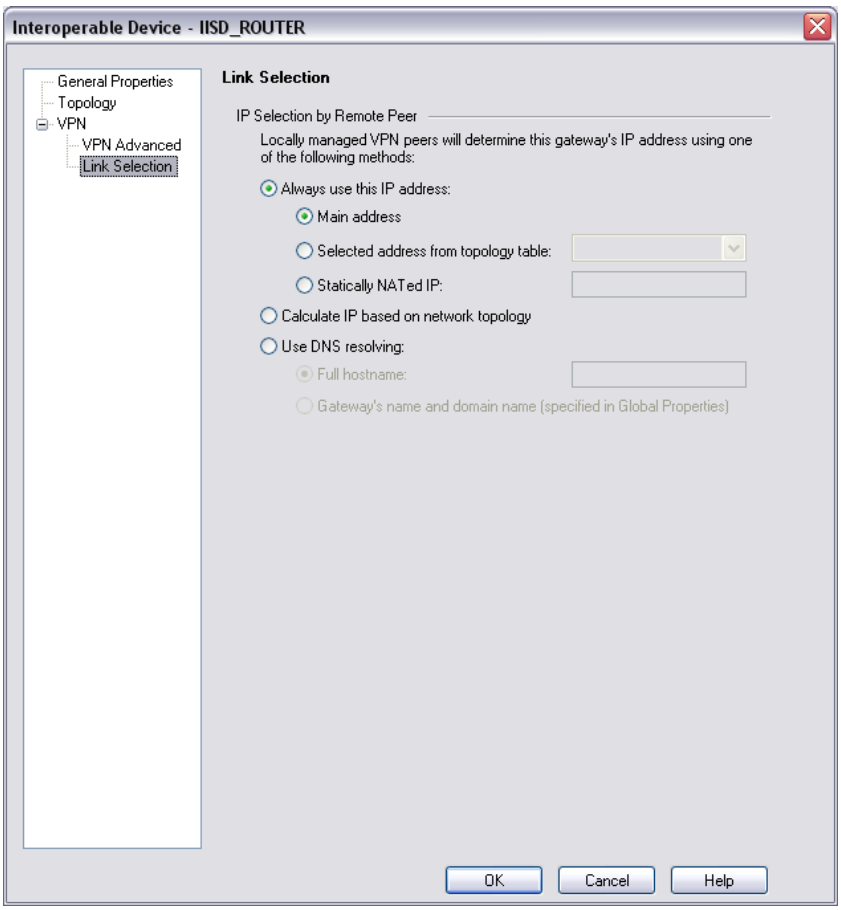


3. Выбираем сети которые находатся за роутером и будут в VPN домене

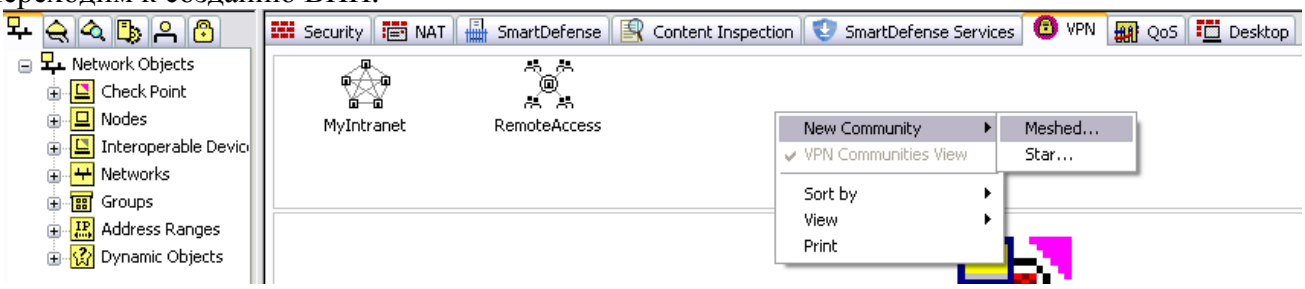


4. CheckPoint делает summary на сеть из впн домена, на пример если на чекпоинте есть две сети 172.19.10.0/24 и 172.19.11.0/24 то он зделает summary 172.19.10.1/23. И если на роутере в ACL стоит 172.19.10.0/24 то трафик генерируемый из сети 172.19.10.0/24 в сеть 172.19.70.0/24 не будет проходить. Чтобы CheckPoint не делал сумаризацию на interoperable device делаем следующее.

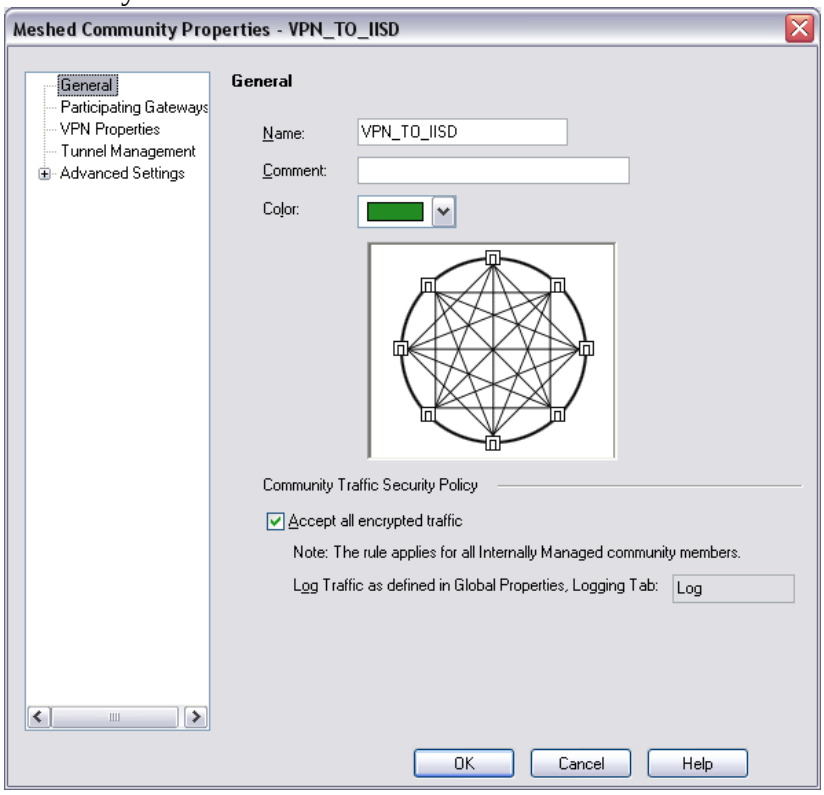




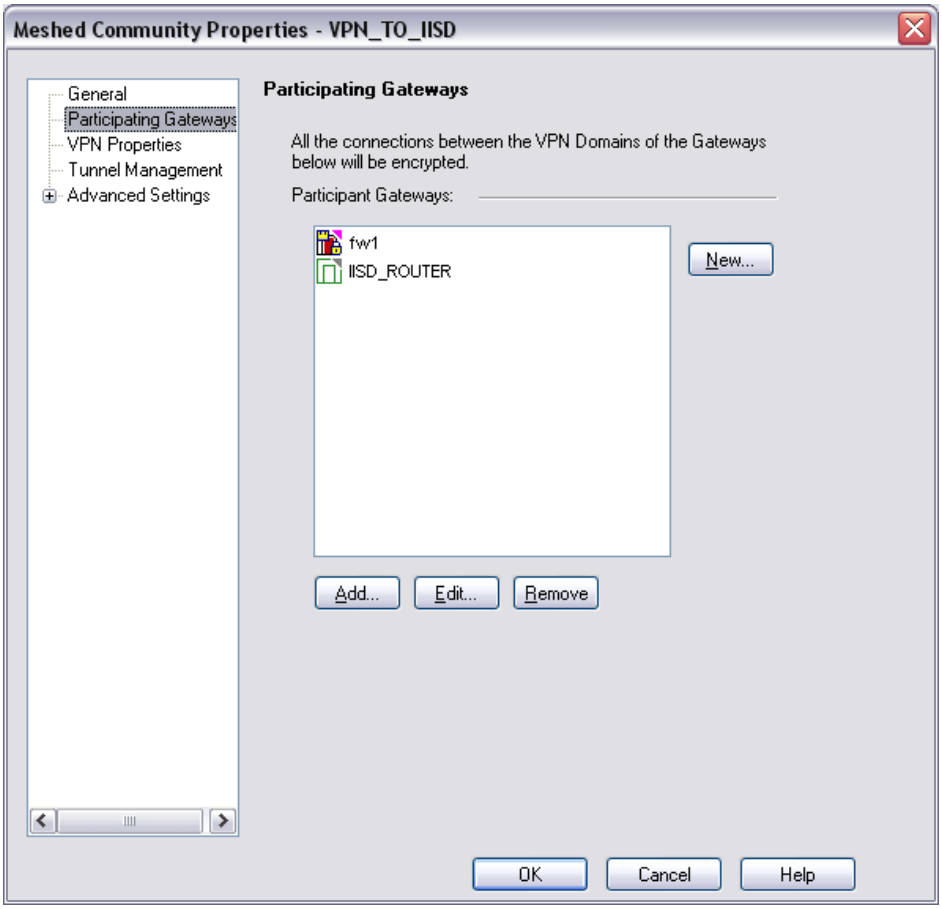
5. Переходим к созданию ВПН.



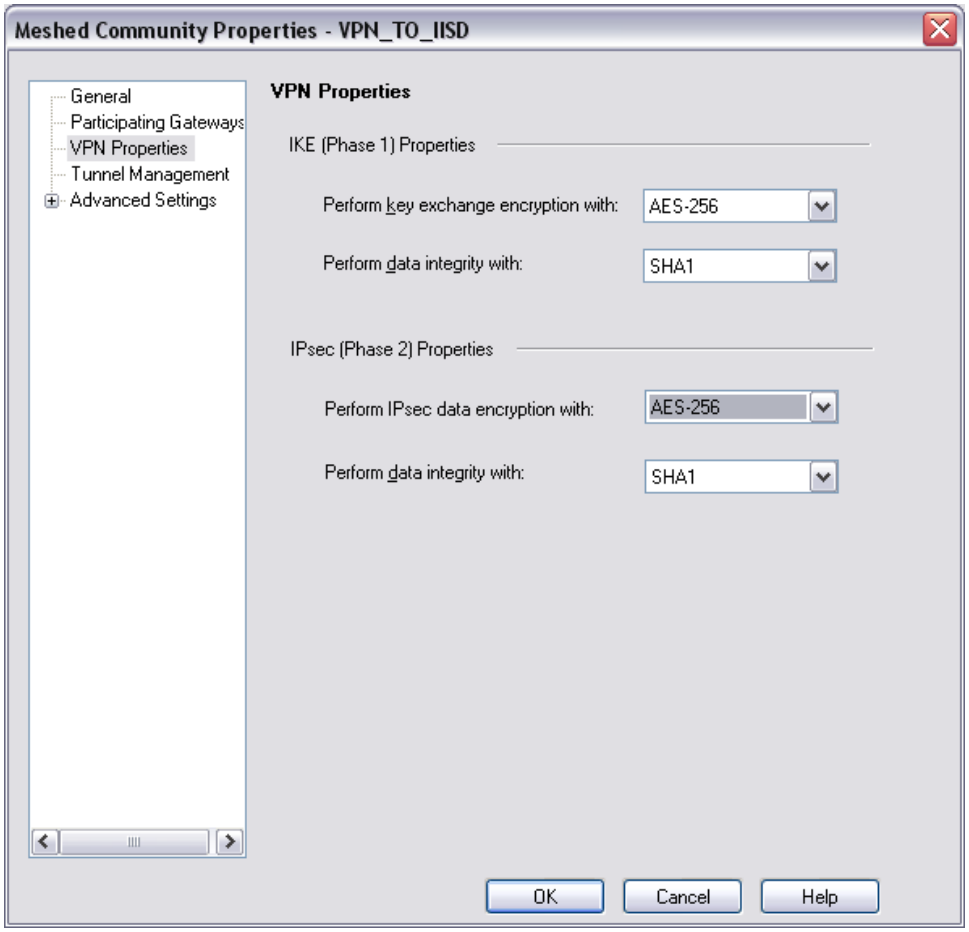
6. Создаем VPN Community



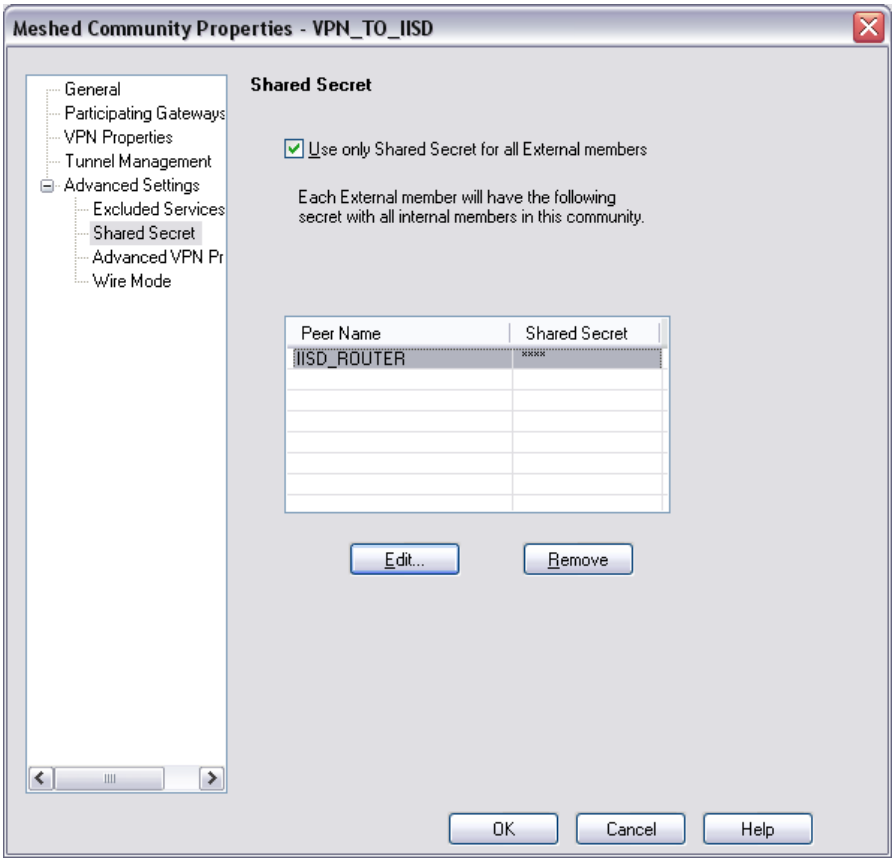
7. Добавляем девайсы



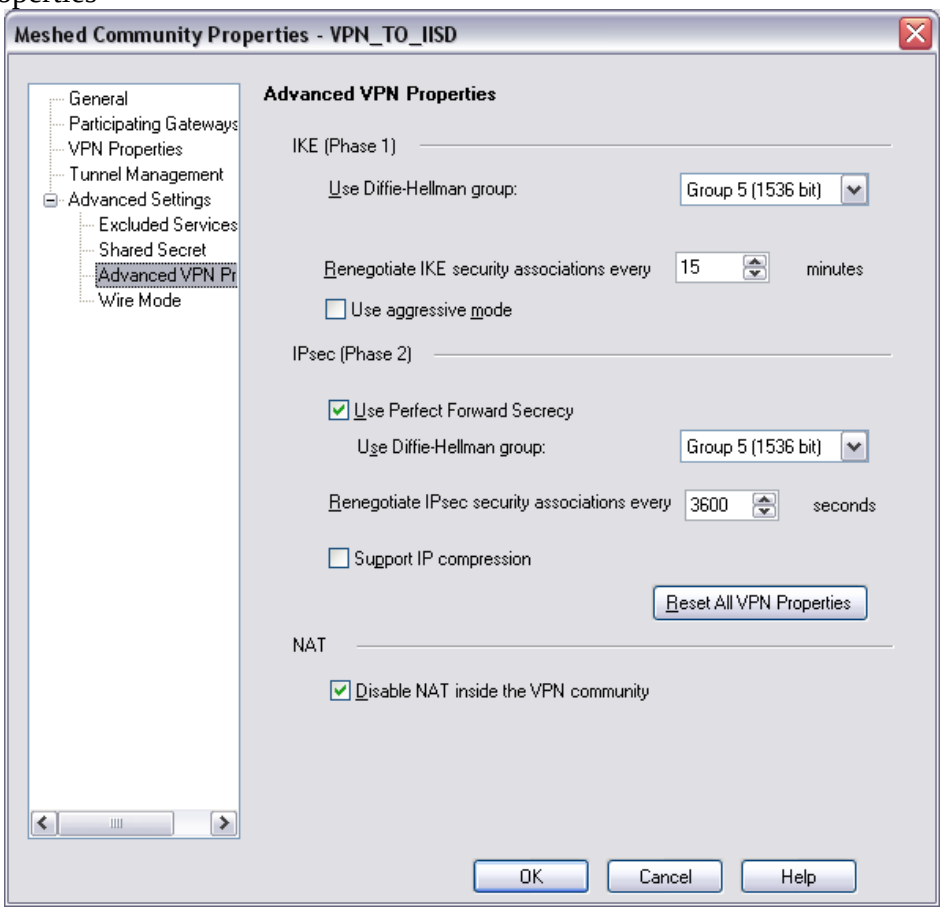
8. VPN Properties



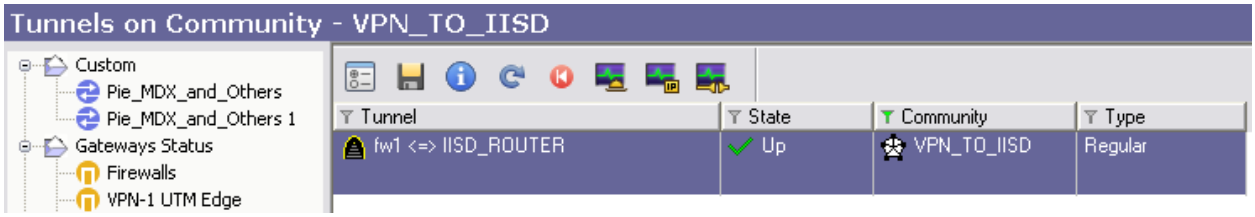
9. добавляем shared secret



10. Advanced vpn properties



11. Применяем правила



Примечание. У меня на чекпоинте сети в впн домене не нателись.

Router configuration

```
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp key ********************** address 0.0.0.0 0.0.0.0

crypto ipsec transform-set 60 esp-aes 256 esp-sha-hmac

crypto map MYMAP 10 ipsec-isakmp
 set peer 10.1.1.1
 set security-association lifetime seconds 900
 set transform-set 60
 set pfs group5
 match address VPN

interface GigabitEthernet0/0
 description <<LINK-ISP>>
 ip address 10.1.1.2 255.255.255.240
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
 crypto map MYMAP

ip nat inside source list NAT interface GigabitEthernet0/0 overload

ip access-list extended NAT
 deny   ip 172.19.70.0 0.0.0.255 172.19.10.0 0.0.0.255
 permit ip 172.19.70.0 0.0.0.255 any

ip access-list extended VPN
 permit ip 172.19.70.0 0.0.0.255 172.19.10.0 0.0.0.255
```