Настройка туннеля IPSec между межсетевым экраном Cisco Secure PIX и межсетевым экраном Checkpoint NG

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Схема сети
Условные обозначения
Настройка PIX
Настройте контрольную точку NG
Проверка
Проверьте конфигурацию PIX
Обзорный статус туннеля на контрольной точке NG
Устранение неполадок
Устраните неполадки конфигурации PIX
Суммирование сетей
Обзорные журналы контрольной точки NG
Дополнительные сведения

Введение

Этот документ демонстрирует, как настроить Туннель IPSec с предварительными общими ключами для передачи между двумя частными сетями. В данном примере связывающиеся сети 192.168.10.x частная сеть в межсетевом экране Cisco Secure PIX и 10.32. x . x частная сеть в Межсетевом экране Следующего поколения (NG) CheckpointTM.

Предварительные условия

Требования

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

- Трафик из PIX и в NG CheckpointTM к Интернету (представленный здесь 172.18.124.x сети) должен течь перед началом этой конфигурации.
- Пользователи должны быть знакомы с принципами согласования IPSec. Этот процесс

может быть разделен на пять этапов, включая две фазы Протокола IKE.Туннель IPSec инициирован содержательным трафиком. Трафик считается содержательным при передаче между двумя одноранговыми узлами IPsec.На втором этапе обмена ключами (IKE) для равноправных пользователей протокола IPSec выполняется согласование установленной политики сопоставлений безопасности (SA) IKE. По завершении аутентификации одноранговых узлов создается защищенный туннель с применением протокола ISAKMP.На втором этапе обмена ключами (IKE) одноранговые узлы IPsec используют проверенный и безопасный туннель для согласования преобразований IPSec SA. Согласование общей политики определяет то, как будет установлен туннель IPSec.Туннель IPSec создан, и данные передаются между узлами IPSec на основании параметров IPSec, настроенных в наборах преобразования IPSec.Разъединение туннеля IPSec выполняется при удалении сопоставлений безопасности (IPSec SA) или по истечении срока их действия.

Используемые компоненты

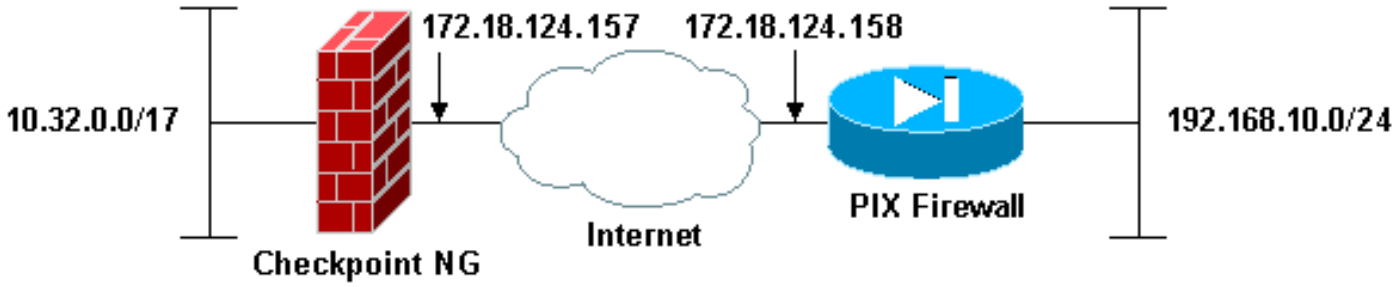
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Программное обеспечение PIX версии 6.2. 1
- Межсетевой экран NG CheckpointTM

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.

Схема сети

В настоящем документе используется следующая схема сети:



Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка PIX

Этот раздел предоставляет вам информацию по настройке функций, описанную в этом документе.

Конфигурация PIX

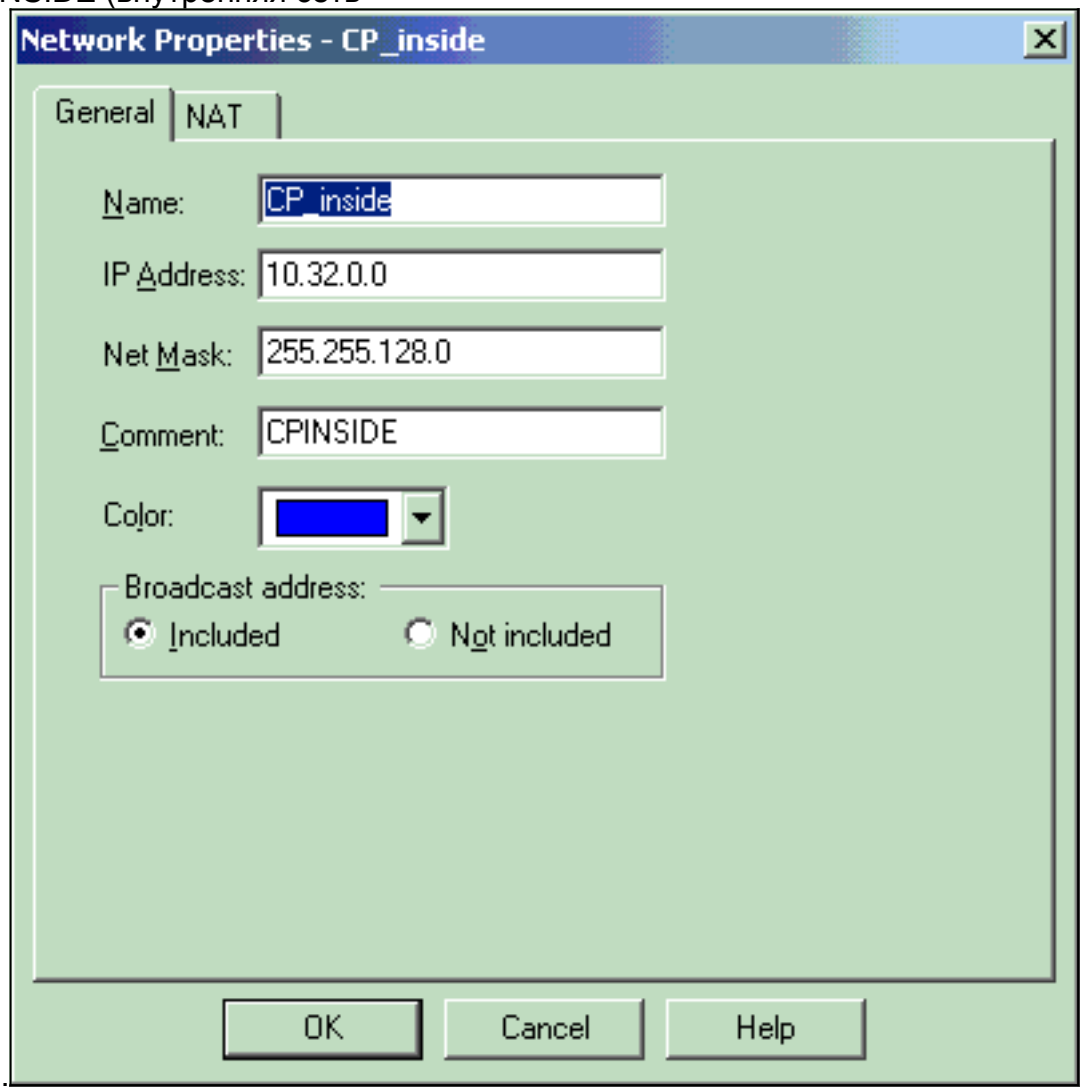
```
PIX Version 6.2(1)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname PIXRTPVPNdomain-name
cisco.comfixup protocol ftp 21fixup protocol http
80fixup protocol h323 h225 1720fixup protocol h323 ras
1718-1719fixup protocol ils 389fixup protocol rsh
514fixup protocol rtsp 554fixup protocol smtp 25fixup
protocol sqlnet 1521fixup protocol sip 5060fixup
protocol skinny 2000names!--- Interesting traffic to be
encrypted to the Checkpoint? NG.access-list 101 permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0!--
- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint? NG.access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0
255.255.128.0pager lines 24interface ethernet0
10basetinterface ethernet1 10fullmtu outside 1500mtu
inside 1500ip address outside 172.18.124.158
255.255.255.0ip address inside 192.168.10.1
255.255.255.0ip audit info action alarmip audit attack
action alarmpdm history enablearp timeout 14400global
(outside) 1 interface!--- Do not perform NAT on traffic
to the Checkpoint? NG.nat (inside) 0 access-list
nonatnat (inside) 1 0.0.0.0 0.0.0.0 0 0route outside
0.0.0.0 0.0.0.0 172.18.124.1 1timeout xlate
3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media
0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+aaa-server RADIUS protocol radiusaaa-
server LOCAL protocol localno snmp-server locationno
snmp-server contactsnmp-server community publicno snmp-
server enable trapsfloodguard enable!--- Permit all
inbound IPsec authenticated cipher sessions.sysopt
connection permit-ipsecno sysopt route dnat!--- Defines
IPsec encryption and authentication algorithms.crypto
ipsec transform-set rtptac esp-3des esp-md5-hmac!---
Defines crypto map.crypto map rtprules 10 ipsec-
isakmpcrypto map rtprules 10 match address 101crypto map
rtprules 10 set peer 172.18.124.157crypto map rtprules
10 set transform-set rtptac!--- Apply crypto map on the
outside interface.crypto map rtprules interface
outsideisakmp enable outside!--- Defines pre-shared
secret used for IKE authentication.isakmp key ********
address 172.18.124.157 netmask 255.255.255.255!---
Defines ISAKMP policy.isakmp policy 1 authentication
pre-shareisakmp policy 1 encryption 3desisakmp policy 1
hash md5isakmp policy 1 group 2isakmp policy 1 lifetime
86400telnet timeout 5ssh timeout 5terminal width
80Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5: end
```

Настройте контрольную точку NG

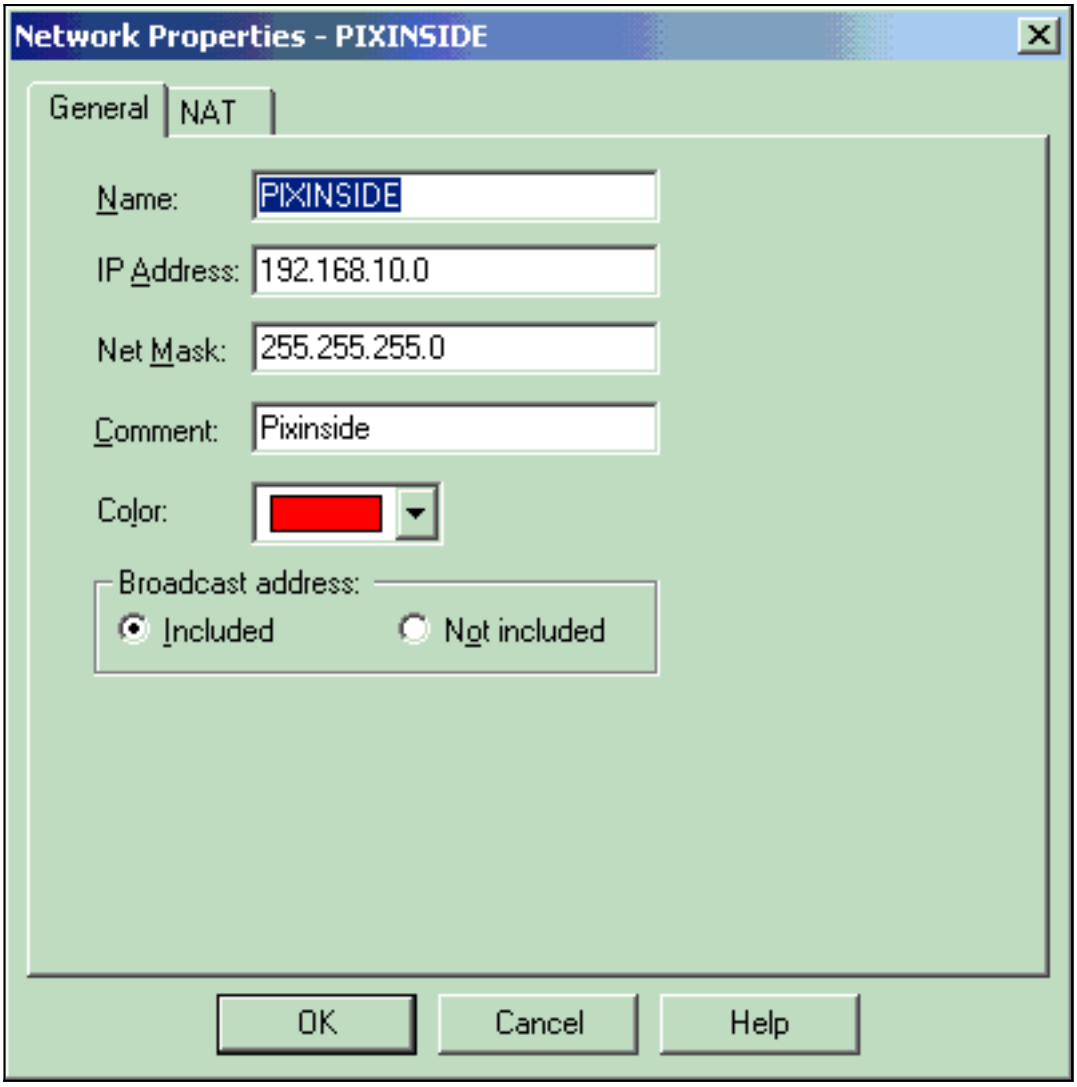
Сетевые объекты и правила определены на NG CheckpointTM для составления политики, которая принадлежит конфигурации VPN, которая будет установлена. Эта политика тогда установлена с помощью Редактора политики NG CheckpointTM для завершения стороны NG CheckpointTM конфигурации.

1. Создайте эти два сетевых объекта для сети Сеть Checkpoint и PIX Firewall, которые шифруют представляющий интерес трафик.Чтобы сделать это, выберите **Manage>**

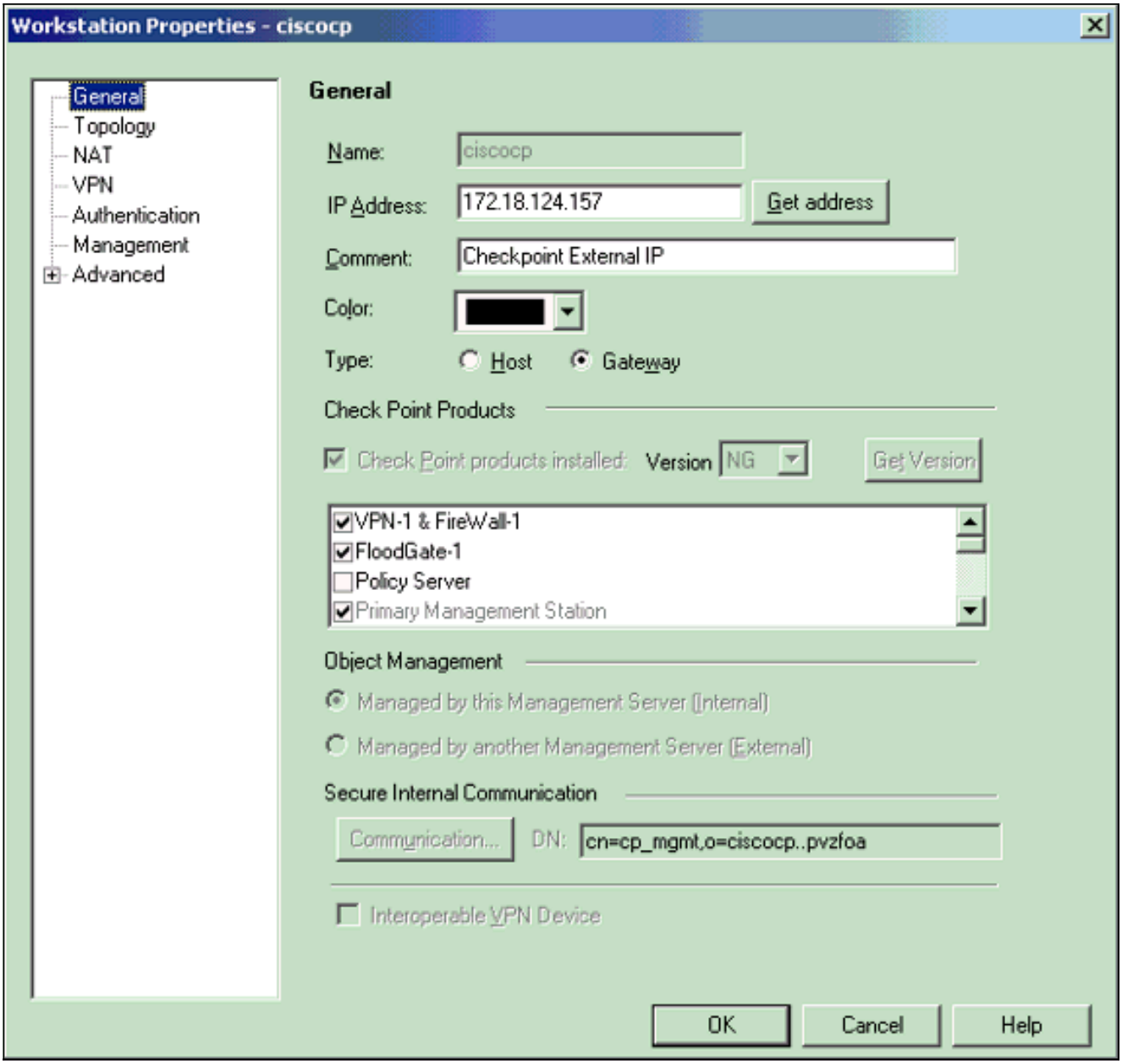
Network Objects, затем выберите **New> Network**. Введите соответствующую информацию о сети, затем нажмите **OK**.Эти примеры показывают установленный из сетевых объектов под названием CP_inside (внутренняя сеть NG CheckpointTM) и PIXINSIDE (внутренняя сеть

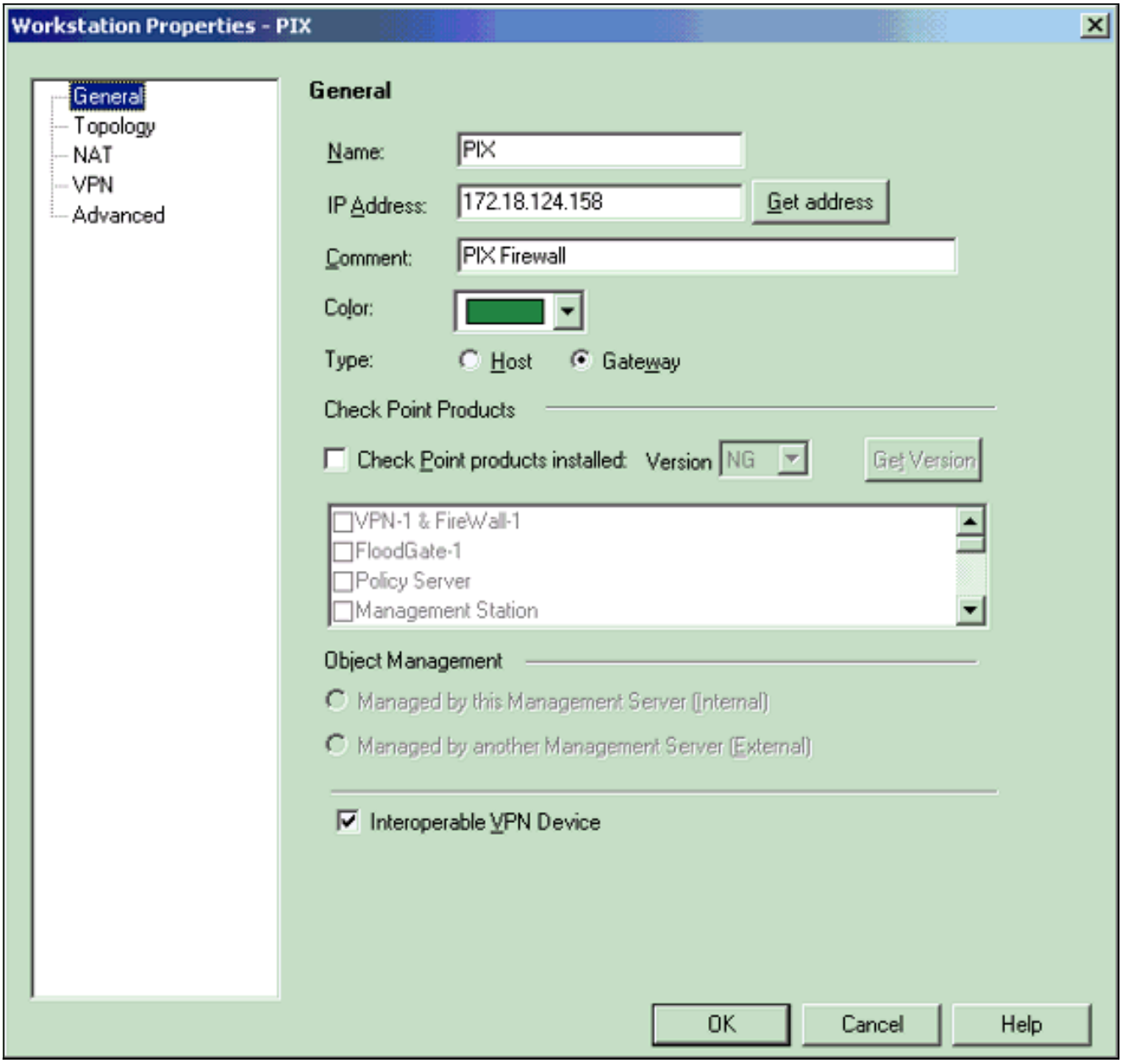


PIX).

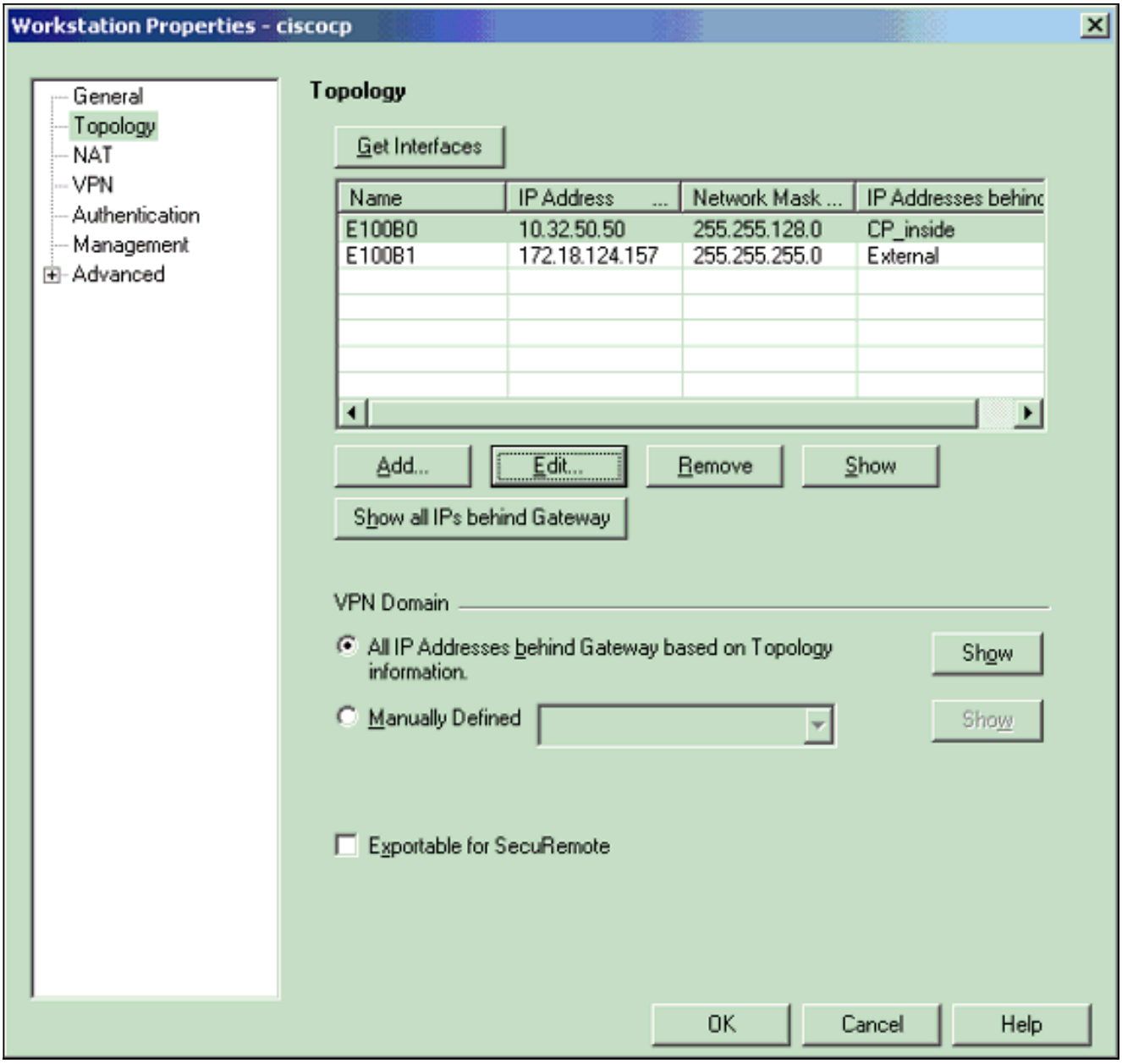


2. Создайте объекты рабочей станции для NG CheckpointTM и PIX. Чтобы сделать это, выберите **Manage> Network Objects> New> Workstation**.Обратите внимание на то, что можно использовать объект рабочей станции NG CheckpointTM, созданный во время начальной настройки NG CheckpointTM. Выберите опции, чтобы установить рабочую станцию как шлюз и взаимодействующее устройство VPN, и затем нажать **OK**.Эти примеры показывают установленный из объектов, названных ciscocp (NG **CheckpointTM**) и PIX (Межсетевой экран
PIX).

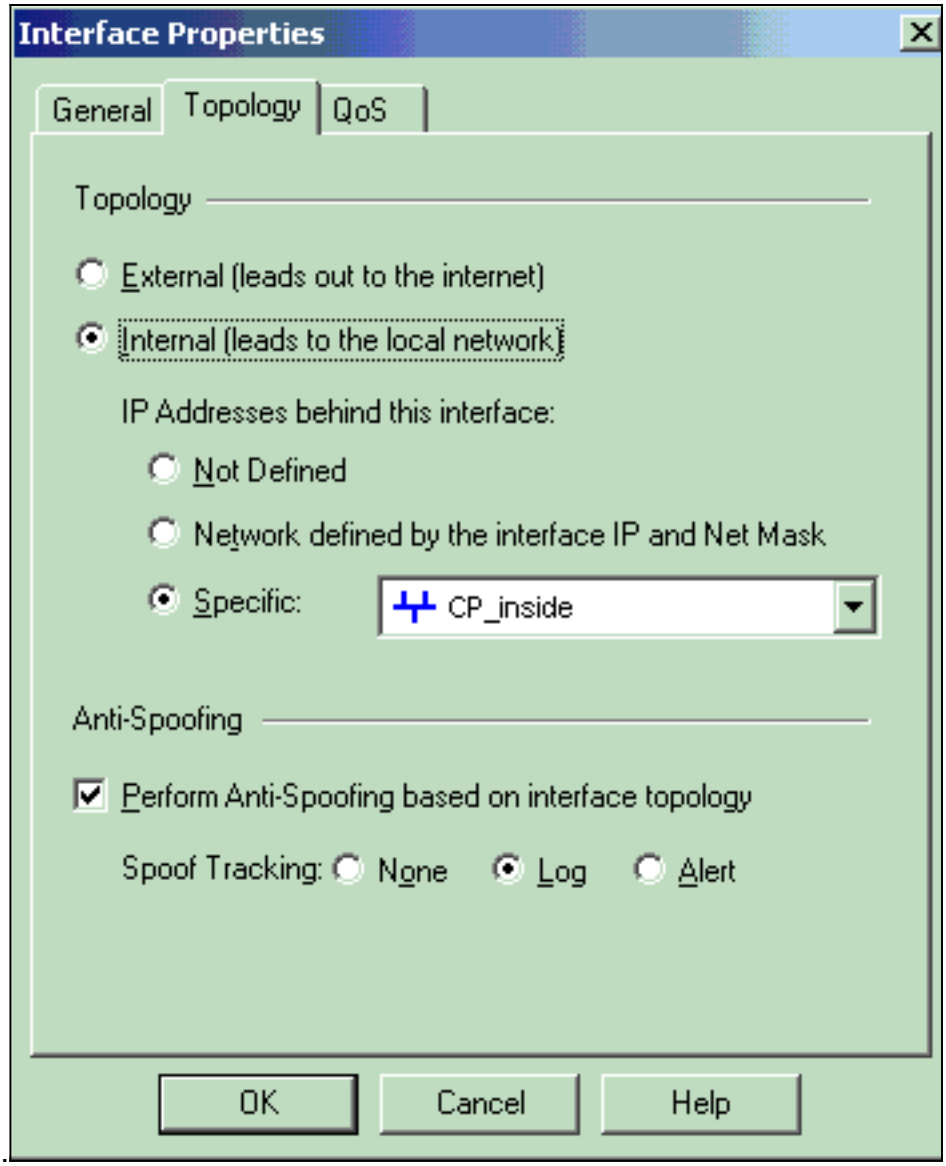

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



3. Выберите **Manage> Network objects> Edit** для открытия Окна Workstation Properties для рабочей станции NG CheckpointTM (ciscocp в данном примере).Выберите **Topology** от выборов на левой части окна, затем выберите сеть, которая будет зашифрована. Нажмите **Edit** для установки интерфейсных свойств.

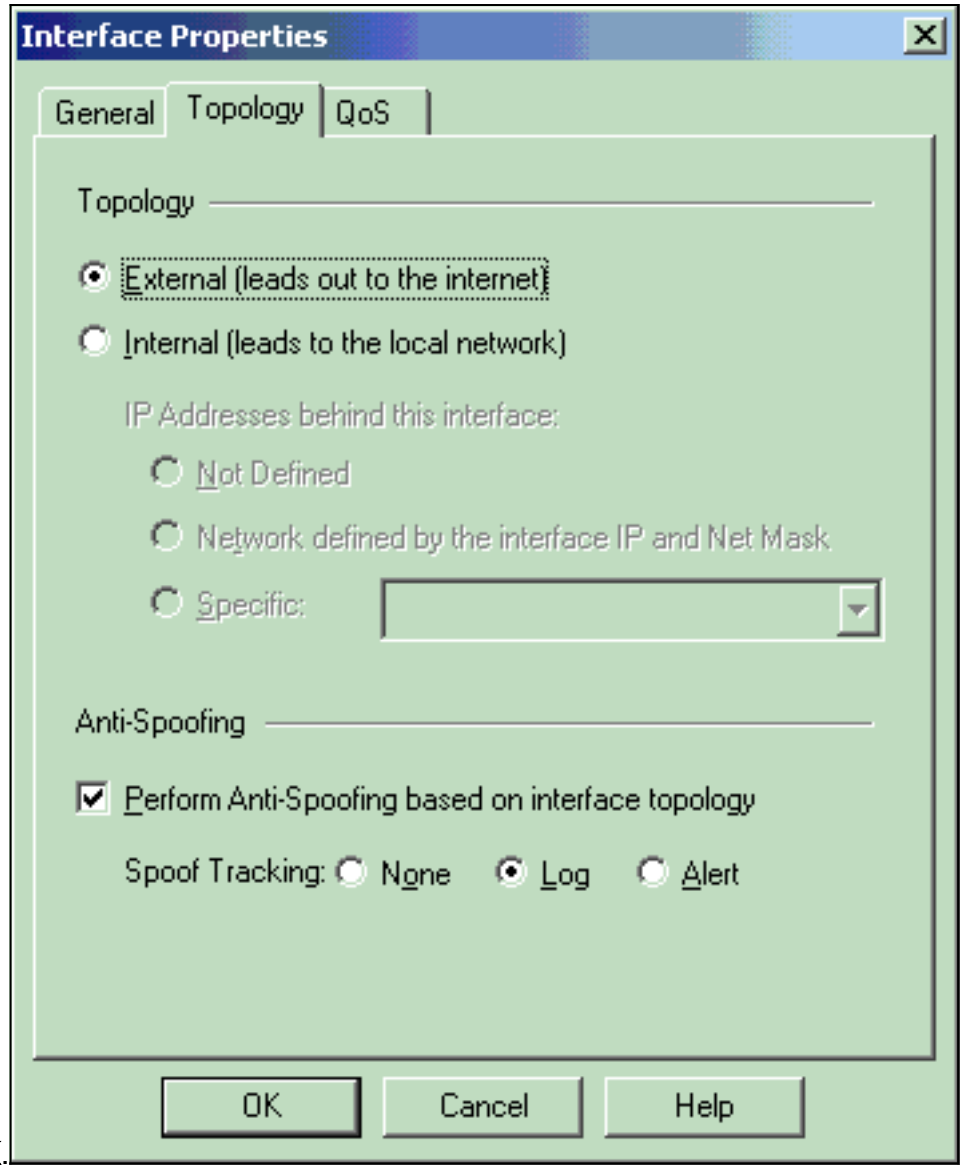


4. Выберите опцию, чтобы определять рабочую станцию как внутреннюю, затем задать соответствующий IP-адрес. **Нажмите кнопку OK.**В этой конфигурации CP_inside является внутренней сетью NG CheckpointTM. Выборы топологии, показанные здесь, называют рабочую станцию столь же внутренней и задают адрес как



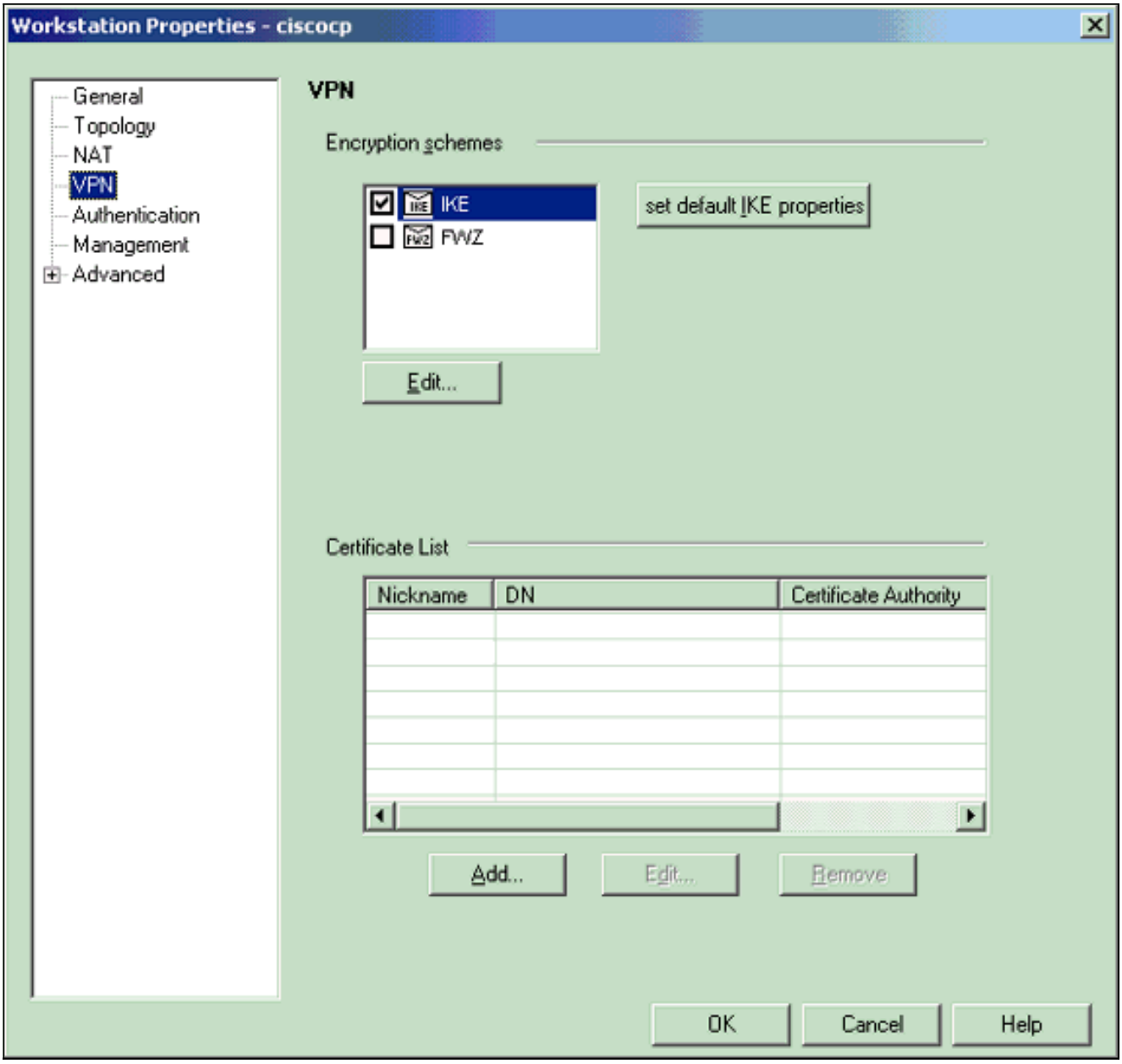
CP_inside.

5. От Окна Workstation Properties выберите внешний интерфейс на NG CheckpointTM, который выводит к Интернету, затем нажмите **Edit** для установки интерфейсных свойств. Выберите опцию, чтобы определять топологию как внешнюю, затем нажать

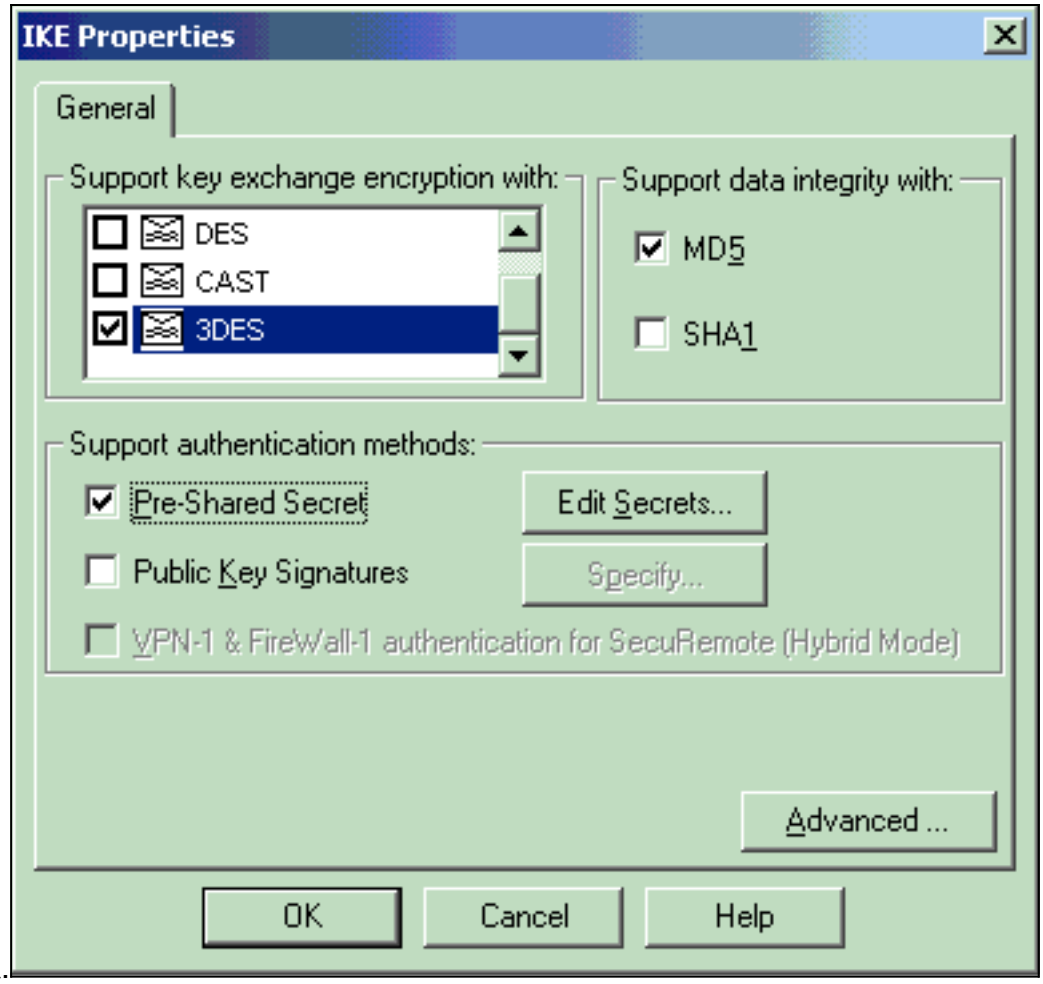


OK.

6. От Окна Workstation Properties на NG CheckpointTM выберите **VPN** от выборов на левой части окна, затем выберите параметры IKE для шифрования и алгоритмы аутентификации. Нажмите **Edit** для настройки Свойств ike.

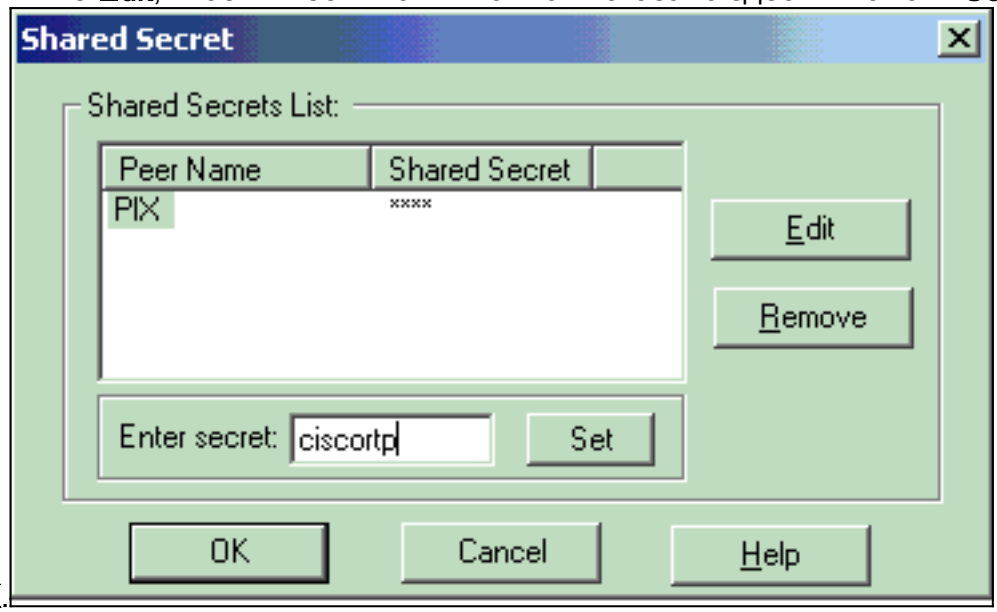


7. Настройте Свойства ike:Выберите опцию для шифрования **3DES** так, чтобы Свойства ike были совместимы с **политикой ISAKMP # шифрование 3des** команда.Выберите опцию для **MD5** так, чтобы Свойства ike были совместимы с **crypto isakmp policy #** команда **md5**



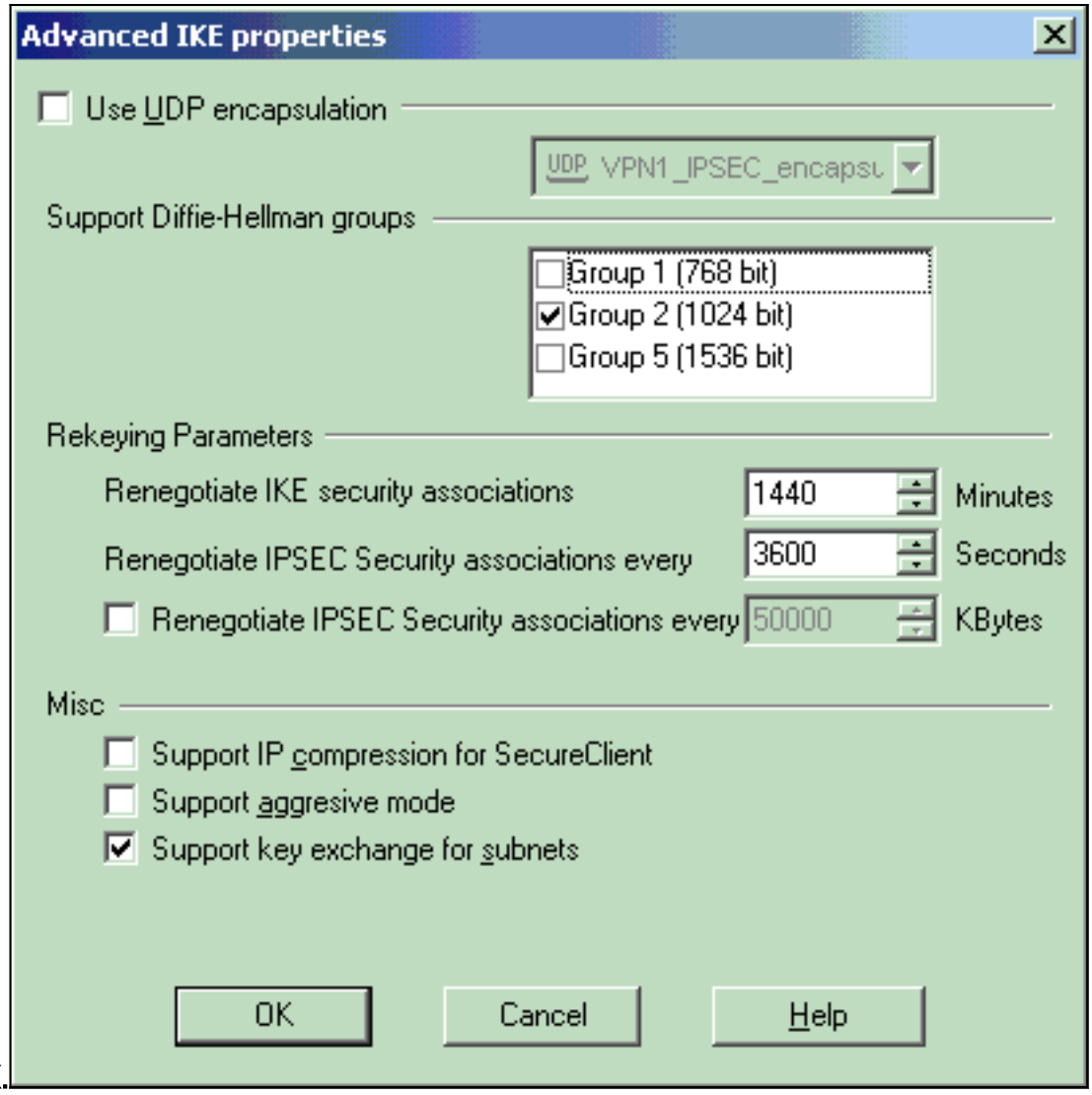
хэша.

8. Выберите параметр проверки подлинности для **Предварительных общих ключей**, затем нажмите **Edit Secrets** для установки предварительного общего ключа как совместимого с *маской подсети* **маски подсети** *адреса основного адреса* **ключа isakmp** команды PIX. Нажмите **Edit**, чтобы ввести ваш ключ как показано здесь и нажать **Set,**



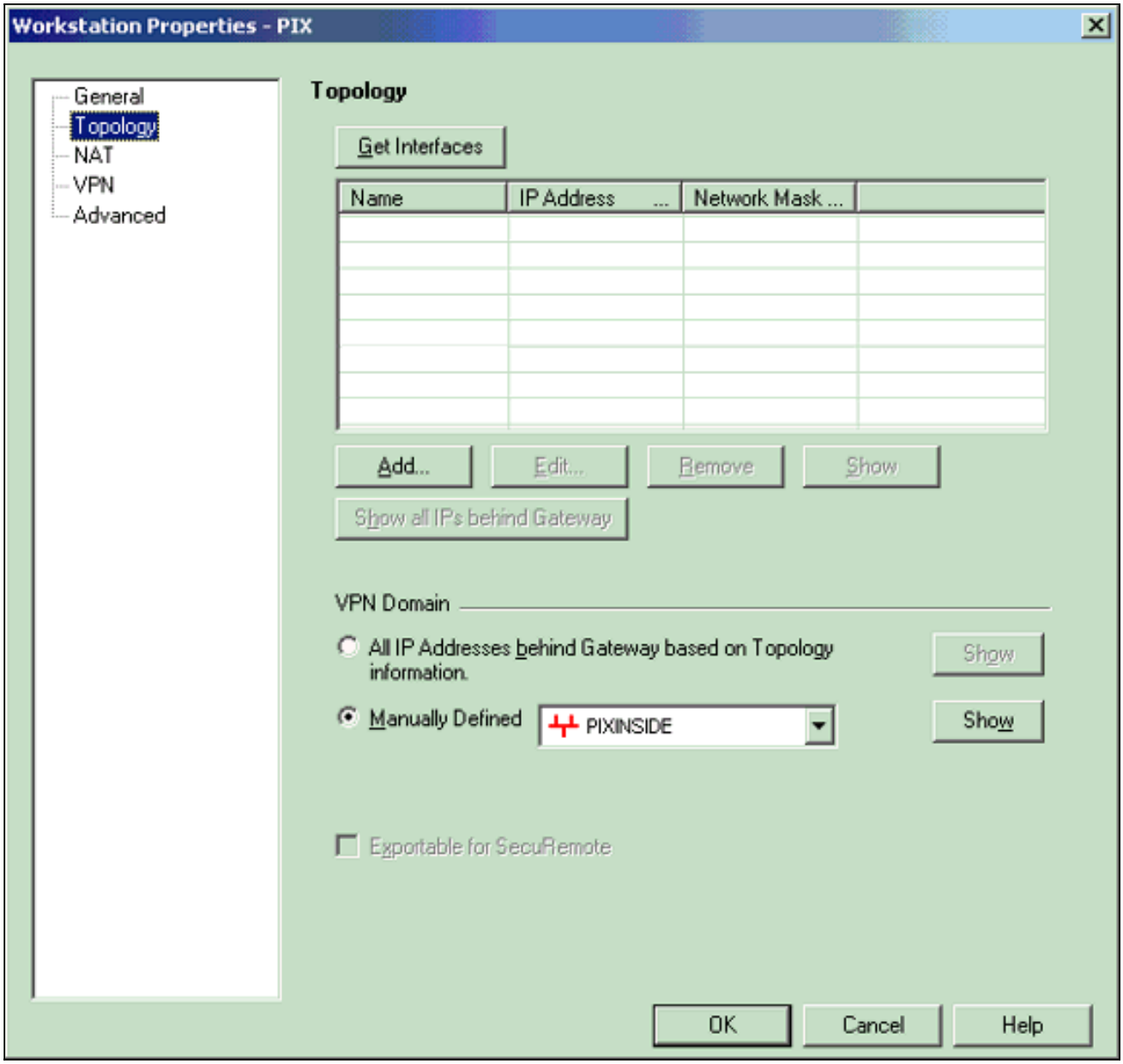
OK.

9. Из окна Свойств ike нажмите **Advanced...** и измените эти настройки:Отмените выбор опции для **Поддержки агрессивного режима**.Выберите опцию для **обмена ключами Поддержки для подсетей**.**Закончив все действия, нажмите кнопку**

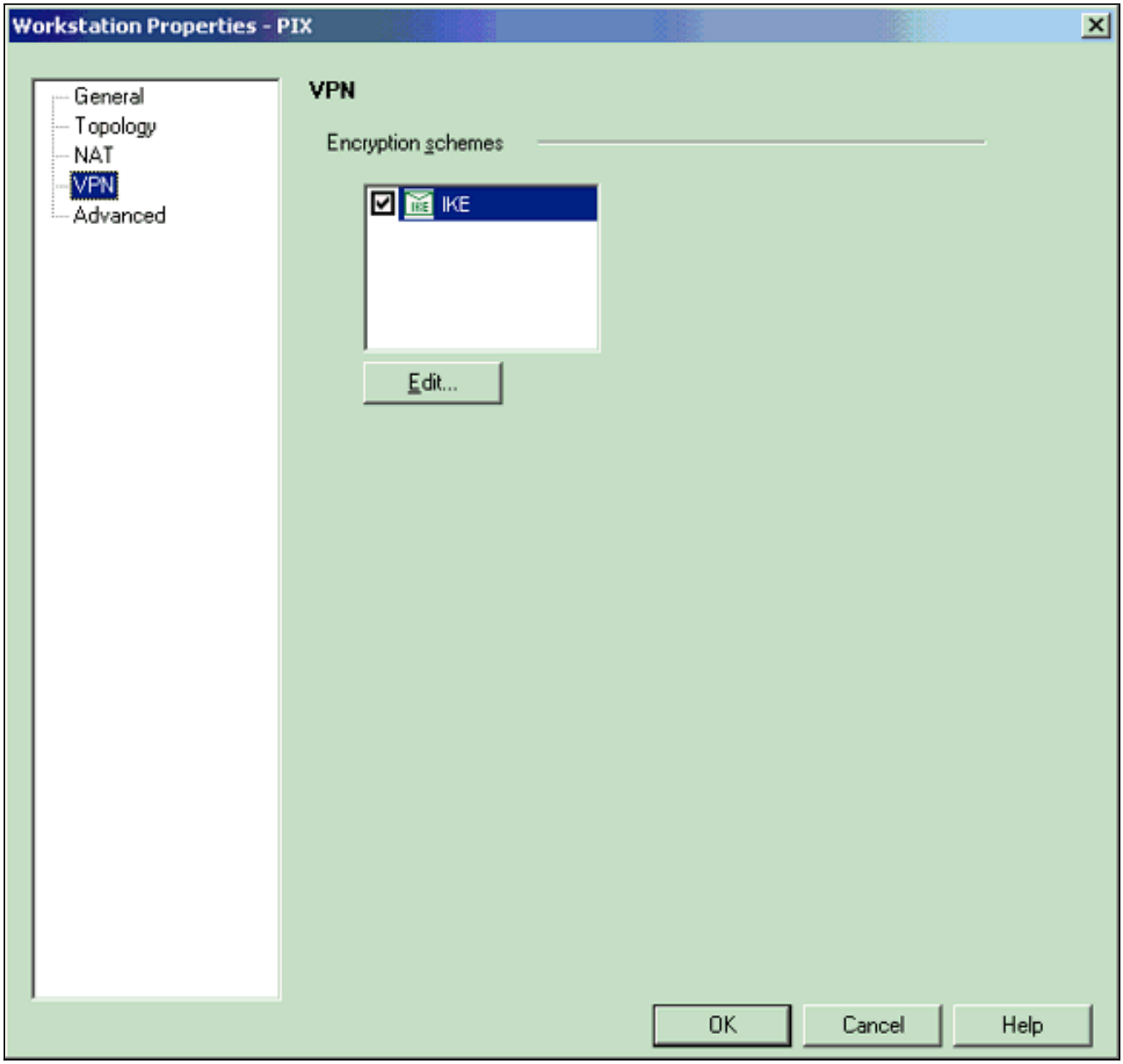


OK.

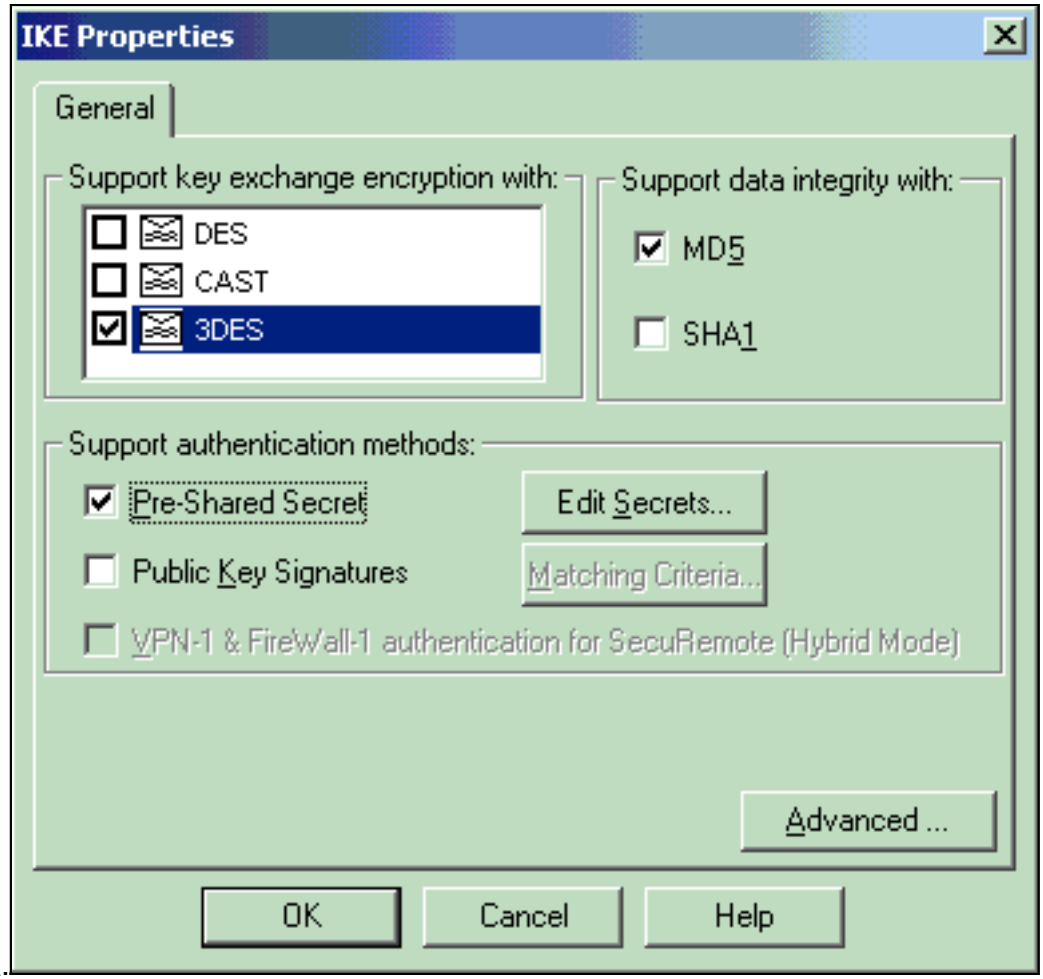
10. Выберите **Manage> Network objects> Edit** для открытия Окна Workstation Properties для PIX. Выберите **Topology** от выборов на левой части окна для ручного определения домена VPN.В этой конфигурации PIXINSIDE (внутренняя сеть PIX) определен как домен
VPN.



11. Выберите **VPN** от выборов на левой части окна, затем выберите IKE как схему шифрования. Нажмите **Edit** для настройки Свойств ike.

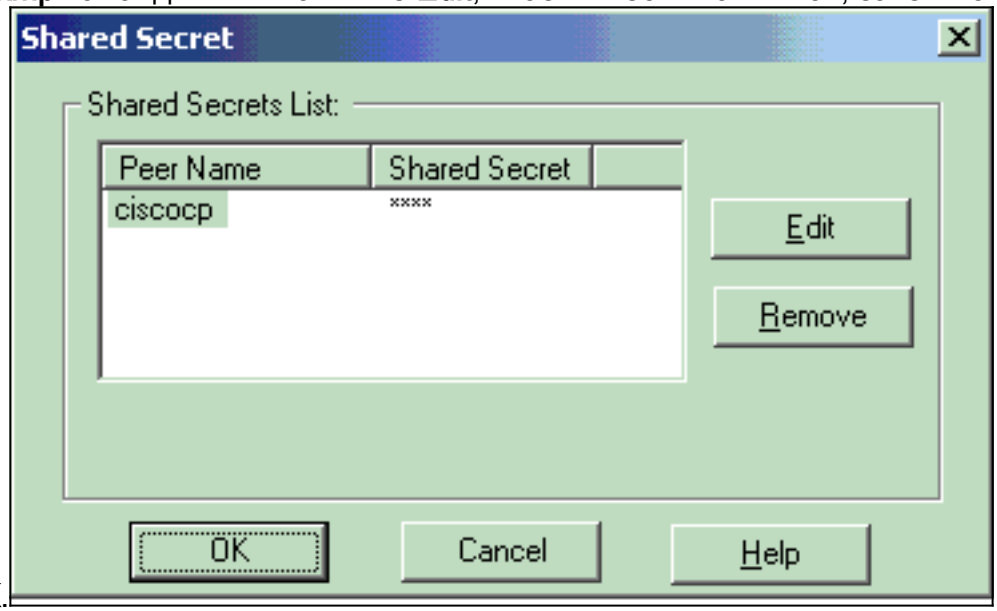


12. Настройте Свойства ike как показано здесь:Выберите опцию для шифрования **3DES** так, чтобы Свойства ike были совместимы с **политикой ISAKMP # шифрование 3des** команда.Выберите опцию для **MD5** так, чтобы Свойства ike были совместимы с **crypto isakmp policy #** команда **md5**



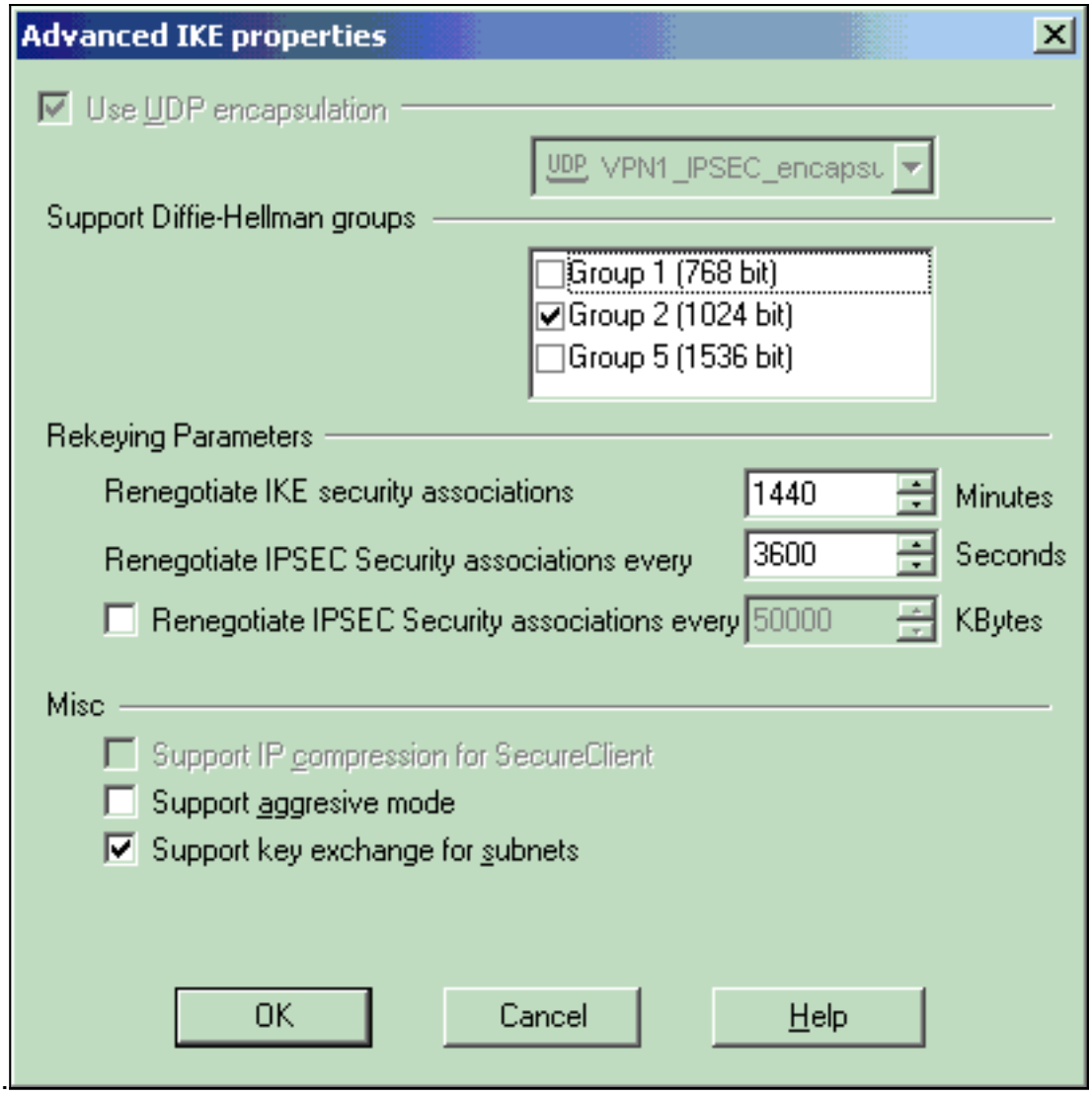
хэша.

13. Выберите параметр проверки подлинности для **Предварительных общих ключей**, затем нажмите **Edit Secrets** для установки предварительного общего ключа как совместимого с *маской подсети* **маски подсети** *адреса основного адреса* **ключа isakmp** команды PIX. Нажмите **Edit**, чтобы ввести ваш ключ, затем нажать **Set,**



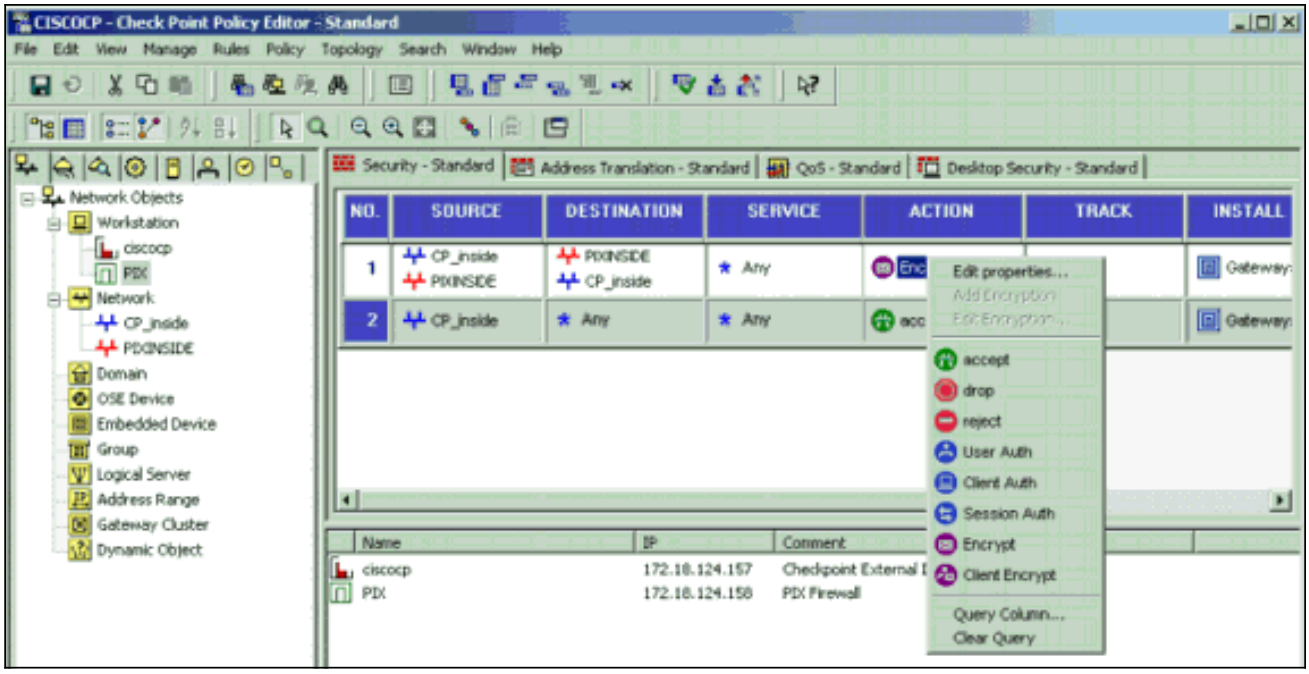
OK.

14. Из окна Свойств ike нажмите **Advanced...** и измените эти настройки.Выберите Группу Диффи-Хеллмана, соответствующую Свойствам ike.Отмените выбор опции для **Поддержки агрессивного режима**.Выберите опцию для **обмена ключами Поддержки для подсетей**.**Нажмите OK, OK**, когда вы будете

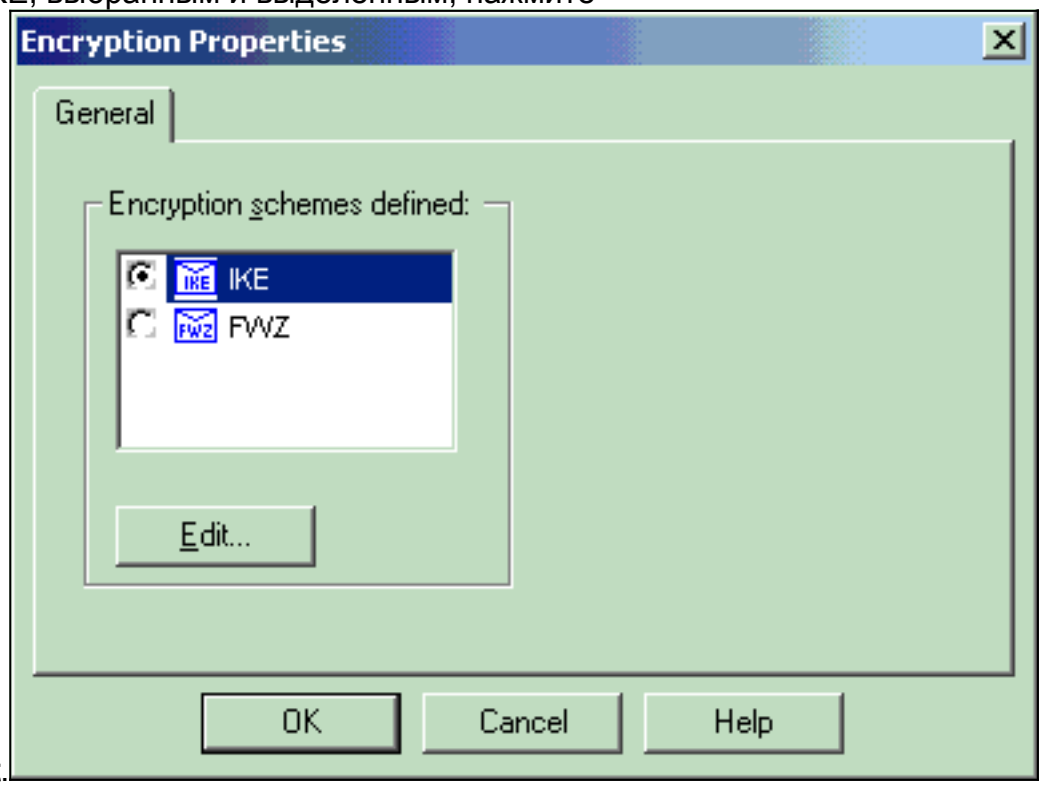


сделаны.

15. Выберите **Rules> Add Rules> Top** для настройки правил шифрования для политики.В Окне редактора политики вставьте правило с источником CP_inside (внутренняя сеть NG ™ Контрольной точки) и PIXINSIDE (внутренняя сеть PIX) и на источнике и на столбцах назначения. Значения набора для **Сервиса = Любой**, **Действие = Шифрует**, и **Дорожка = Журнал**. Когда вы добавили Зашифровать раздел Действия правила, щелкаете правой кнопкой мыши **Действие** и выбираете **Edit Properties**.

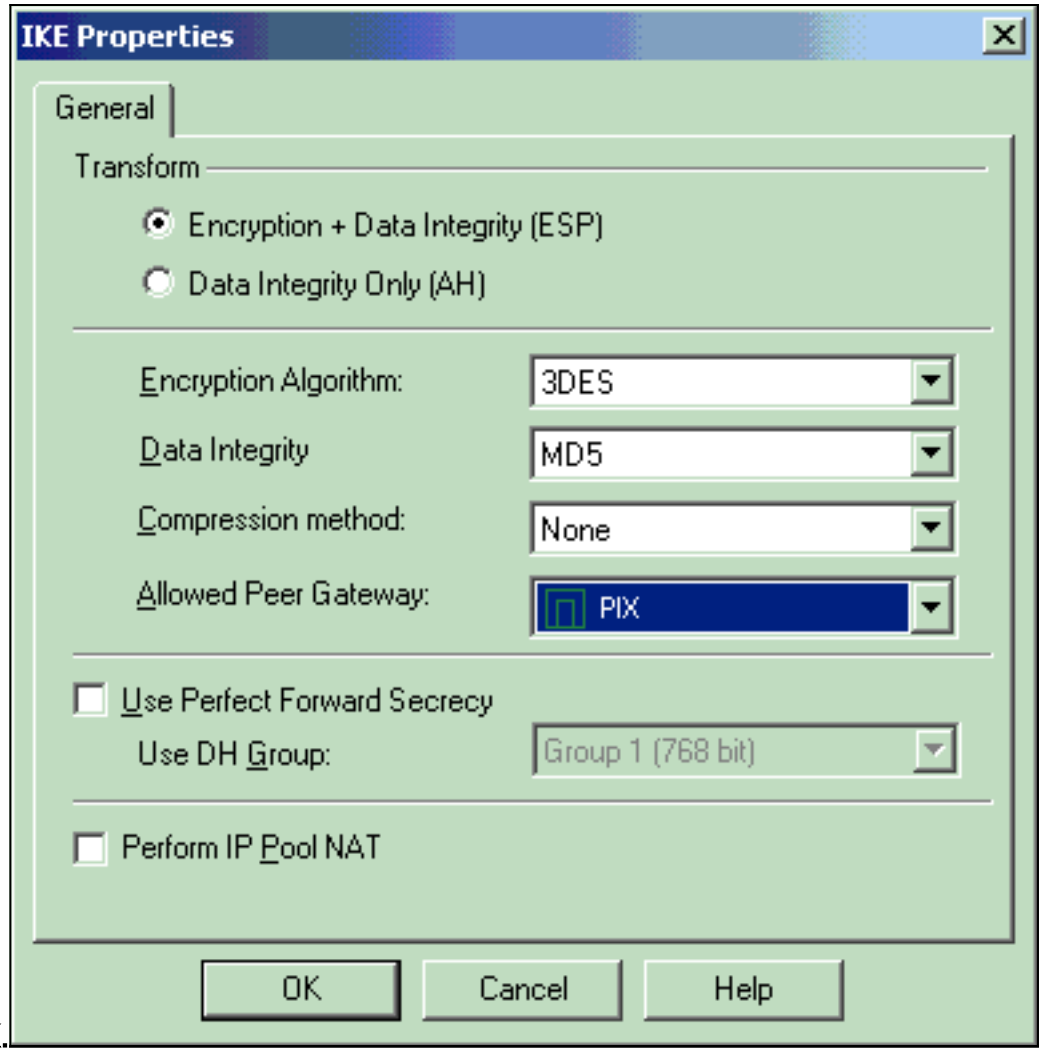


16. С IKE, выбранным и выделенным, нажмите



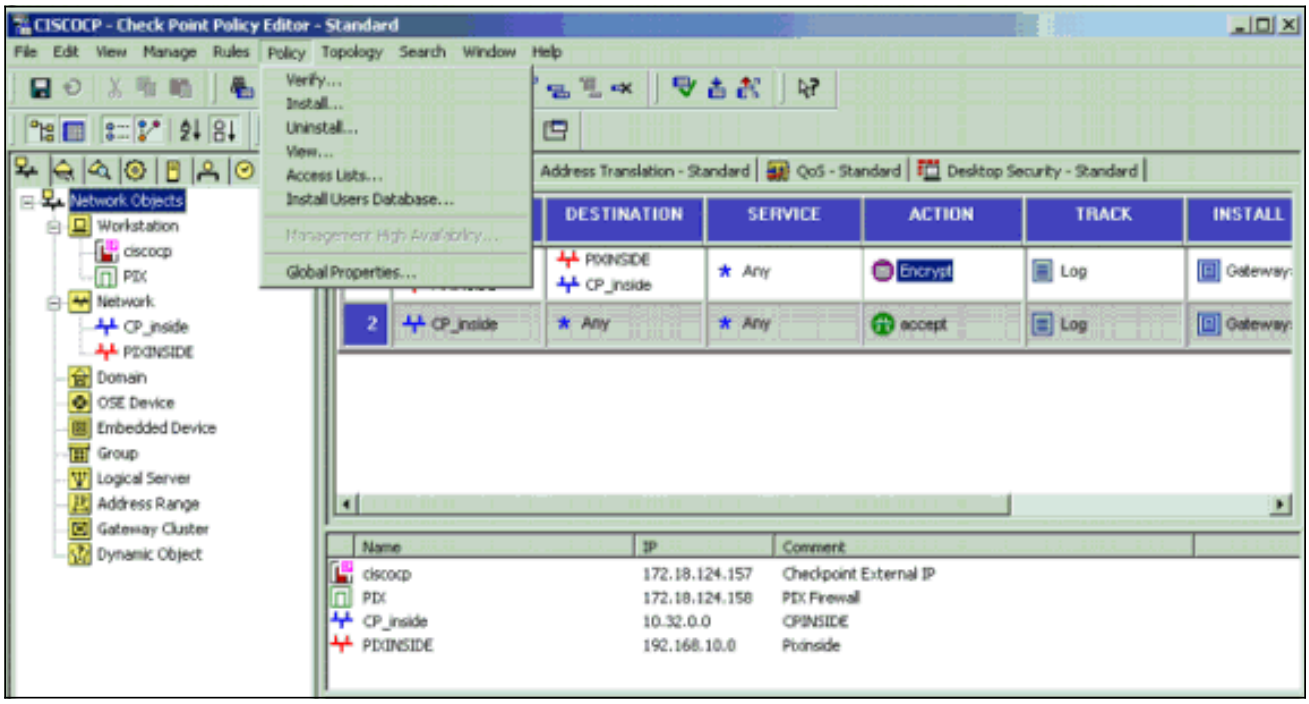
Edit.

17. На окне IKE Properties изменитесь, свойства для согласия с PIX IPSEC преобразовывает в **команду crypto ipsec transform-set rtptac esp-3des esp-md5-hmac**.Установите опцию Transform в **Шифрование + Целостность данных (ESP)**, установите Алгоритм шифрования в **3DES**, установите Целостность данных в **MD5** и заставьте Позволенный Шлюз одноранговой сети совпадать с внешним шлюзом PIX (названный PIX здесь). **Нажмите кнопку**

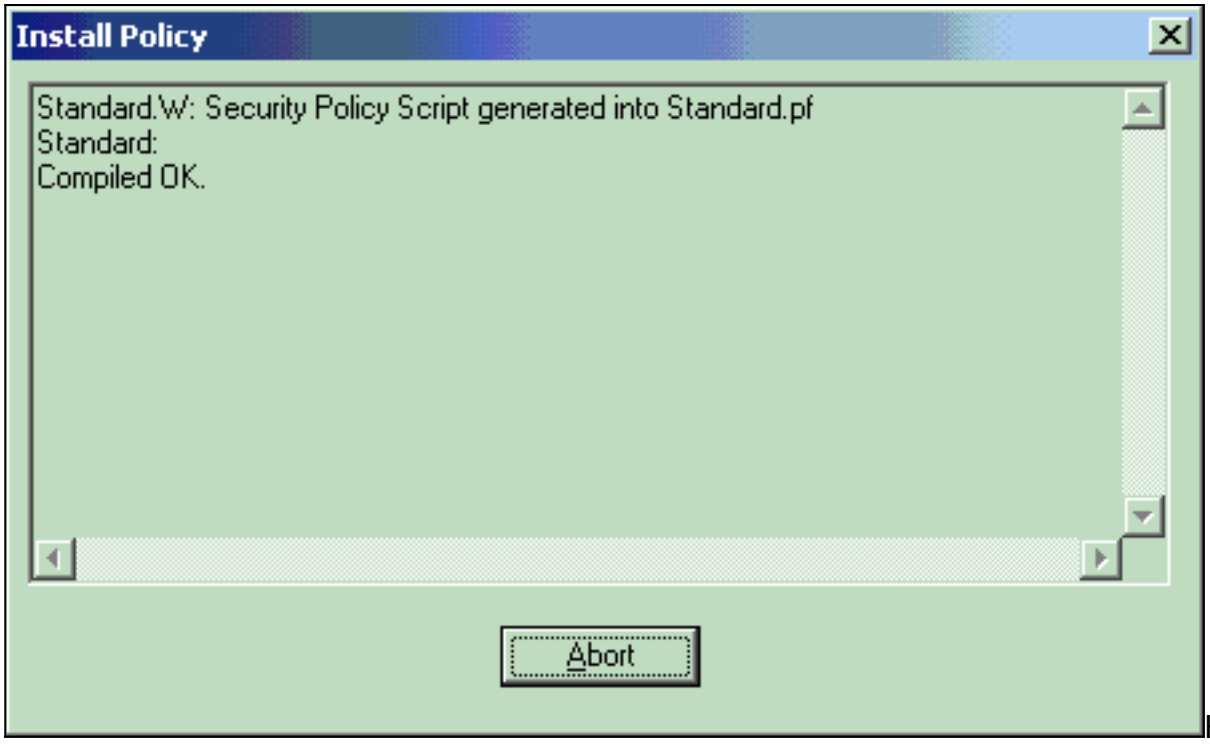


OK.

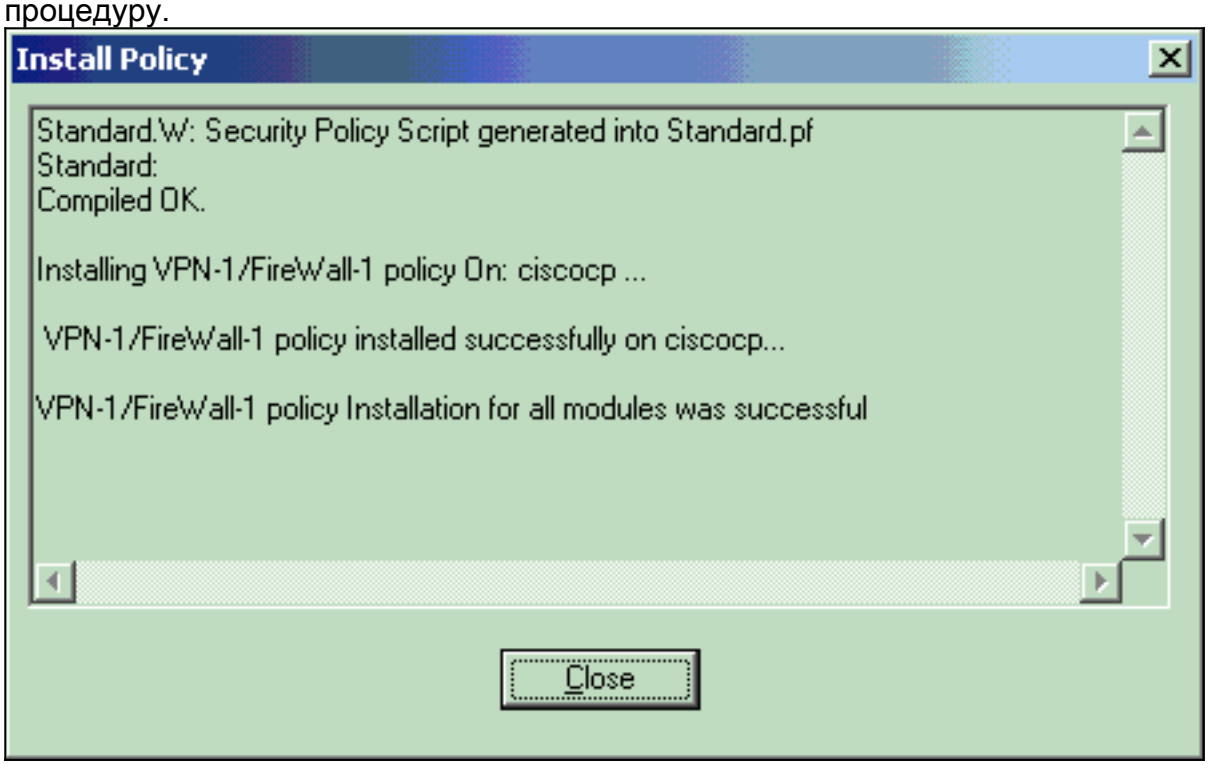
18. После того, как вы настраиваете NG CheckpointTM, сохраняете политику и выбираете **Policy> Install** для включения его.



Замечания о ходе работы показов окна установки как политика скомпилированы.



Когда окно установки указывает, что установка политики завершена. Нажмите **Close to** заканчивают
процедуру.



Проверка

Проверьте конфигурацию PIX

Этот раздел позволяет убедиться, что конфигурация работает правильно.

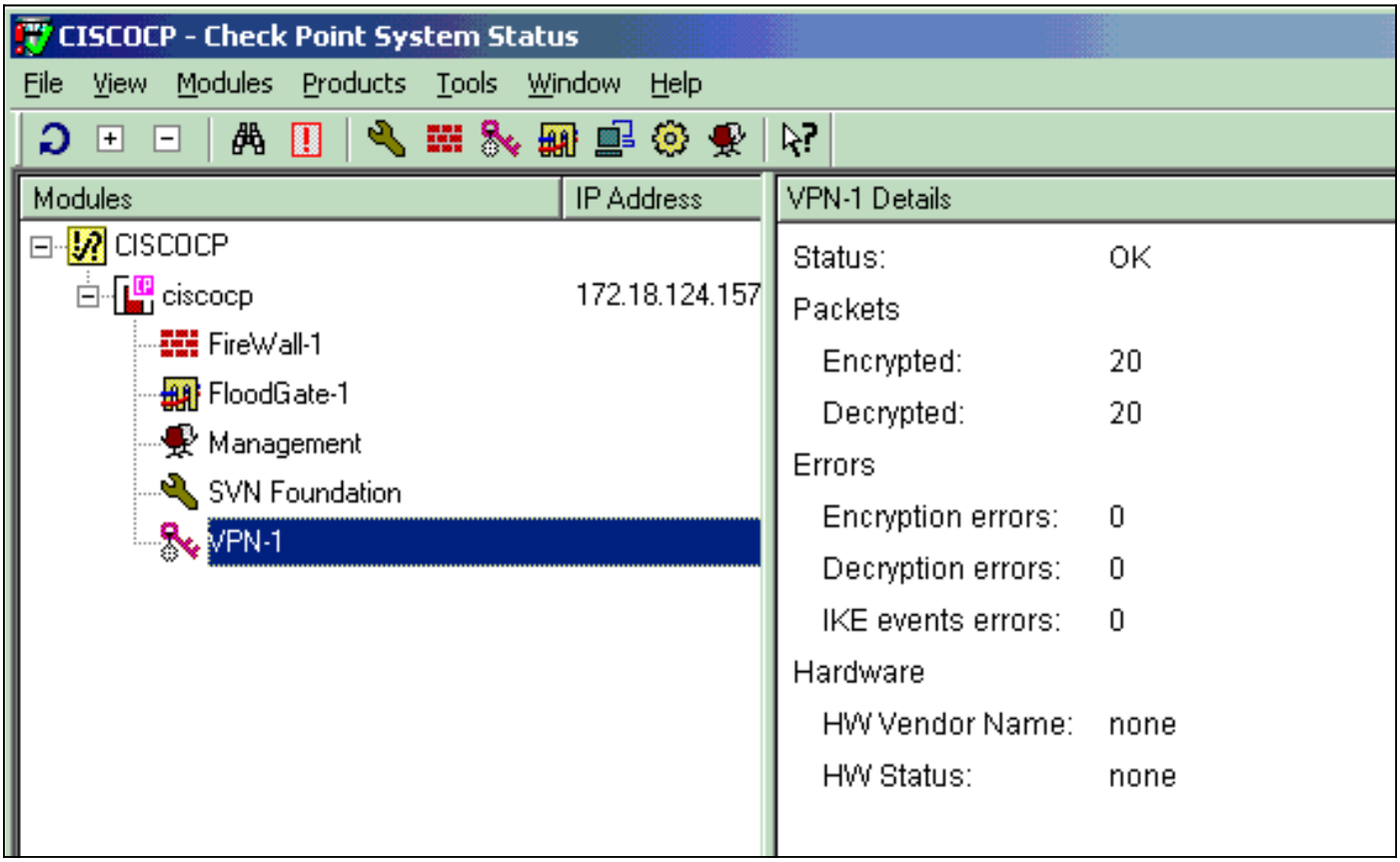
Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Инициируйте эхо-запрос от одной из частных сетей к другой частной сети для тестирования связи между этими двумя частными сетями. В этой конфигурации эхо-запрос передавался со стороны PIX (192.168.10.2) к внутренней сети NG CheckpointTM (10.32.50.51).

- **show crypto isakmp sa — отображает все текущие IKE SA на одноранговом узле.**`show crypto isakmp saTotal : 1Embryonic : 0 dst src state pending created 172.18.124.157 172.18.124.158 QM_IDLE 0 1`
- **show crypto ipsec sa — отображает настройки, используемые текущими SA.**`PIX501A#show cry ipsec sainterface: outside Crypto map tag: rtprules, local addr. 172.18.124.158 local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0) current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19 #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 1, #recv errors 0 local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157 path mtu 1500, ipsec overhead 56, media mtu 1500 current outbound spi: 6b15a355 inbound esp sas: spi: 0xced238c7(3469883591) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map: rtprules sa timing: remaining key lifetime (k/sec): (4607998/27019) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x6b15a355(1796580181) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 4, crypto map: rtprules sa timing: remaining key lifetime (k/sec): (4607998/27019) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:`

Обзорный статус туннеля на контрольной точке NG

Перейдите к Редактору политики и выберите **Window> System Status** для просмотра статуса туннеля.



Устранение неполадок

Устраните неполадки конфигурации PIX

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

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

Используйте эти команды для включения отладок на Межсетевом экране PIX.

- **debug crypto engine?** Отображает сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.
- **debug crypto isakmp – отображает сообщения о событиях IKE.**

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1VPN Peer: ISAKMP: Peer
ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1ISAKMP (0): beginning Main Mode
exchangecrypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158OAK_MM
exchangeISAKMP (0): processing SA payload. message ID = 0ISAKMP (0): Checking ISAKMP transform 1
against priority 1 policyISAKMP: encryption 3DES-CBCISAKMP: hash MD5ISAKMP: default group
2ISAKMP: auth pre-shareISAKMP: life type in secondsISAKMP: life duration (VPI) of 0x0 0x1 0x51
0x80ISAKMP (0): atts are acceptable. Next payload is 0ISAKMP (0): SA is doing pre-shared key
authentication using id type ID_IPV4_ADDRreturn status is
IKMP_NO_ERRORcrypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158OAK_MM
exchangeISAKMP (0): processing KE payload. message ID = 0ISAKMP (0): processing NONCE payload.
message ID = 0ISAKMP (0): ID payloadnext-payload : 8type : 1protocol : 17port : 500length :
8ISAKMP (0): Total payload length: 12return status is IKMP_NO_ERRORcrypto_isakmp_process_block:
src 172.18.124.157, dest 172.18.124.158OAK_MM exchangeISAKMP (0): processing ID payload. message
ID = 0ISAKMP (0): processing HASH payload. message ID = 0ISAKMP (0): SA has been
authenticatedISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4
IPSEC(key_engine): got a queue event...IPSEC(spi_response): getting spi 0xced238c7(3469883591)
for SAfrom 172.18.124.157 to 172.18.124.158 for prot 3return status is IKMP_NO_ERRORISAKMP (0):
sending INITIAL_CONTACT notifyISAKMP (0): sending NOTIFY message 24578 protocol 1ISAKMP (0):
sending INITIAL_CONTACT notifycrypto_isakmp_process_block: src 172.18.124.157, dest
172.18.124.158OAK_QM exchangeoakley_process_quick_mode:OAK_QM_IDLEISAKMP (0): processing SA
payload. message ID = 322868148ISAKMP : Checking IPSec proposal 1ISAKMP: transform 1,
ESP_3DESISAKMP: attributes in transform:ISAKMP: encaps is 1ISAKMP: SA life type in
secondsISAKMP: SA life duration (basic) of 28800ISAKMP: SA life type in kilobytesISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0ISAKMP: authenticator is HMAC-MD5ISAKMP (0): atts are
acceptable. IPSEC(validate_proposal_request): proposal part #1,(key eng. msg.) dest=
172.18.124.157, src= 172.18.124.158,dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),src_proxy=
192.168.10.0/255.255.255.0/0/0 (type=4),protocol= ESP, transform= esp-3des esp-md5-hmac
,lifedur= 0s and 0kb,spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4ISAKMP (0): processing NONCE
payload. message ID = 322868148ISAKMP (0): processing ID payload. message ID = 322868148ISAKMP
(0): processing ID payload. message ID = 322868148ISAKMP (0): processing NOTIFY payload 24576
protocol 3spi 3469883591, message ID = 322868148ISAKMP (0): processing responder lifetimeISAKMP
(0): processing NOTIFY payload 24576 protocol 3spi 3469883591, message ID = 322868148ISAKMP (0):
processing responder lifetimeISAKMP (0): Creating IPSec SAsinbound SA from 172.18.124.157 to
172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)has spi 3469883591 and conn_id 3 and flags
4lifetime of 28800 secondslifetime of 4608000 kilobytesoutbound SA from 172.18.124.158 to
172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)has spi 1796580181 and conn_id 4 and flags
4lifetime of 28800 secondslifetime of 4608000 kilobytesIPSEC(key_engine): got a queue
event...IPSEC(initialize_sas): ,(key eng. msg.) dest= 172.18.124.158, src=
172.18.124.157,dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),src_proxy=
10.32.0.0/255.255.128.0/0/0 (type=4),protocol= ESP, transform= esp-3des esp-md5-hmac ,lifedur=
28800s and 4608000kb,spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags=
0x4IPSEC(initialize_sas): ,(key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157,src_proxy=
192.168.10.0/255.255.255.0/0/0 (type=4),dest_proxy= 10.32.0.0/255.255.128.0/0/0
(type=4),protocol= ESP, transform= esp-3des esp-md5-hmac ,lifedur= 28800s and 4608000kb,spi=
0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4VPN Peer: IPSEC: Peer
```

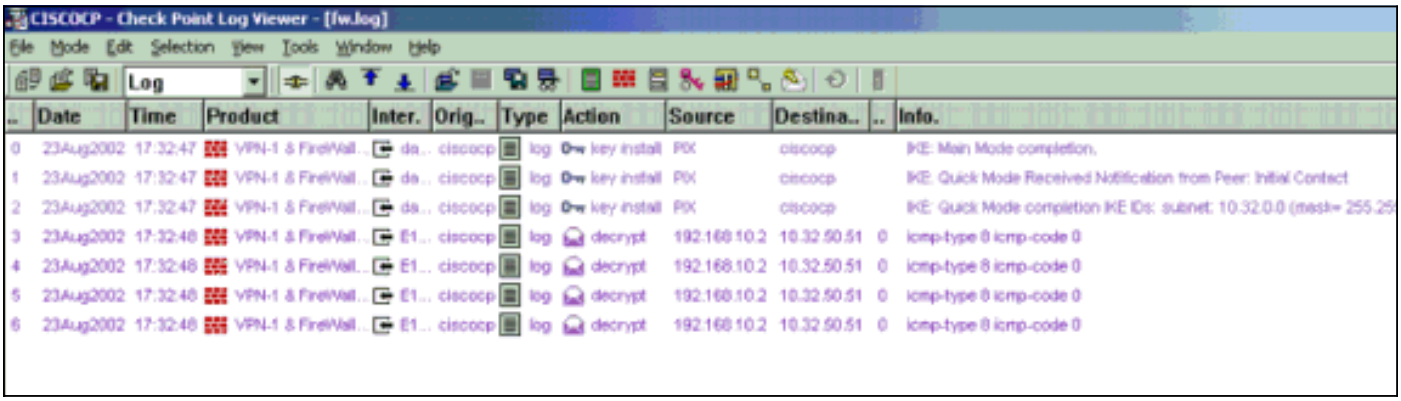
```
ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1VPN Peer: IPSEC: Peer
ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1return status is IKMP_NO_ERROR
```

Суммирование сетей

При настройке нескольких смежных внутренних сетей в домене шифрования на устройстве Checkpoint последнее может автоматически суммировать сети с точки зрения трафика, представляющего интерес. Если крипто-список контроля доступа (ACL) на PIX не будет настроен для соответствия, то туннель, вероятно, откажет. Например, если внутренние сети 10.0.0.0 / 24 и 10.0.1.0 / 24 настроены, чтобы быть включенными в туннель, они могут быть суммированы к 10.0.0.0 / 23.

Обзорные журналы контрольной точки NG

Выберите **Window> Log Viewer** для просмотра журналов.



Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация