# Настройка Туннеля IPSec - от Cisco Secure PIX Firewall к брандмауэру Checkpoint Firewall 4.1

## Содержание



## Введение

Эта выборка configration демонстрирует, как сформировать Туннель IPSec с предварительными общими ключами для присоединения к двум частным сетям. В данном примере сети, для которых выполняется присоединение, — это частная сеть 192.168.1.X в пределах межсетевого экрана Cisco Secure Pix Firewall (PIX) и частная сеть 10.32.50.X в пределах межсетевого экрана Checkpoint. Предполагается что трафик из PIX и в Контрольной точке 4.1 Межсетевых экрана к Интернету (представленный здесь 172.18.124. X сетей), течет до начала этой конфигурации.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

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

- Программное обеспечение PIX версии 5.3.1
- Межсетевой экран Checkpoint 4.1

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.

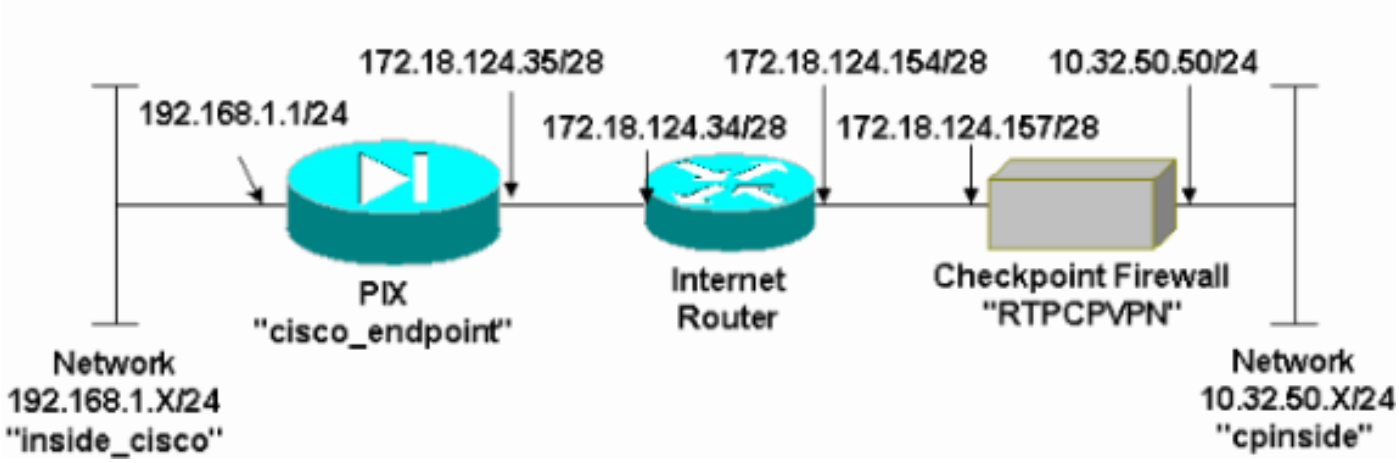
## Настройка

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

**Примечание:** Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

### Схема сети

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




### Конфигурации

Этот документ использует конфигурации, показанные в этом разделе.

**Конфигурация PIX**

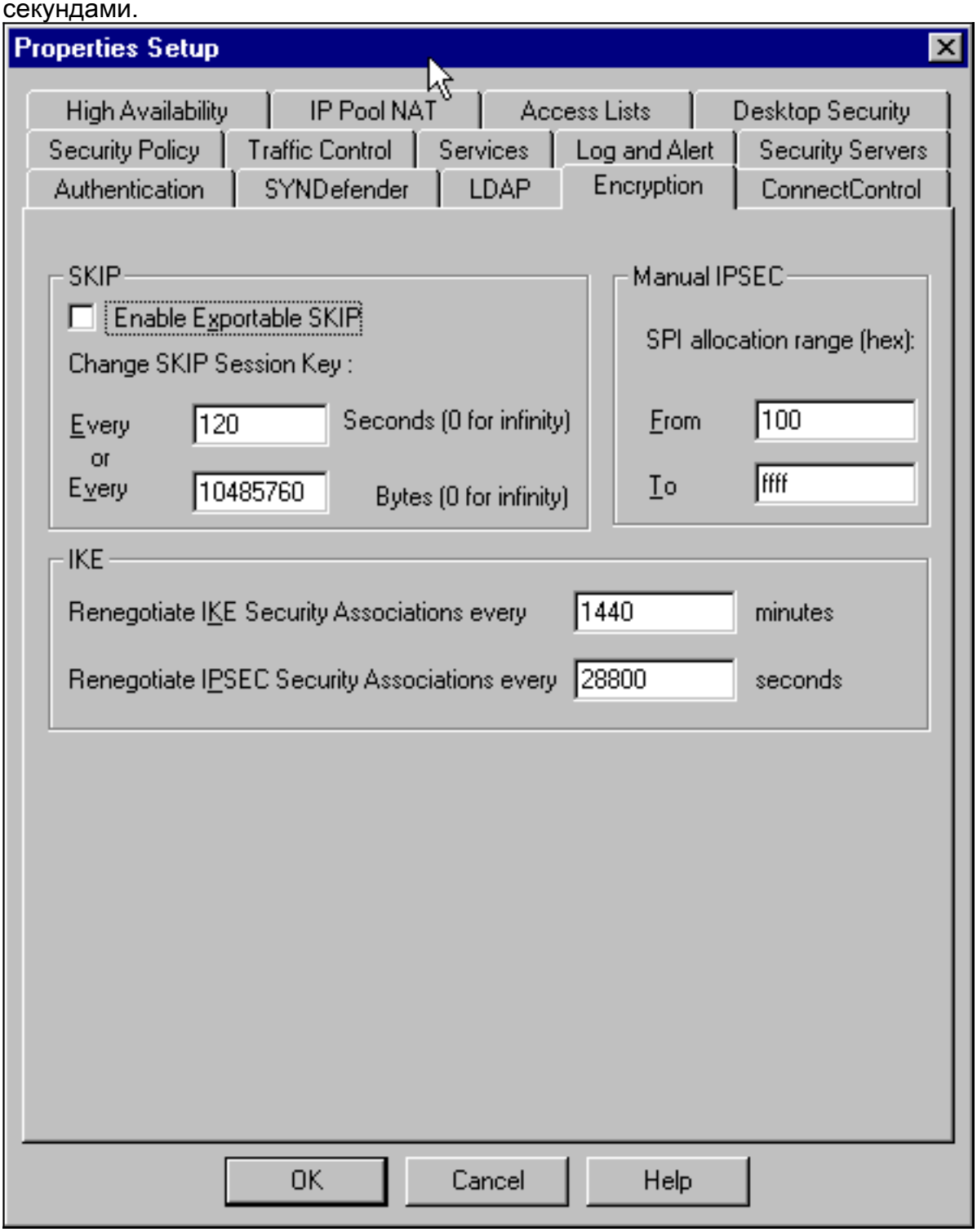
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
```

```
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0 access-list 115 deny ip
192.168.1.0 255.255.255.0 any pager lines 24 logging on
no logging timestamp no logging standby no logging
console logging monitor debugging no logging buffered
logging trap debugging no logging history logging
facility 20 logging queue 512 interface ethernet0 auto
interface ethernet1 auto mtu outside 1500 mtu inside
1500 ip address outside 172.18.124.35 255.255.255.240 ip
address inside 192.168.1.1 255.255.255.0 ip audit info
action alarm ip audit attack action alarm no failover
failover timeout 0:00:00 failover poll 15 failover ip
address outside 0.0.0.0 failover ip address inside
0.0.0.0 arp timeout 14400 global (outside) 1
172.18.124.36 nat (inside) 0 access-list 115 nat
(inside) 1 0.0.0.0 0.0.0.0 0 0 route outside 0.0.0.0
0.0.0.0 172.18.124.34 1 timeout xlate 3:00:00g SA
0x80bd6a10, conn_id = 0 timeout 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 0:02:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius no snmp-server location no snmp-server
contact snmp-server community public no snmp-server
enable traps floodguard enable !--- IPSec configuration
sysopt connection permit-ipsec no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp crypto map rtpmap 10
match address 115 crypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
myset crypto map rtpmap 10 set security-association
lifetime seconds 3600 kilobytes 4608000 crypto map
rtpmap interface outside !--- IKE configuration isakmp
enable outside isakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address isakmp policy 10 authentication pre-share isakmp
policy 10 encryption des isakmp policy 10 hash sha
isakmp policy 10 group 1 isakmp policy 10 lifetime 86400
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79 : end
[OK]
```

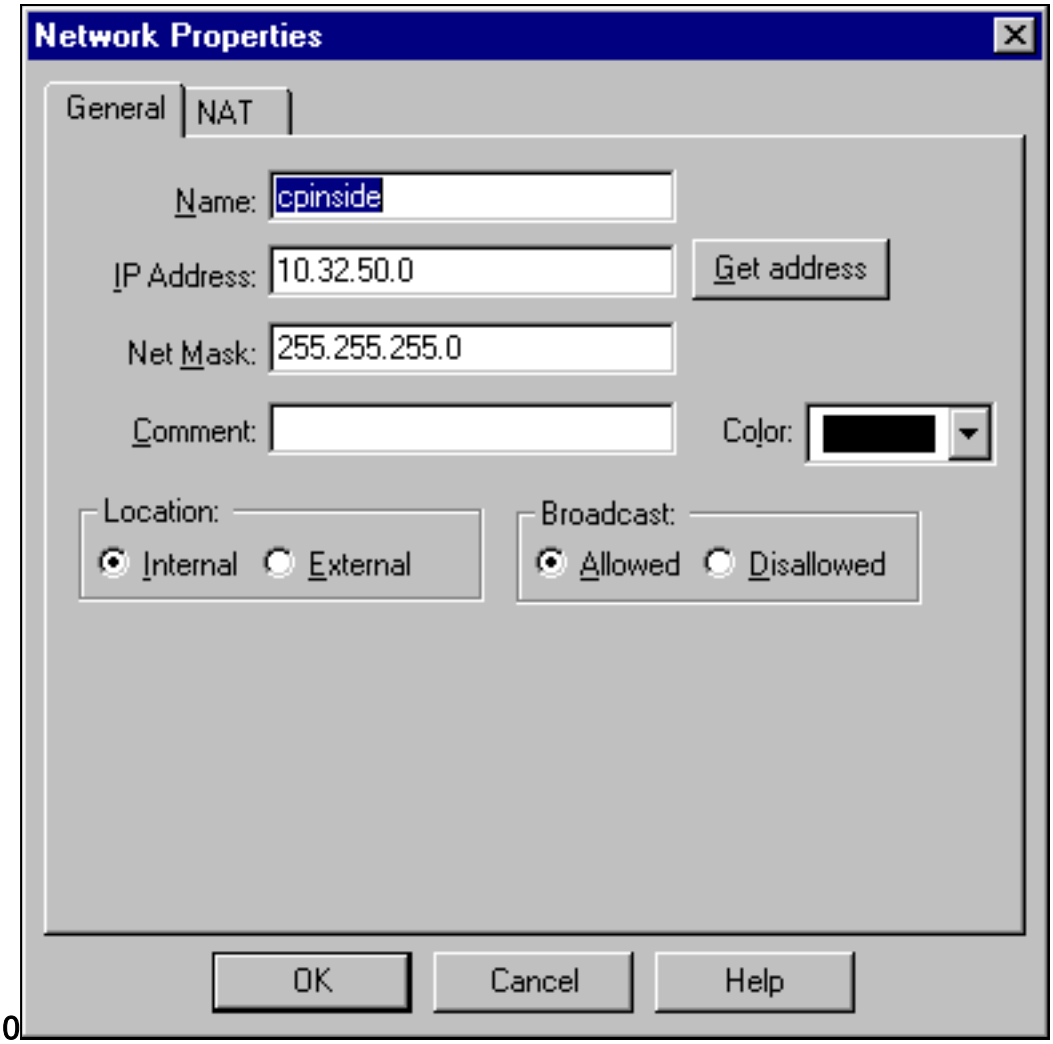
## Брандмауэр Checkpoint

1. **Так как у производителей отличаются установленные по умолчанию времена жизни для IKE и IPSec, щелкните Properties > Encryption, чтобы установить время жизни контрольной точки, соответствующей значениям по умолчанию PIX.**Время жизни IKE по умолчанию в PIX составляет 86400 секунд (=1440 минут), модифицируемый этой командой: **isakmp policy # lifetime 86400**Срок действия IKE PIX может быть настроен между 60-86400 секундами.Срок действия IPSec Pix по умолчанию составляет 28800 секунд, модифицируемых этой командой: **rypto ipsec security-время продолжительности связи в секундах #**Можно настроить срок действия PIX IPSEC между 120-86400

секундами.

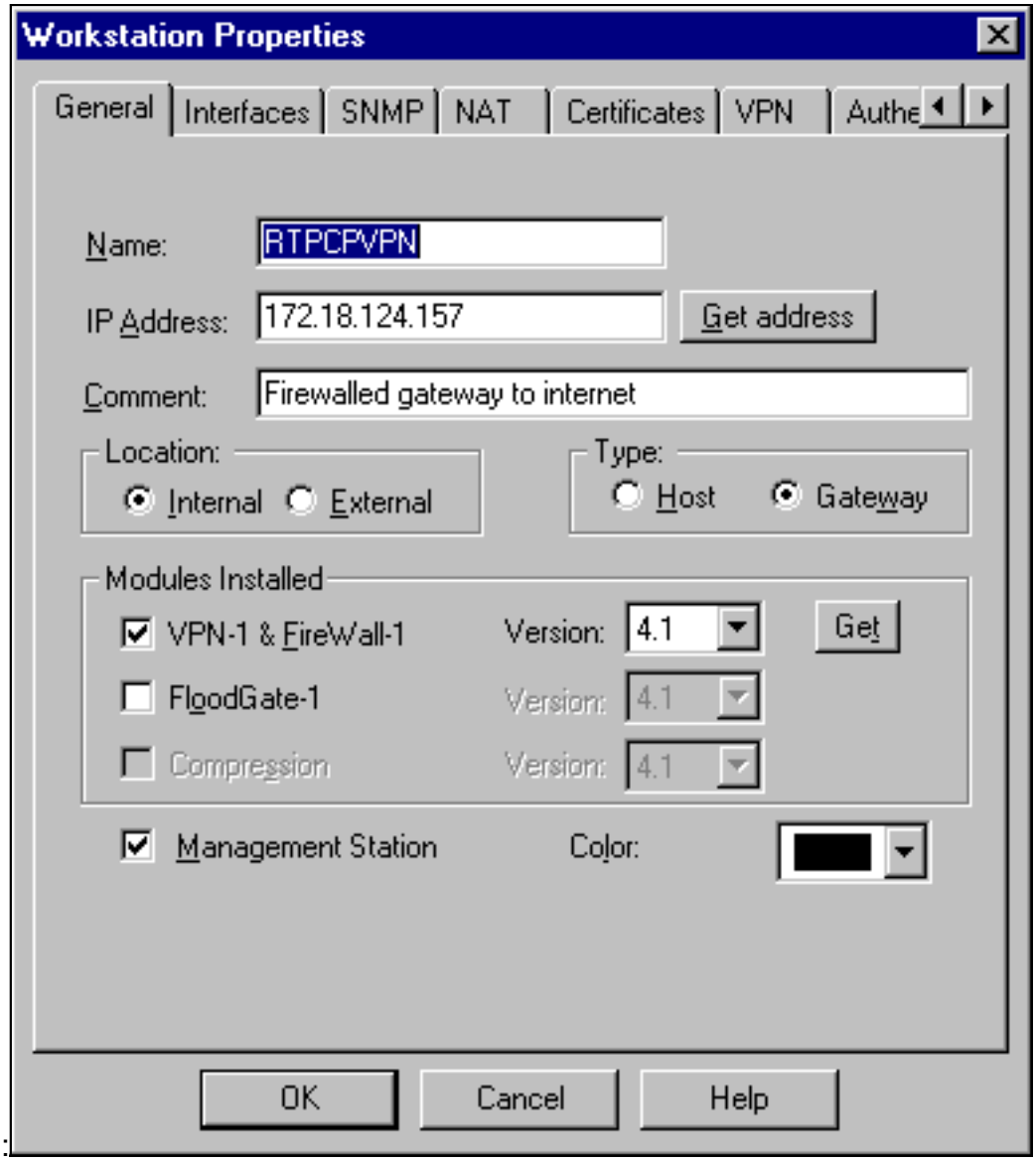



2. **Для настройки объекта внутренней (cpinside) сети за устройством Checkpoint выберите Manage > Network objects > New (или Edit) > Network (Управление > Объекты сетей > Создать (Изменить) > Сеть).**Это должно согласиться с сетью назначения (дополнительная) в этой команде PIX: **список доступа 115 разрешает ip 192.168.1.0 255.255.255.0 10.32.50.0**



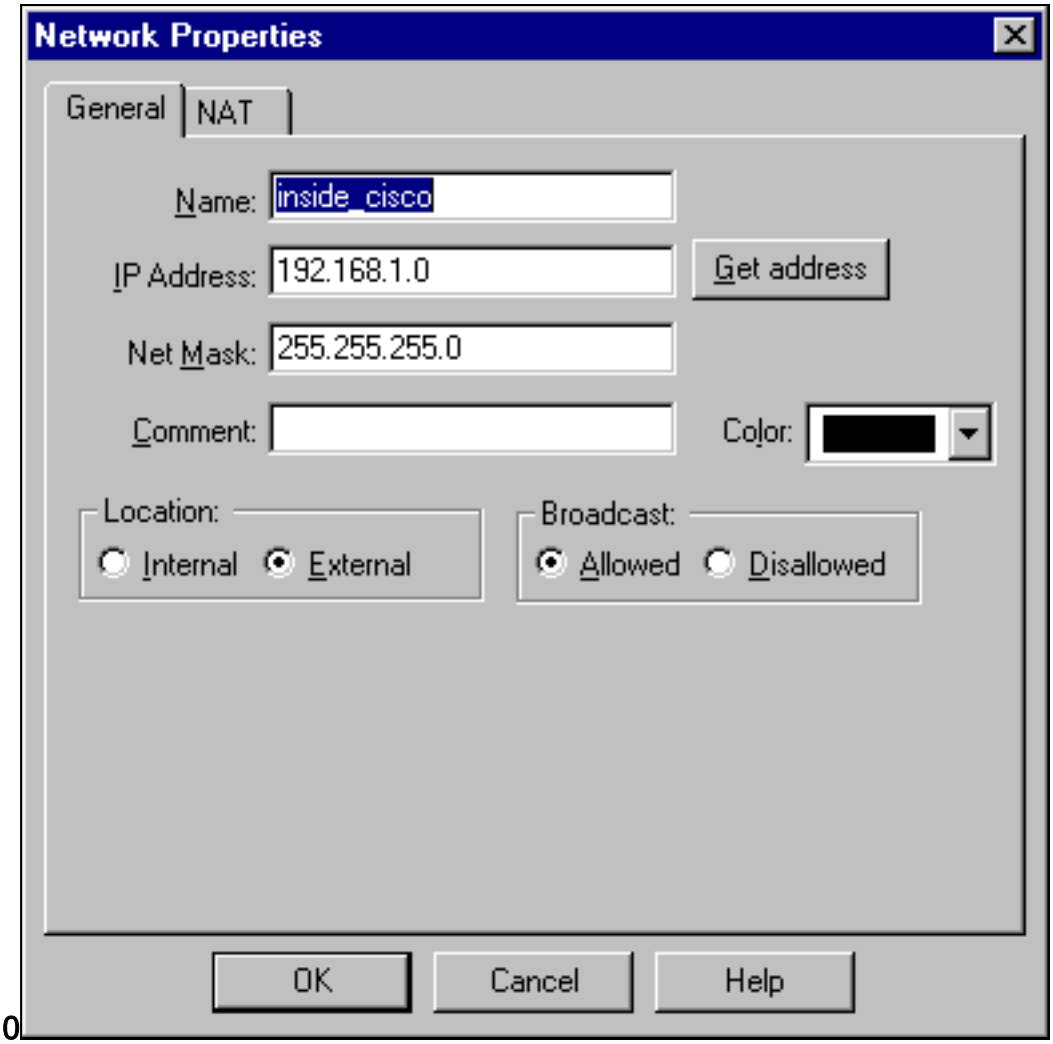

**255.255.255.0**

3. Выберите **Manage> Network objects> Edit** для редактирования объекта для шлюза (Контрольная точка "RTPCPVPN") оконечная точка, к которой указывает PIX в этой команде: **crypto map name # set peer ip-адресB поле Location (Местоположение) выберите Internal (Внутри). В поле Type (Тип) выберите Gateway (Шлюз).** Под Установленными Модулями установите флажок **VPN-1 & FireWall 1**, и также установите флажок **Management**



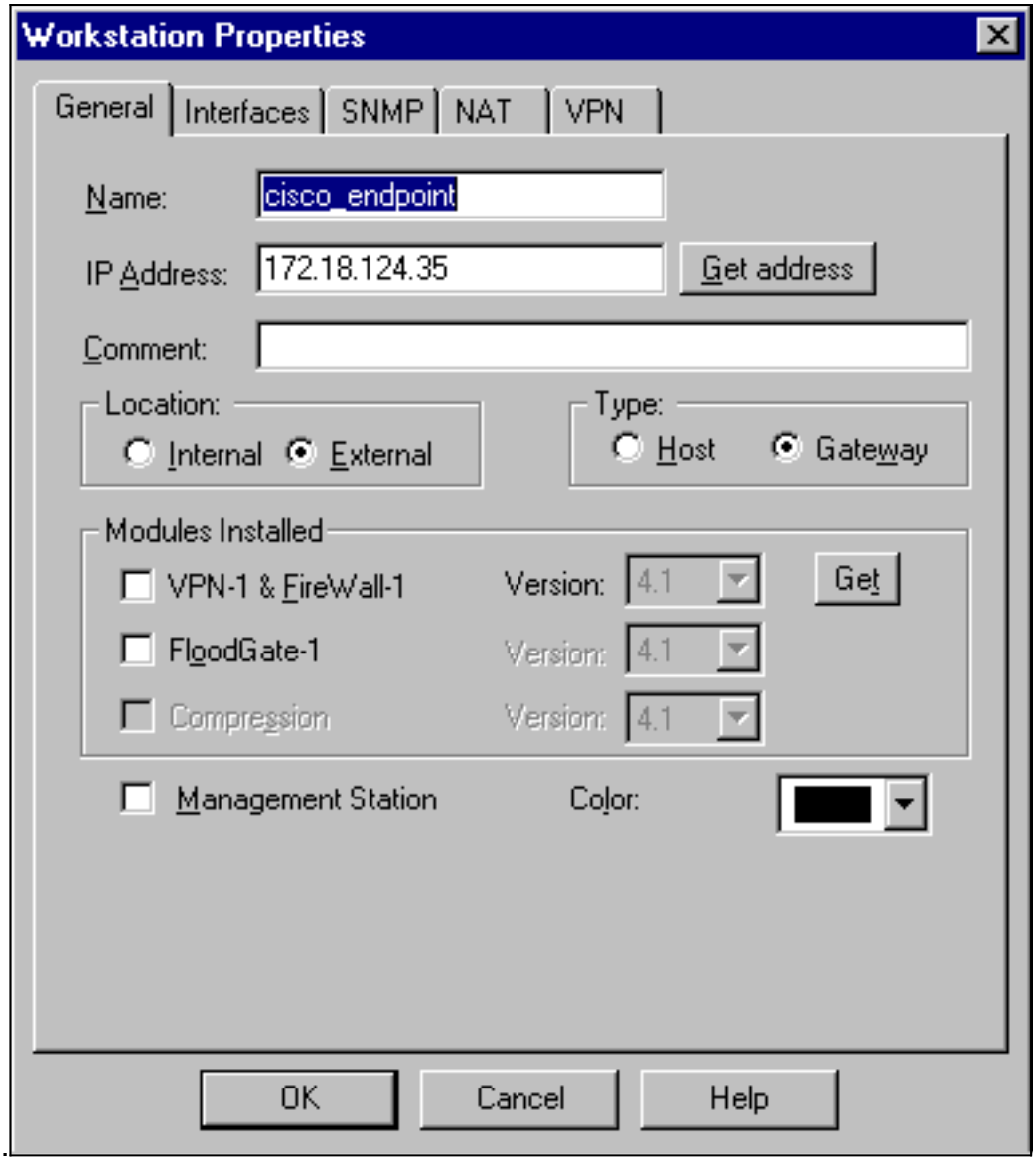

**Station**:

4. Выберите **Manage> Network objects> New> Network** для настройки объекта для внешнего ("inside_cisco") сеть позади PIX.Это должно согласовать с источником (первую) сеть в этой команде PIX: **список доступа 115 разрешает ip 192.168.1.0 255.255.255.0 10.32.50.0**



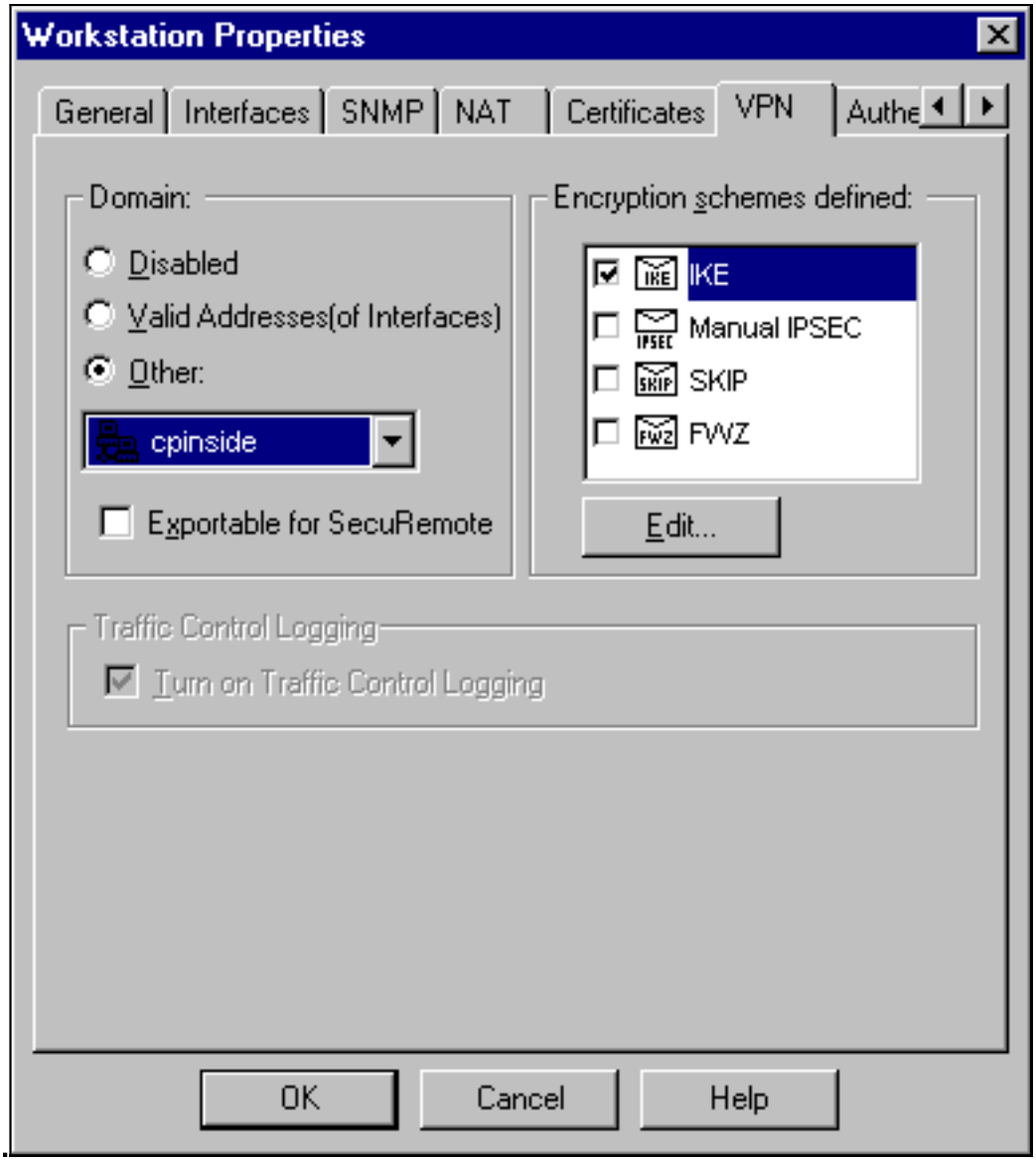

**255.255.255.0**

5. **Чтобы добавить объект для внешнего шлюза PIX ("cisco_endpoint"), выберите Manage > Network objects > New > Workstation.** Это - интерфейс PIX, к которому применена эта команда: **интерфейс** *имени криптокарты* **снаружиВ разделе Location (Местоположение) выберите External (Снаружи). В поле Type (Тип) выберите Gateway (Шлюз).Примечание:** Не выбирать флажок "VPN-1/FireWall-



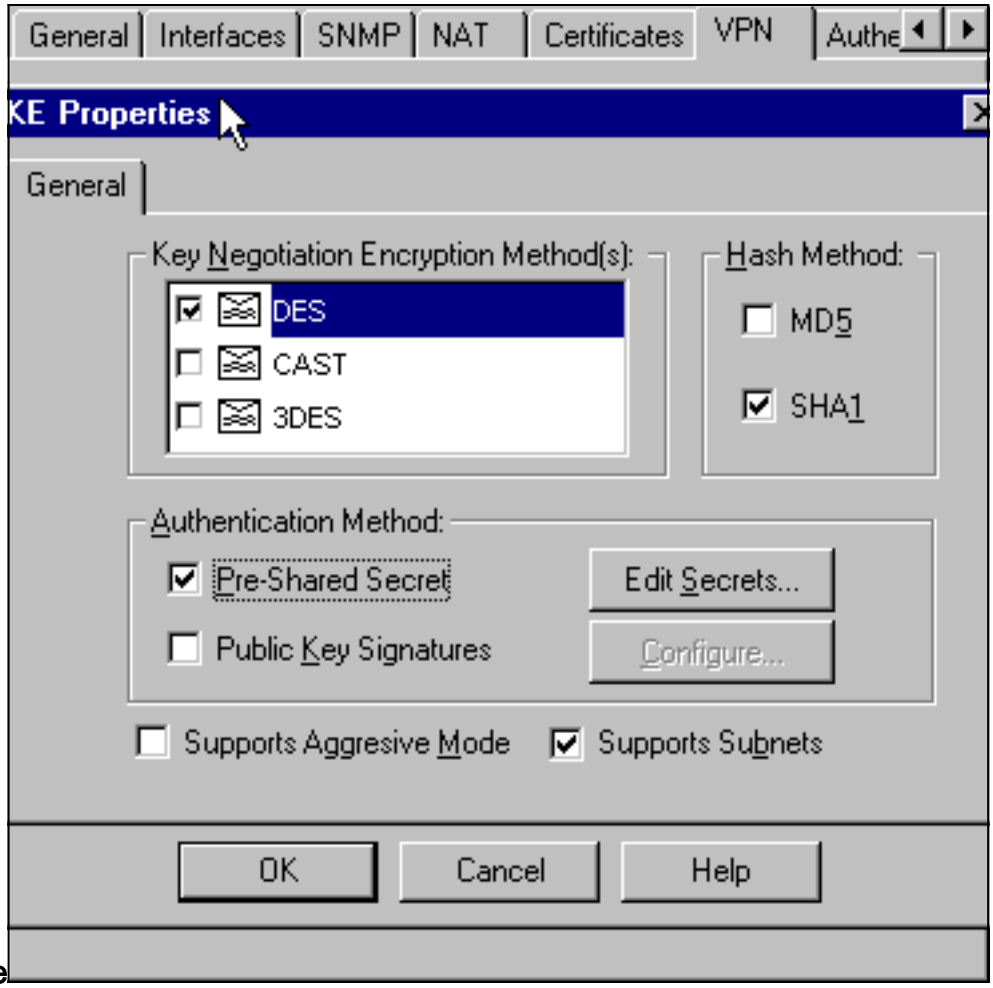

1".

6. Для изменения параметров на вкладке VPN оконечного устройства шлюза Checkpoint (именуемого RTPCPVPN) выберите Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить). На вкладке Domain (Домен) выберите Other (Другой) и затем адрес внутри сети Checkpoint (cpinside) в раскрывающемся списке. В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit



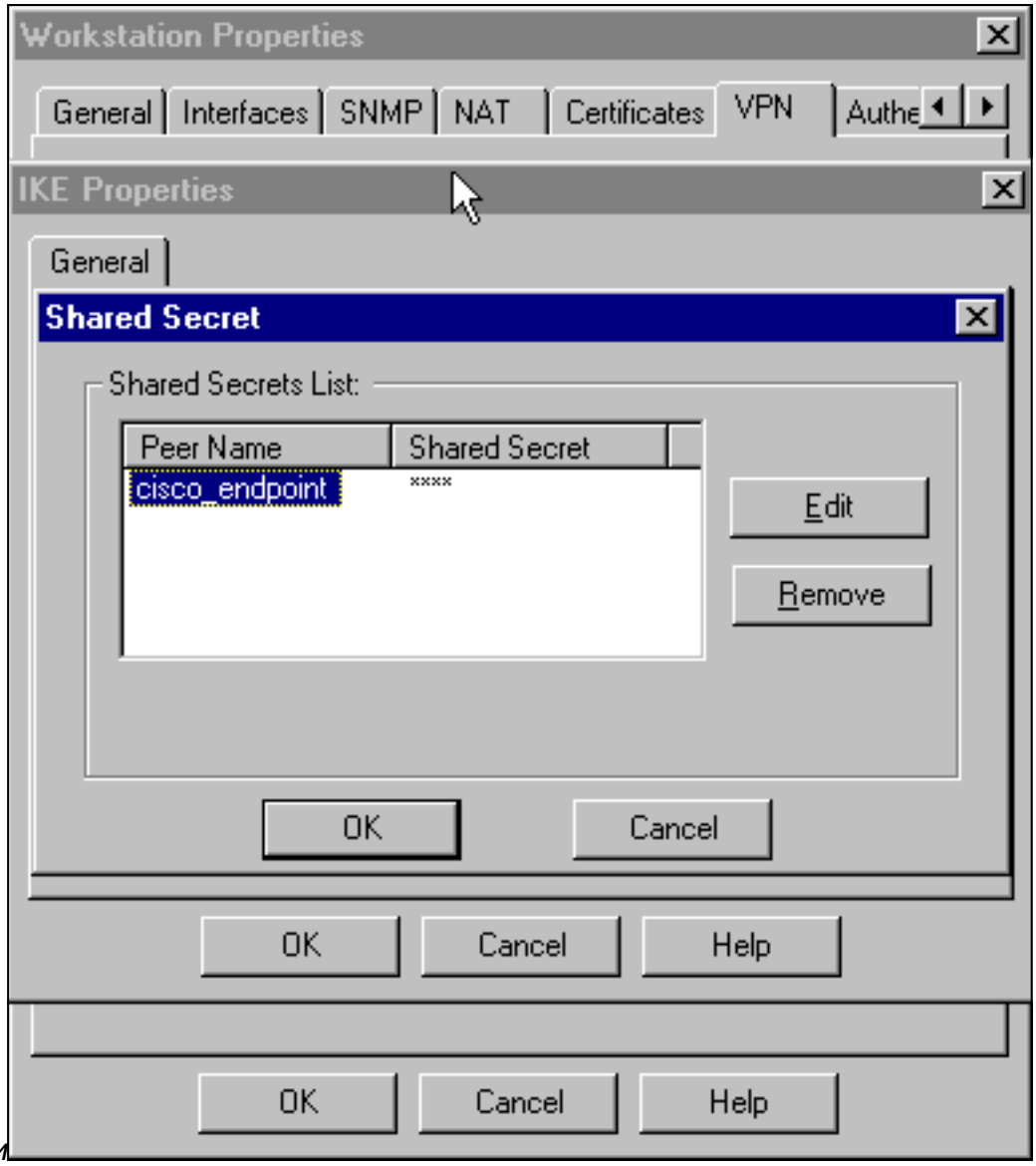

**(Редактировать).**

7. Измените Свойства ike для Шифрования по алгоритму DES (стандарт шифрования данных) для согласия с этой командой:**isakmp policy # encryption des**
8. Измените Свойства ike на хеширование SHA1 для согласия с этой командой:**isakmp policy # hash sha**Измените следующие настройки:**Отмените Aggressive Mode (Агрессивный режим).Установите флажок Supports Subnets (Поддержка подсетей).В разделе Authentication Method (Метод проверки подлинности) установите флажок Pre-Shared Secret (Предварительный секрет).** Это соглашается с этой командой:**политика isakmp # authentication pre-**



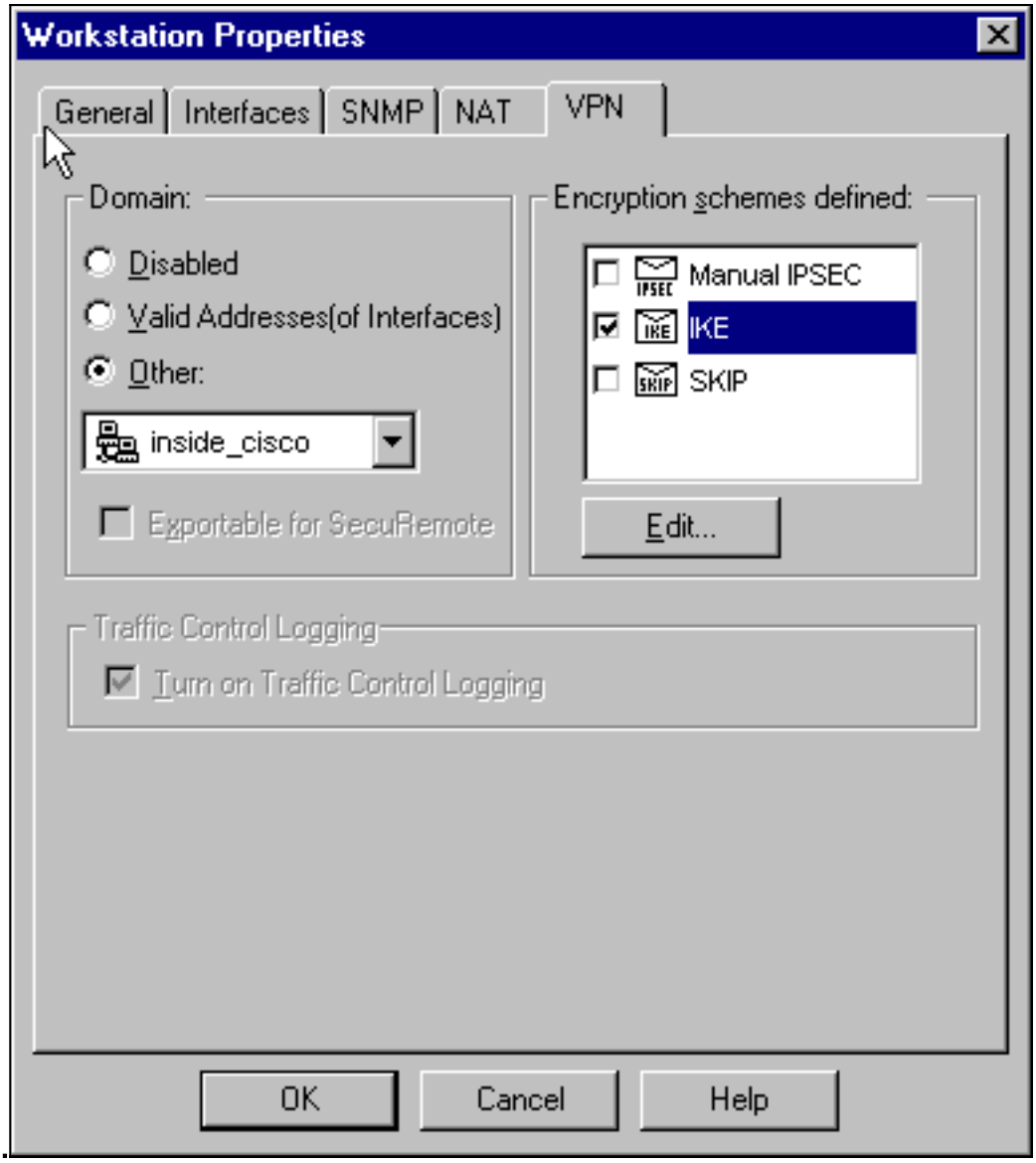

**share**

9. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с командой PIX:*isakmp key ключ address адрес netmask*



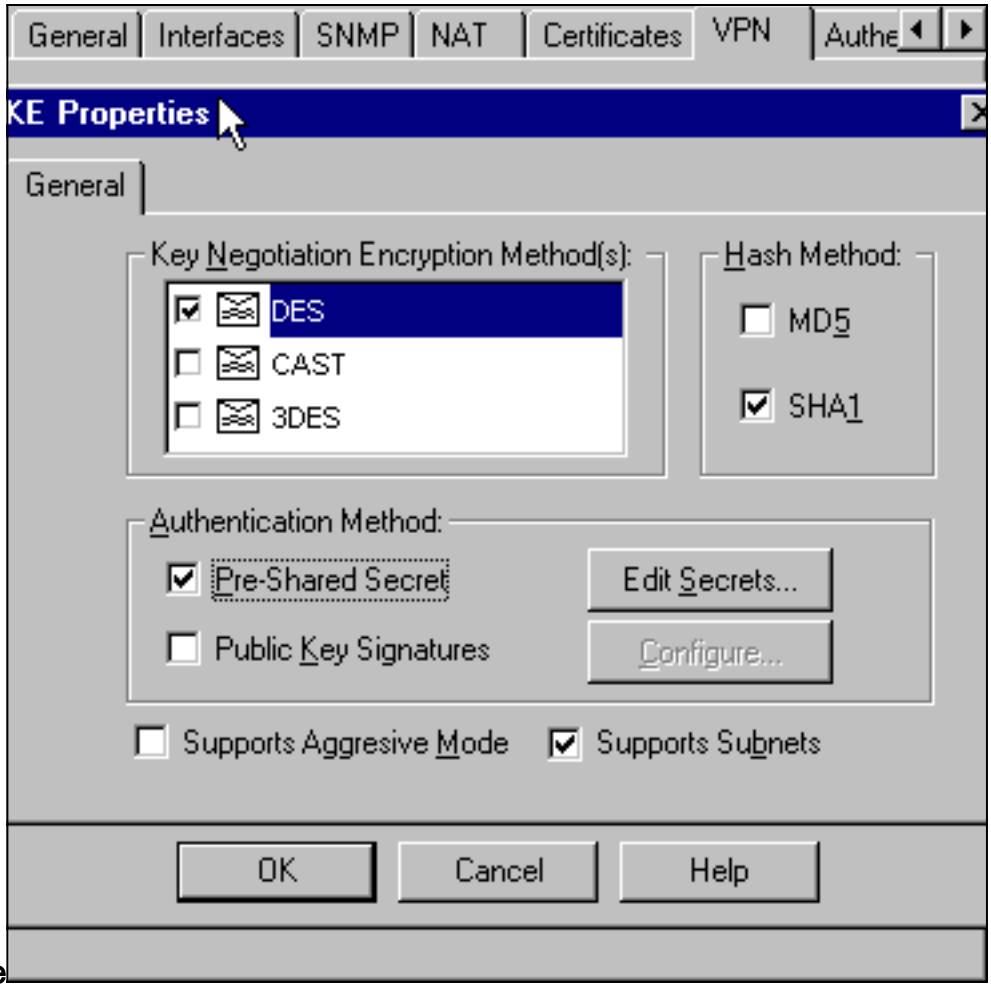

*маска_подсети*

10. Для редактирования вкладки VPN cisco_endpoint Manage > Network objects > Edit (Управление > Сетевые объекты > Изменить). В разделе Domain выберите элемент Other и выберите внутреннюю часть сети PIX (которая называется inside_cisco). В разделе Encryption schemes defined (Определенные схемы шифрования) выберите IKE и нажмите кнопку Edit



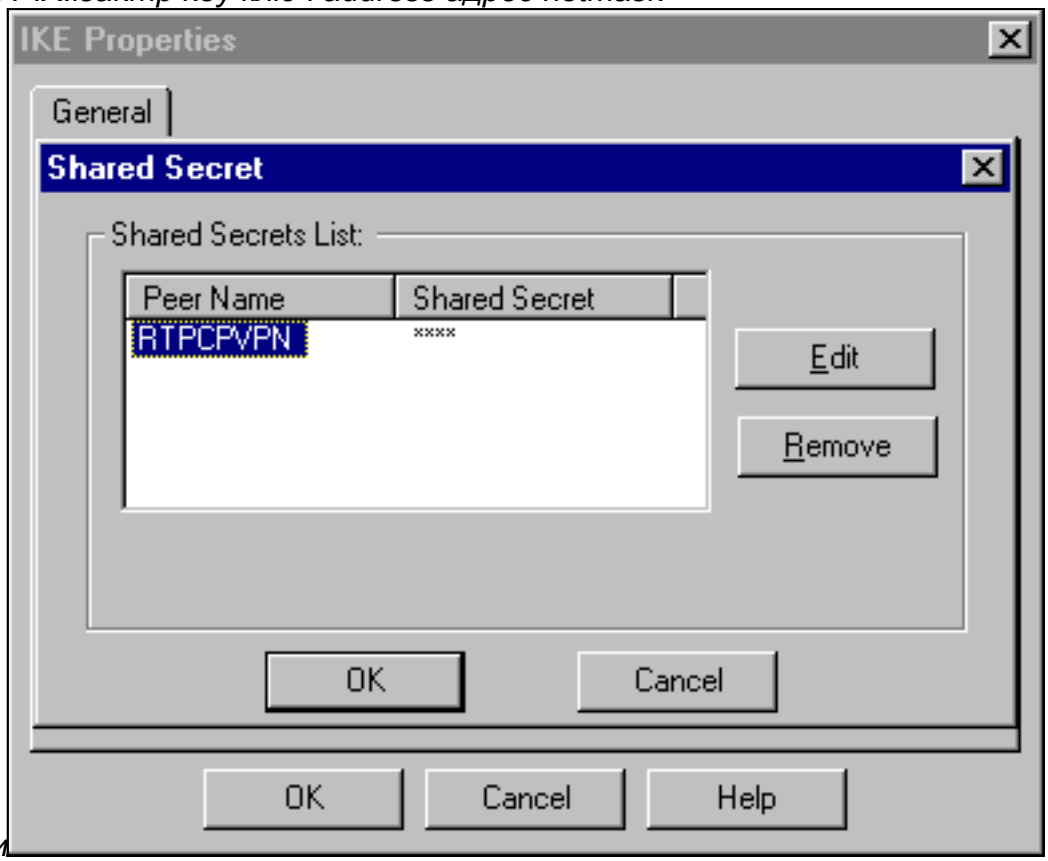

**(Редактировать).**

11. Измените Шифрование по алгоритму DES (стандарт шифрования данных) Свойств ike для согласия с этой командой:**isakmp policy # encryption des**
12. Измените Свойства ike на хеширование SHA1 для согласия с этой командой:**crypto isakmp policy # hash sha**Измените следующие настройки:**Отмените Aggressive Mode (Агрессивный режим).Установите флажок Supports Subnets (Поддержка подсетей).В разделе Authentication Method (Метод проверки подлинности) установите флажок Pre-Shared Secret (Предварительный секрет).** Это действие соглашается с этой командой:**политика isakmp # authentication pre-**




**share**

13. Нажмите **Edit Secrets**, чтобы заставить предварительный общий ключ соглашаться с этой командой PIX:*isakmp key ключ address адрес netmask*

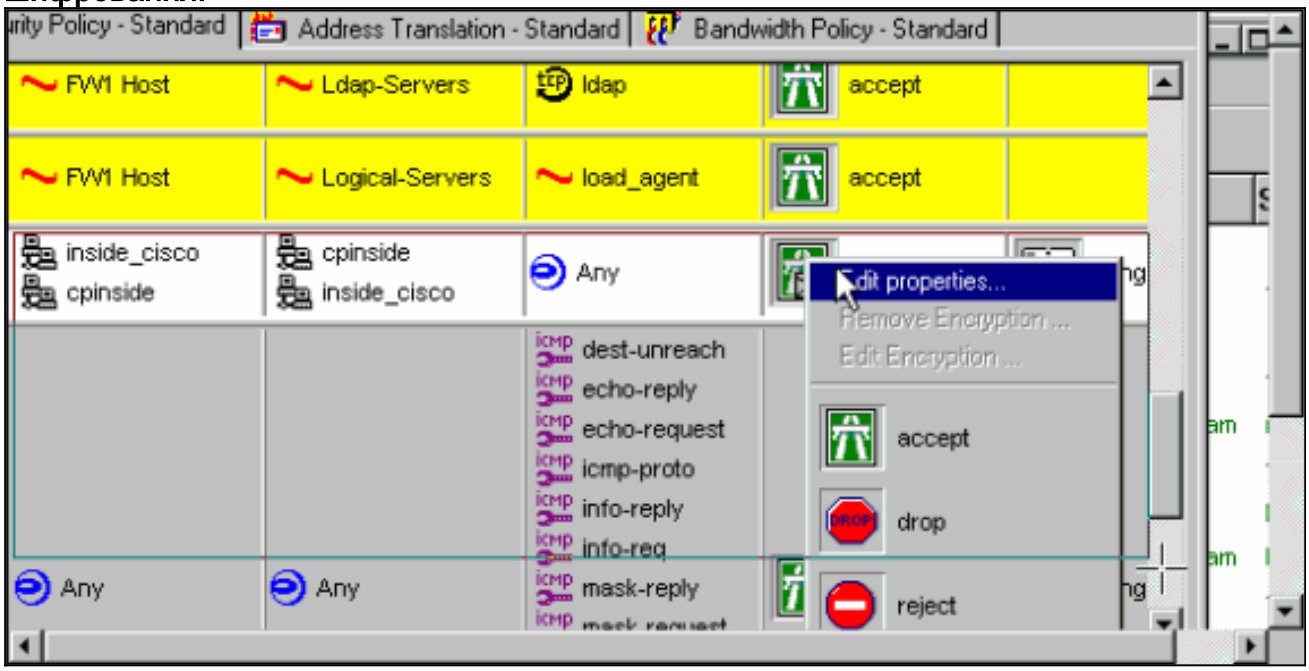



*маска_подсети*

14. В окне Policy Editor (Редактор политик) вставьте правило, в качестве источника и назначения для которого используется inside_cisco и cpinside (двустороннее соединение). **Задайте параметры: Service=Any, Action=Encrypt и**

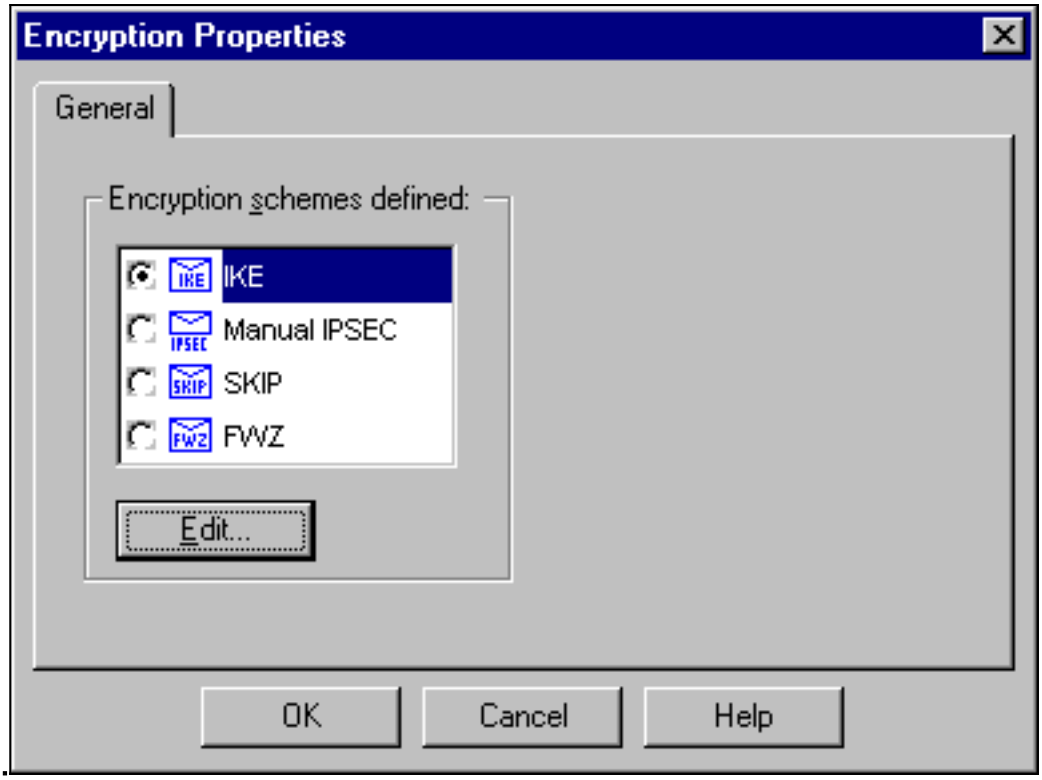
Track=Long.


15. Затем под заголовком Action (Действие) щелкните зеленый значок Encrypt (Шифровать) и выберите пункт Edit properties (Изменить свойства), чтобы настроить политики
шифрования.

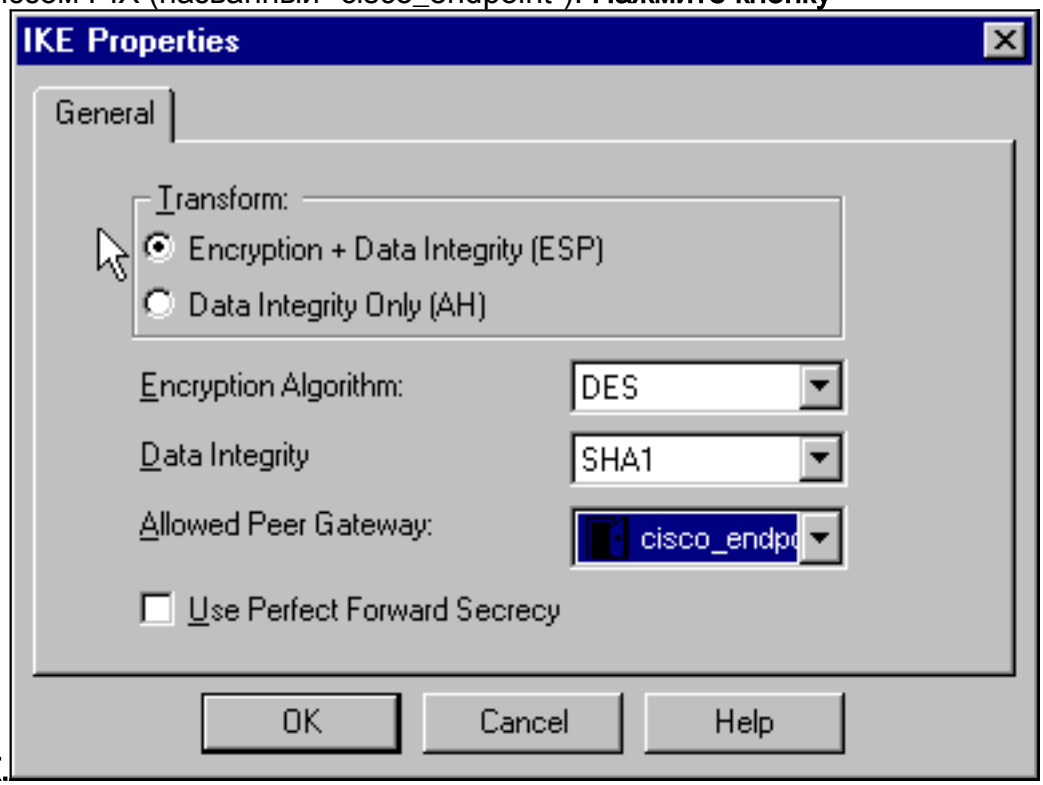



16. Выберите IKE, затем выберите Edit

**(Редактировать).**




17. На экране IKE Properties изменитесь, эти свойства для согласия с PIX IPSEC преобразовывает в эту команду:**crypto ipsec transform-set myset esp-des esp-sha-hmacВ разделе Transform (Преобразование) выберите Encryption + Data Integrity (ESP) (Шифрование + контроль целостности данных [инкапсулирующая защита содержимого]).** Алгоритм шифрования должен быть **DES**, Целостность данных должна быть **SHA1**, и Позволенный Шлюз одноранговой сети должен быть внешним шлюзом PIX (названный "cisco_endpoint"). **Нажмите кнопку**




**OK.**

18. После того, как Контрольная точка настроена, выберите **Policy> Install** на Меню Checkpoint для изменений для вступления в силу.

## [команды debug, show, clear]

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

**Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.**

**Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".**

## Межсетевой экран Cisco PIX

- **debug crypto engine – отображает отладочные сообщения о криптографических устройствах, которые производят шифрование и дешифрование.**
- **debug crypto isakmp – Отображает сообщения о событиях IKE.**
- **debug crypto ipsec—Отображение событий IPSec.**
- **"show crypto isakmp sa" - просмотр всех текущих сопоставлений безопасности IKE (SA IKE) на одноранговом узле.**
- **команда "show crypto ipsec sa" отображает сопоставления безопасности (SA), соответствующие первому этапу.**
- **clear crypto isakmp sa** — (от режима конфигурации) Очищает все соединения активного предложения IKE.
- **clear crypto ipsec sa** — (от режима конфигурации), Удаляют все Сопоставления безопасности IPSec.

## Контрольная точка:

Поскольку Отслеживание долгое время устанавливалось в Окне редактора политики, показанном в шаге 14, отказ в трафике появляется в красном в Log Viewer. Более многословная отладка может быть получена путем ввода:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

и в другом окне:

```
C:\WINNT\FW1\4.1\fwstart
```

**Примечание:** Это было установкой Microsoft Windows NT.

Можно очистить SA на Контрольной точке с этими командами:

```
fw tab -t IKE_SA_table -x fw tab -t ISAKMP_ESP_table -x fw tab -t inbound_SPI -x fw tab -t
ISAKMP_AH_table -x
```

и ответ **на да** при вас уверенный? (приглашение)# .

# Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

## Суммирование сетей

Когда множественные смежные внутренние сети настроены в домене шифрования на Контрольной точке, устройство может автоматически суммировать их относительно представляющего интерес трафика. Если крипто-ACL на PIX не настроен для соответствия, туннель, вероятно, отказывает. 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.

## Пример отладочных выходных данных PIX

```
cisco_endpoint# show debug debug crypto ipsec 1 debug crypto isakmp 1 debug crypto engine debug
fover status tx Off rx Off open Off cable Off txdmp Off rxdmp Off ifc Off rxip Off txip Off get
Off put Off verify Off switch Off fail Off fmsg Off cisco_endpoint# term mon cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange, M-ID of 2112882468:7df00724IPSEC(key_engine): got a
queue event... IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA from
172.18.124.157 to 172.18.124.35 for prot 3 70 crypto_isakmp_process_block: src 172.18.124.157,
dest 172.18.124.35 OAK_QM exchange oakley_process_quick_mode: OAK_QM_IDLE ISAKMP (0): processing
SA payload. message ID = 2112882468 ISAKMP : Checking IPSec proposal 1 ISAKMP: transform 1,
ESP_DES ISAKMP: attributes in transform: ISAKMP: encaps is 1 ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800 ISAKMP: SA life type in kilobytes ISAKMP: SA life
duration (VPI) of 0x0 0x46 0x50 0x0 ISAKMP: authenticator is HMAC-SHA ISAKMP (0): atts are
acceptable.IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest=
172.18.124.157, src= 172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-
hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 ISAKMP (0):
processing NONCE payload. message ID = 2112882468 ISAKMP (0): processing ID payload. message ID
= 2112882468 ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3 map_alloc_entry: allocating entry 4 ISAKMP (0): Creating IPSec SAs inbound SA
from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to 192.168.1.0) has spi 2641490588 and
conn_id 3 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytes outbound SA from
172.18.124.35 to 172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) has spi 3955804195 and conn_id
4 and flags 4 lifetime of 28800 seconds lifetime of 4608000 kilobytesIPSEC(key_engine): got a
queue event... IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src=
172.18.124.157, dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
28800s and 4608000kb, spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): , (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb, spi=
0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4 return status is IKMP_NO_ERROR2303:
sa_request, (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb, spi= 0x0(0),
conn_id= 0, keysize= 0, flags= 0x4004 602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot=
50, sa_spi= 0x9d71f29c(2641490588), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3 602301: sa
created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi= 0xebc8c823(3955804195), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 4 cisco_endpoint# sho cry ips sa interface: outside Crypto
map tag: rtpmap, local addr. 172.18.124.35 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 172.18.124.157 PERMIT, flags={origin_is_acl,} #pkts encaps: 0, #pkts encrypt: 0,
#pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts
decompressed: 0 #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0 local crypto endpt.: 172.18.124.35, remote crypto endpt.:
172.18.124.157 path mtu 1500, ipsec overhead 0, media mtu 1500 current outbound spi: 0 inbound
esp sas: inbound ah sas: inbound pcp sas: outbound esp sas: outbound ah sas: outbound pcp sas:
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT,
flags={origin_is_acl,} #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4 #pkts decaps: 4, #pkts
decrypt: 4, #pkts verify 4 #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.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, ipsec overhead 56,
media mtu 1500 current outbound spi: ebc8c823 inbound esp sas: spi: 0x9d71f29c(2641490588)
transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 3, crypto map:
```

```
rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV size: 8 bytes replay
detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0xebc8c823(3955804195) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 4, crypto map: rtpmap sa timing: remaining key lifetime (k/sec): (4607999/28777) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: cisco_endpoint# sho
cry is sa dst src state pending created 172.18.124.157 172.18.124.35 QM_IDLE 0 2
```

## Дополнительные сведения

- Страница поддержки PIX
- Справочник по командам PIX
- Запросы комментариев (RFC)
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- PIX 5.2: Выбор конфигурации IPSec
- PIX 5.3: Выбор конфигурации IPSec
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems