Настройка туннеля IPSec между маршрутизатором Cisco и Checkpoint NG

Содержание

Введение

Этот документ демонстрирует, как сформировать туннель IPSec с предварительными ключами для соединения 2-х частных сетей:

- 172.16.15.x частная сеть в маршрутизаторе.
- 192.168.10.x частная сеть в Следующем поколении (NG) CheckpointTM.

Предварительные условия

Требования

Процедуры, выделенные в этом документе, основываются на этих предположениях.

- Основная политика NG CheckpointTM установлена.
- Весь доступ, Технология NAT и направляющие настройки настроены.
- Трафик из маршрутизатора и в NG CheckpointTM к интернет-потокам.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного

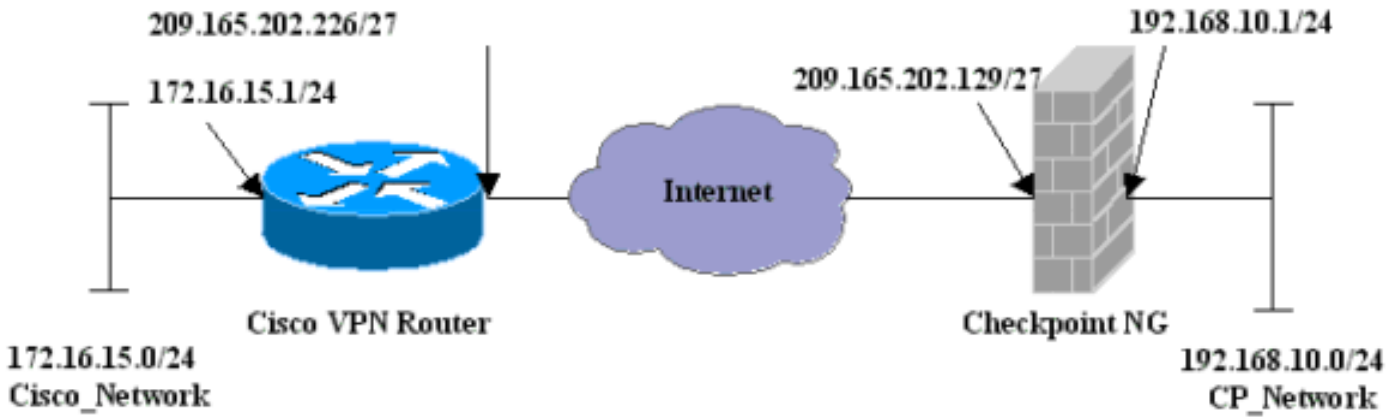
обеспечения и оборудования:

- Маршрутизатор Cisco 1751
- Программное обеспечение Cisco IOS (C1700-K9O3SY7-M), версия 12.2 (8) T4, РЕЛИЗ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (fc1)
- NG CheckpointTM создает 50027

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 в документах см. Cisco Technical Tips Conventions.

Настройте маршрутизатор с поддержкой VPN Cisco 1751

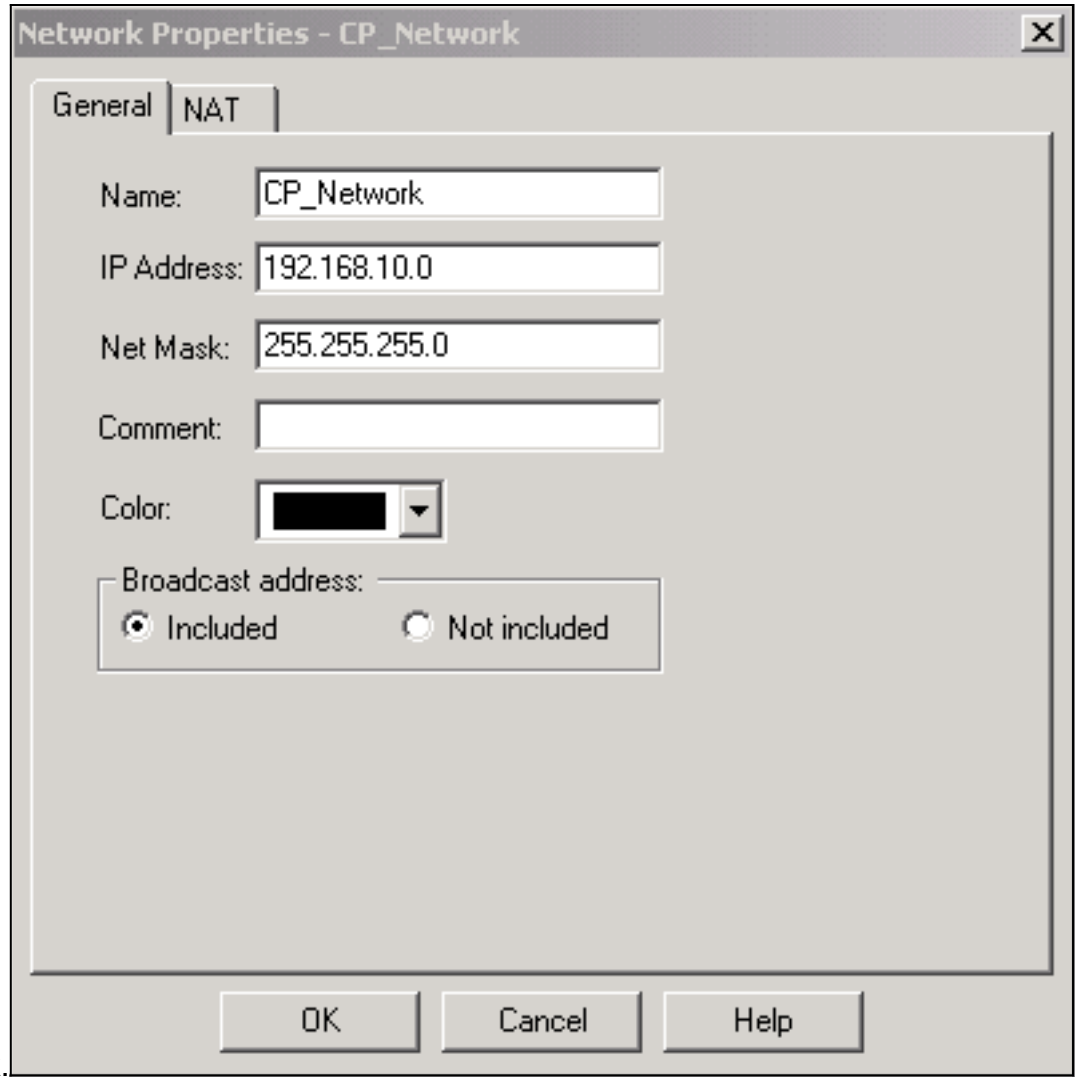
Маршрутизатор VPN Cisco 1751 года
version 12.2 service timestamps debug uptime service timestamps log uptime no service password-encryption hostname sv1-6 memory-size iomem 15 mmi polling-interval 60 no mmi auto-configure no mmi pvc mmi snmp-timeout 180 ip subnet-zero no ip domain-lookup ip audit notify log ip audit po max-events 100 *!--- Internet Key Exchange (IKE) configuration.* **crypto isakmp policy 1 encr 3des hash md5 authentication pre-share group 2 lifetime 1800** *!--- IPSec configuration.* **crypto isakmp key aptrules address 209.165.202.129 !**

```
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
! crypto map aptmap 1 ipsec-isakmp set peer
209.165.202.129 set transform-set aptset match address
110 ! interface Ethernet0/0 ip address 209.165.202.226
255.255.255.224 ip nat outside half-duplex crypto map
aptmap ! interface FastEthernet0/0 ip address
172.16.15.1 255.255.255.0 ip nat inside speed auto !---
NAT configuration. ip nat inside source route-map nonat
interface Ethernet0/0 overload ip classless ip route
0.0.0.0 0.0.0.0 209.165.202.225 no ip http server ip pim
bidir-enable !--- Encryption match address access list.
access-list 110 permit ip 172.16.15.0 0.0.0.255
192.168.10.0 0.0.0.255 !--- NAT access list. access-list
120 deny ip 172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10 match ip address 120 line con
0 exec-timeout 0 0 line aux 0 line vty 0 4 password
cisco login end
```

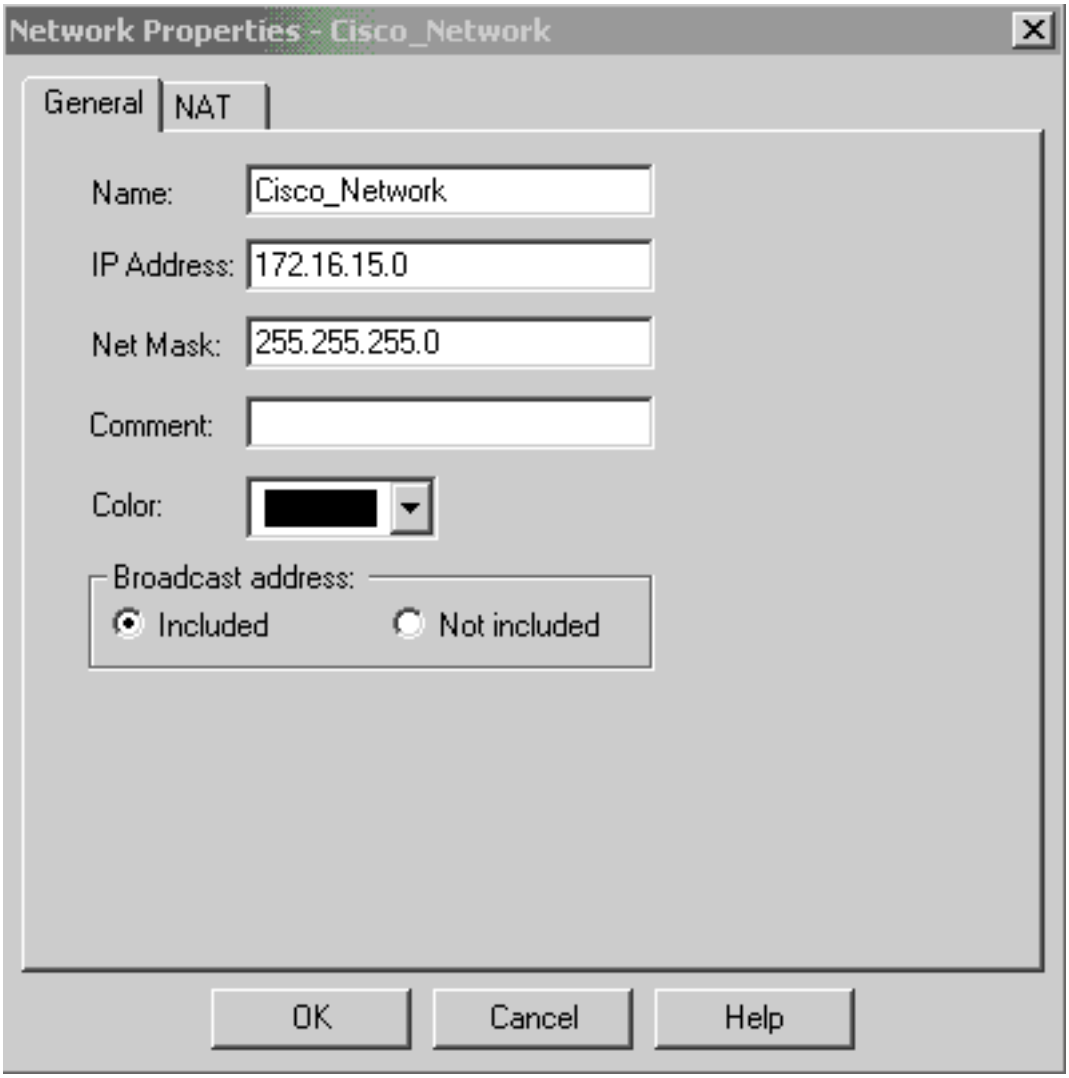
Настройте контрольную точку NG

NG CheckpointTM является объектно-ориентированной конфигурацией. Сетевые объекты и правила определены 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 VPN.

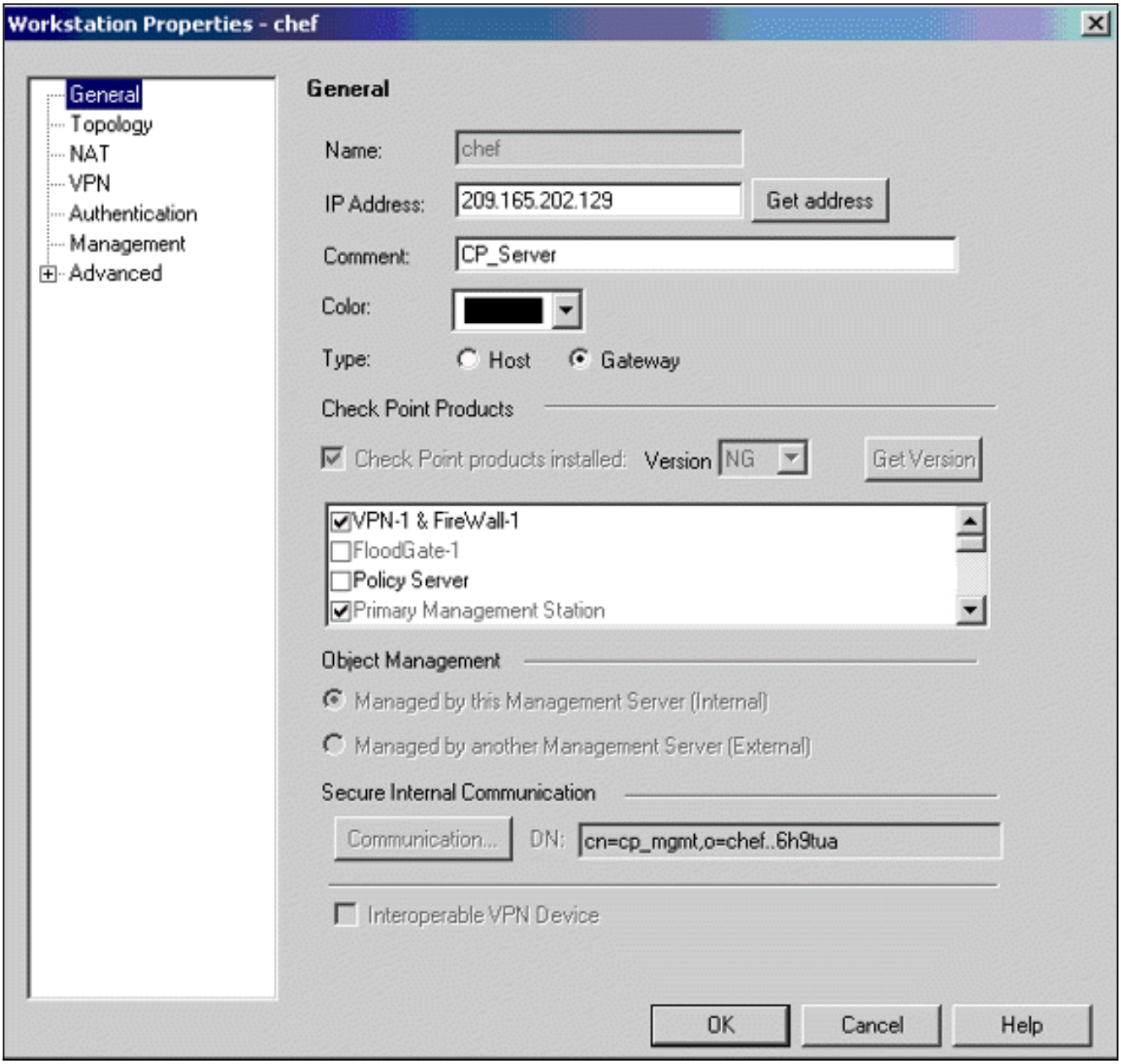
1. Создайте подсеть Сети Cisco и подсеть Сети NG CheckpointTM как сетевые объекты. Это - то, что зашифровано. Для создания объектов выберите **Manage> Network Objects**, затем выберите **New> Network**. Введите соответствующую информацию о сети, затем нажмите **OK**.Эти примеры показывают установленный из объектов под названием CP_Network и

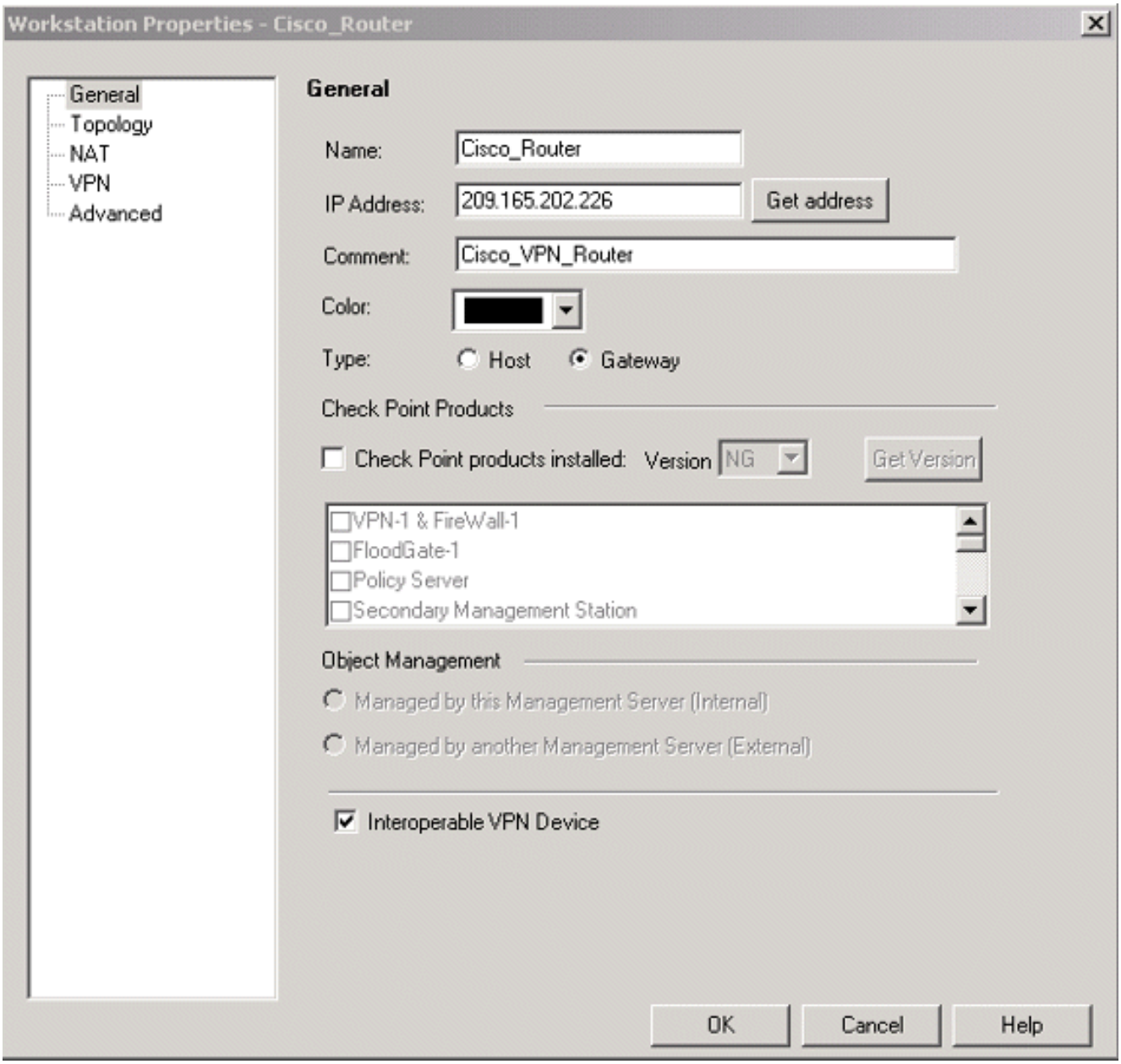


Cisco_Network.

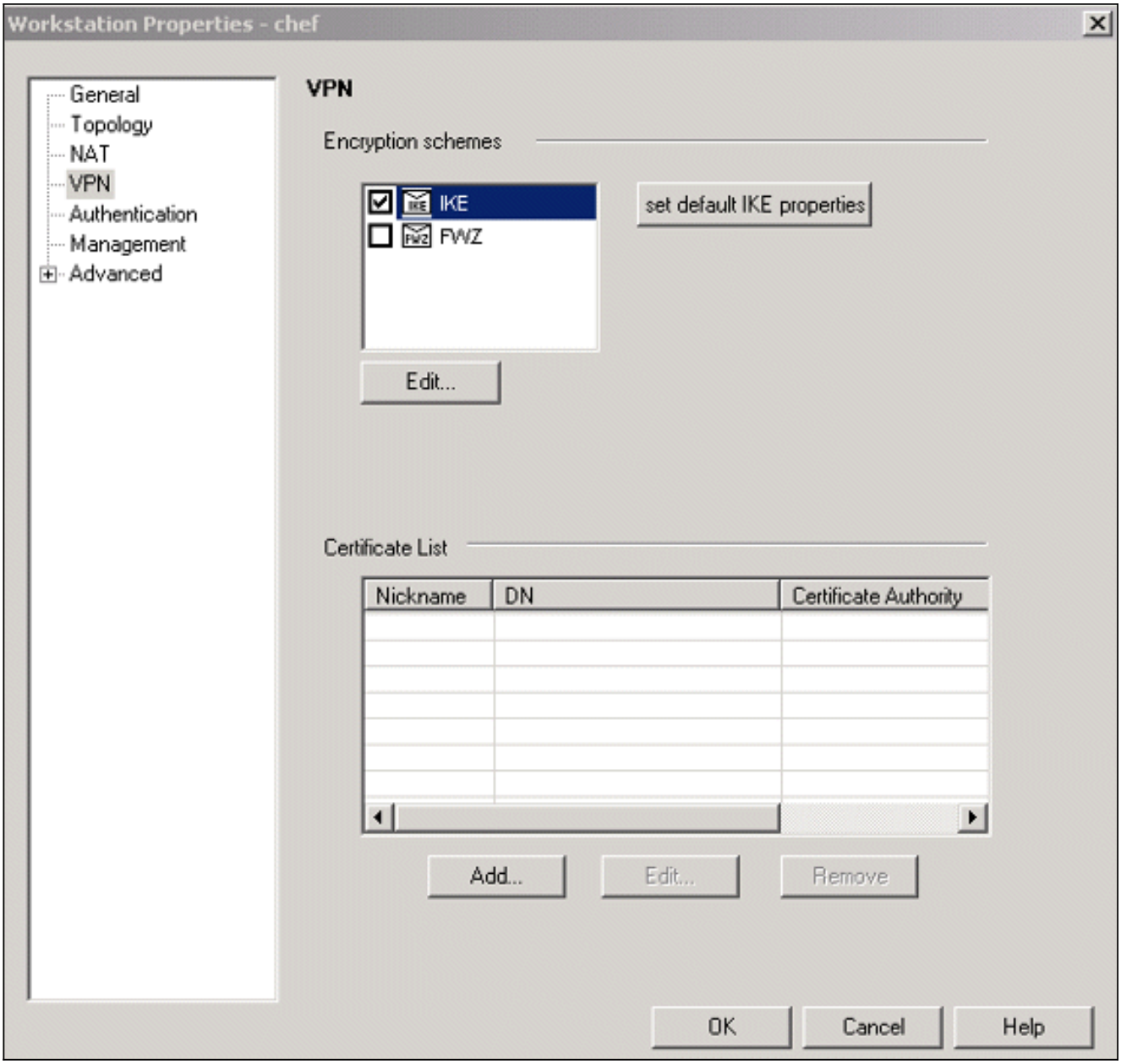


2. Создайте объекты Cisco_Router и Checkpoint_NG как объекты рабочей станции. Это устройства VPN. Для создания объектов выберите **Manage> Network Objects**, затем выберите **New> Workstation**.Обратите внимание на то, что можно использовать объект рабочей станции NG CheckpointTM, созданный во время начальной настройки NG CheckpointTM. Выберите опции для установки рабочей станции как **шлюза** и **взаимодействующего устройства VPN**.Эти примеры показывают установленный из объектов, названных поваром и Cisco_Router.

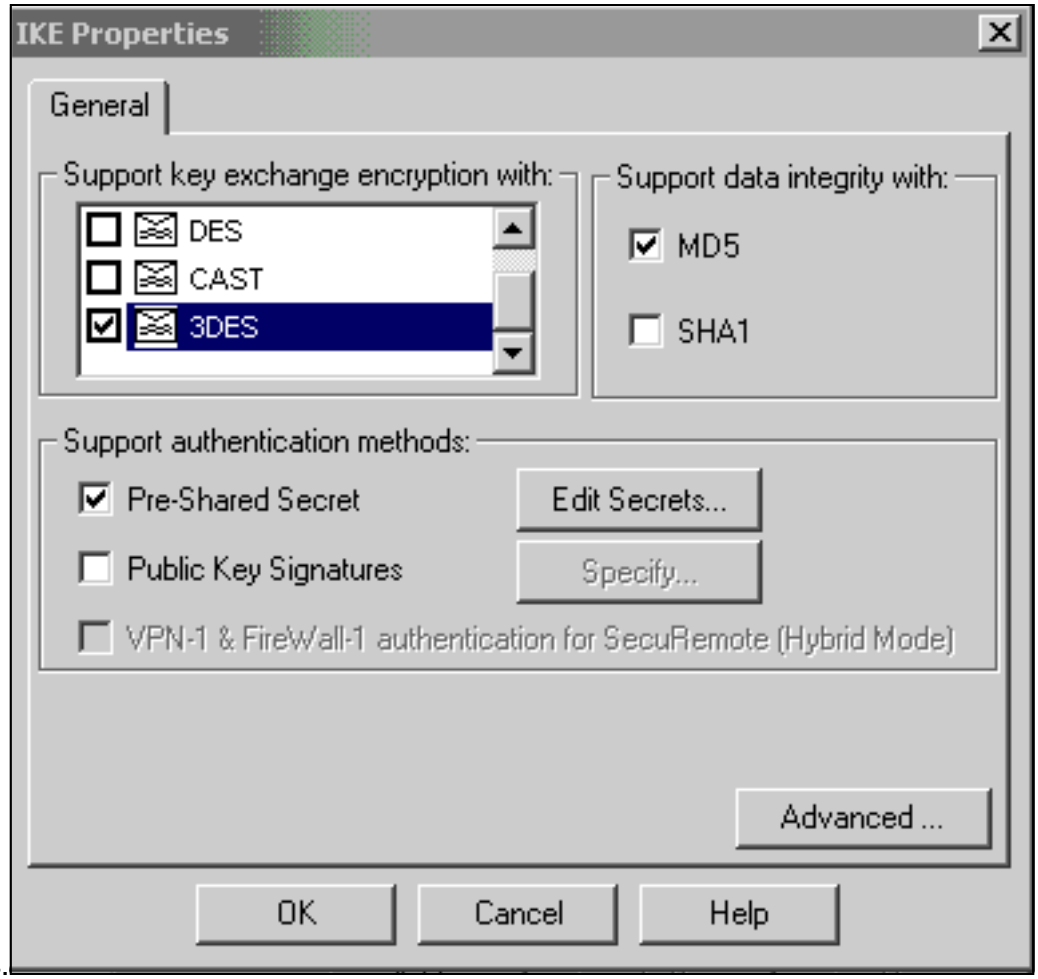

Workstation Properties - chef
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
chef
IP Address:
209.165.202.129
Get address
Comment:
CP_Server
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
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=chef..6h9tua
Interoperable VPN Device
OK
Cancel
Help



3. Настройте IKE на вкладке VPN, затем нажмите **Edit**.

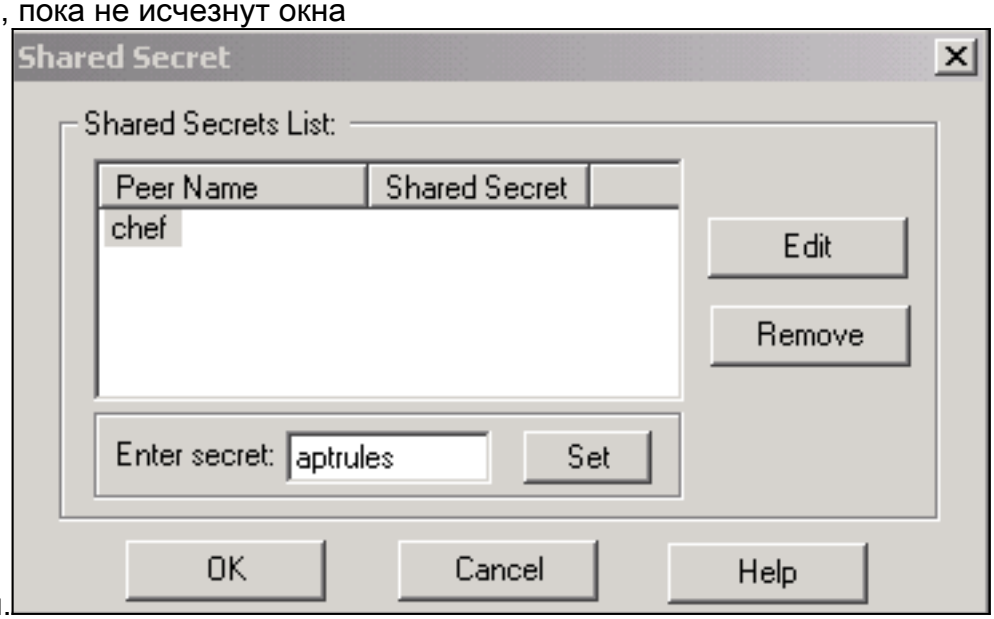


4. Настройте политику обмена ключами и нажмите **Edit**

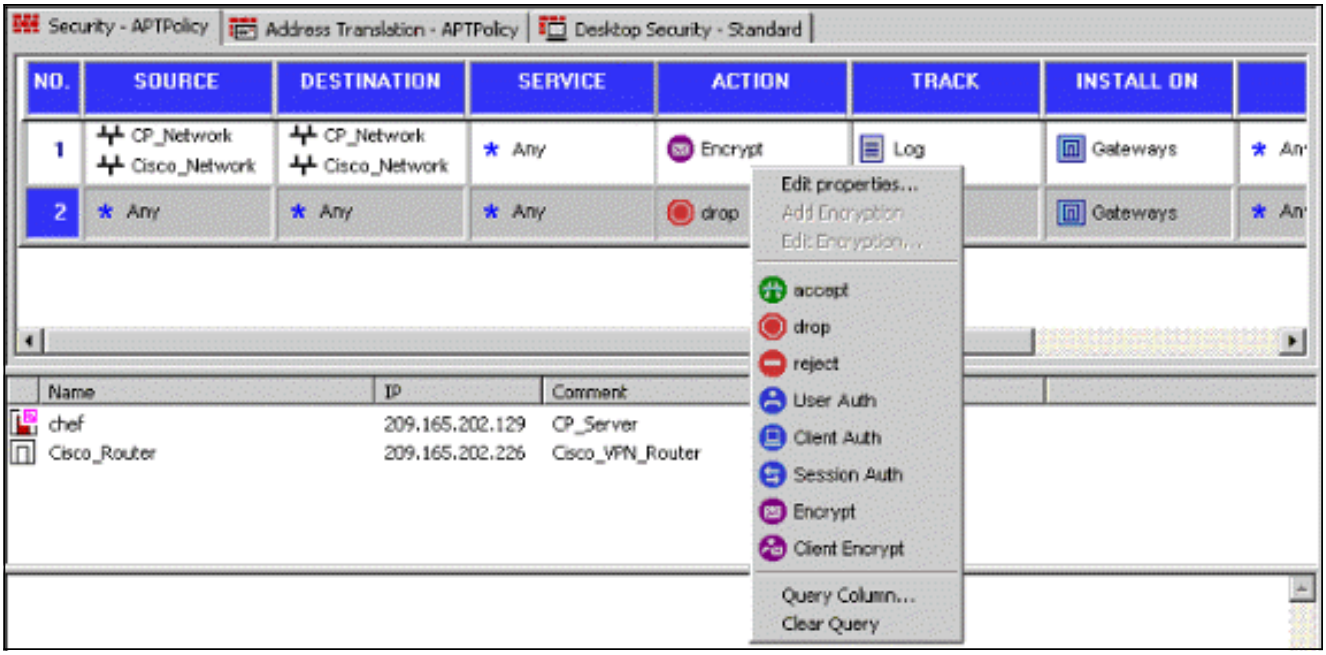


Secrets.

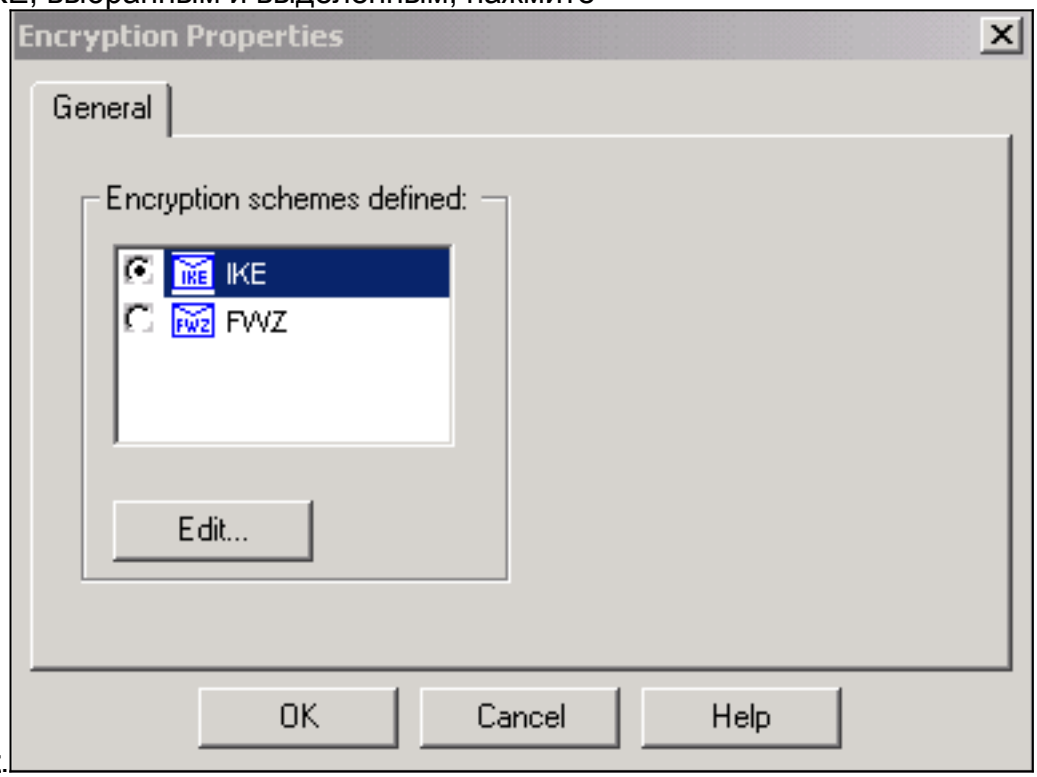
5. Заставьте предварительные общие ключи использоваться, затем нажимать **OK** несколько раз, пока не исчезнут окна конфигурации.



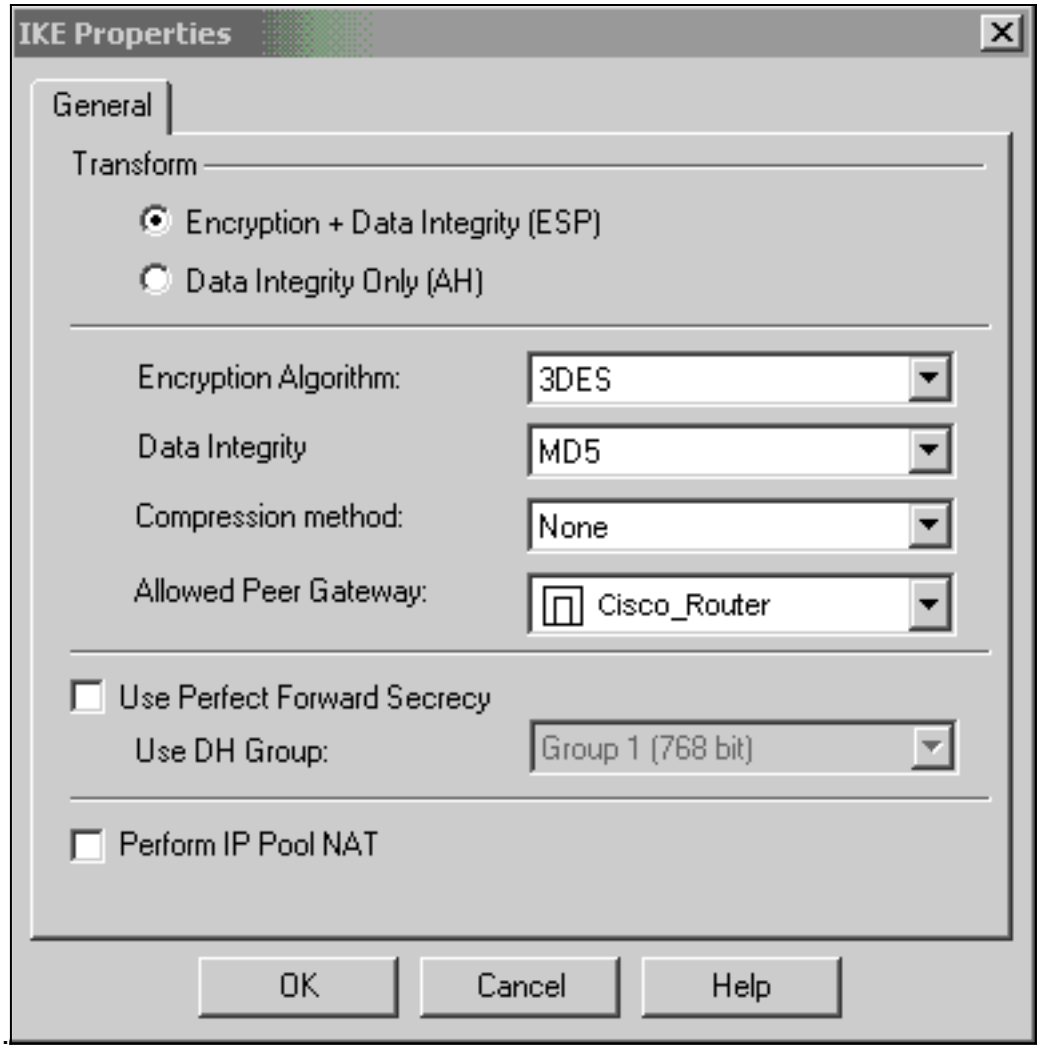
6. Выберите **Rules> Add Rules> Top** для настройки правил шифрования для политики.Правило о вершине является первым правилом, выполненным перед любым другим правилом, которое может обойти шифрование. Настройте Источник и Назначение для включения CP_Network и Cisco_Network, как показано здесь. Как только вы добавили Зашифровать раздел Действия правила, щелкаете правой кнопкой мыши **Действие** и выбираете **Edit Properties**.



7. С IKE, выбранным и выделенным, нажмите **Edit**.

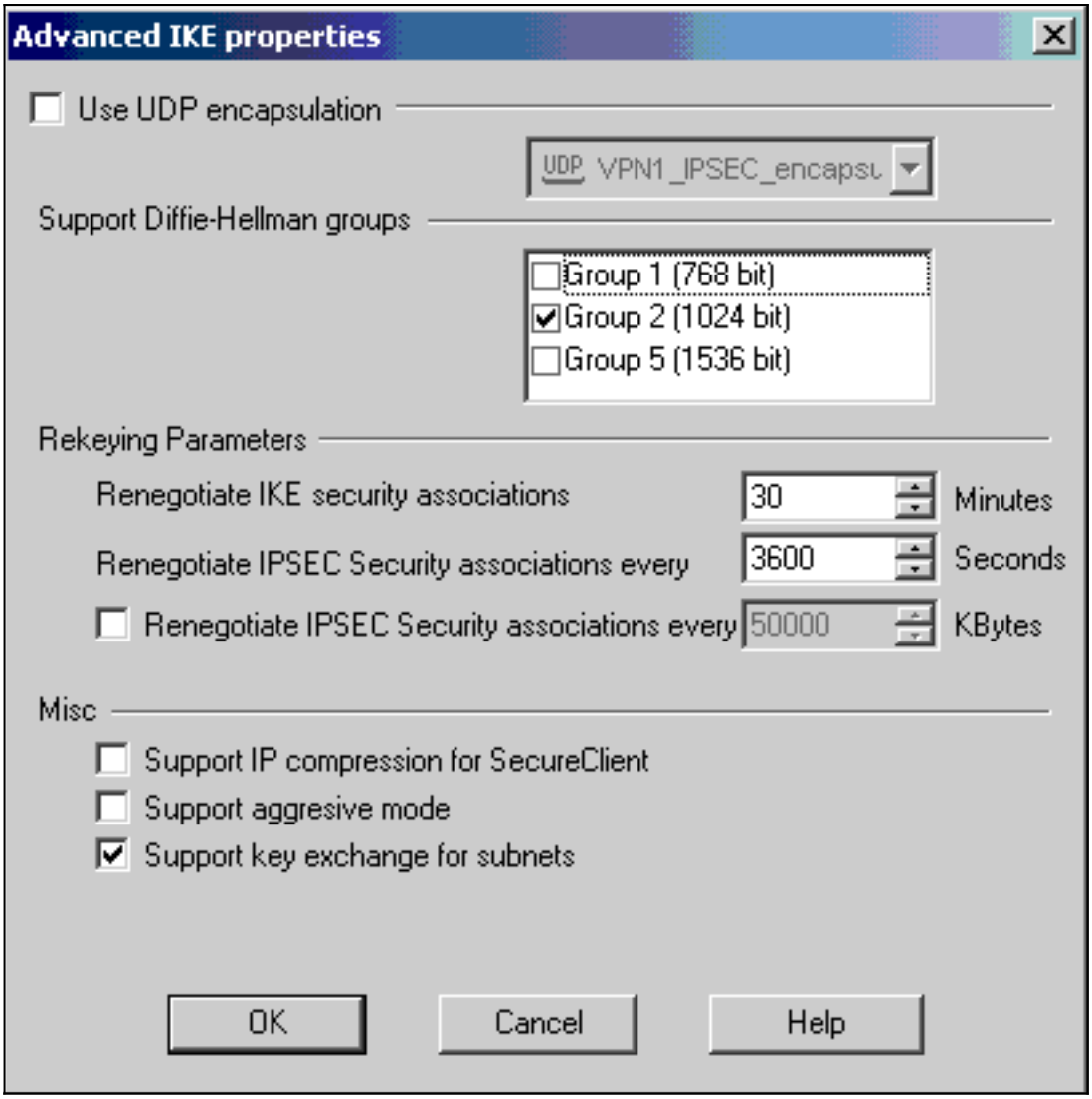


8. Подтвердите конфигурацию

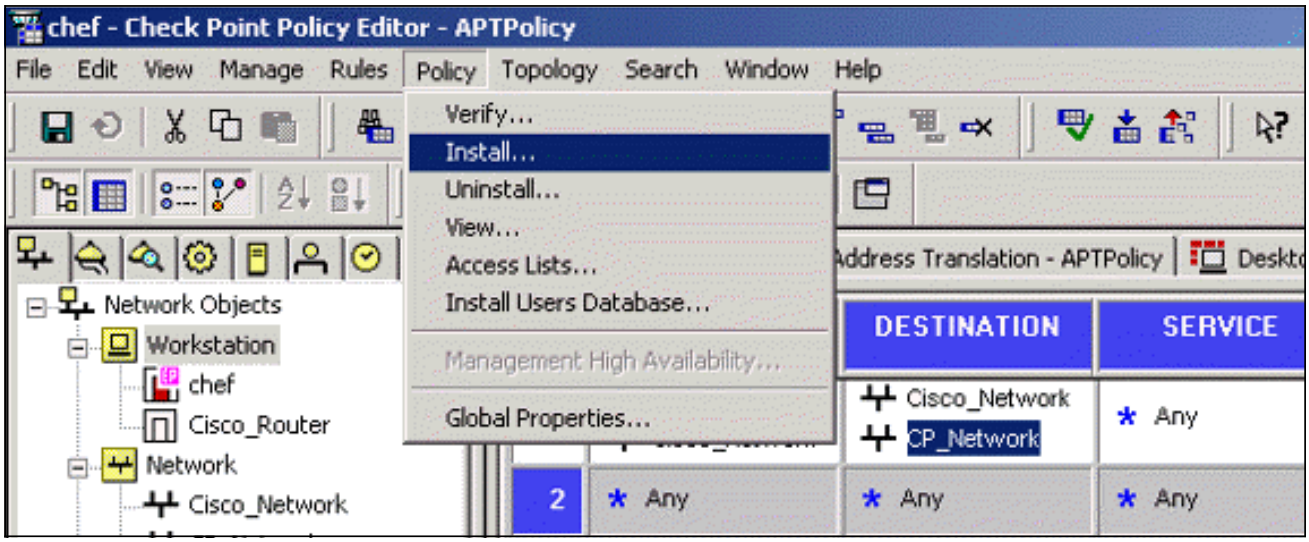


IKE.

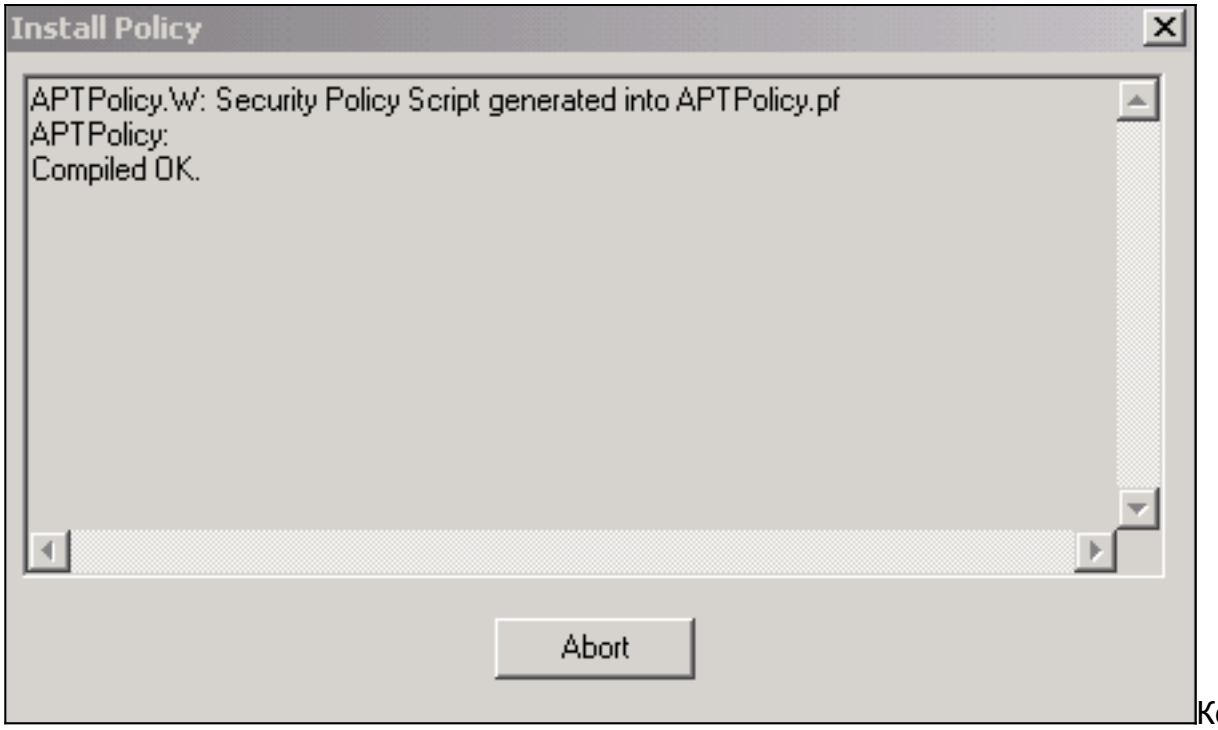
9. Одна из основных проблем с рабочей VPN между устройствами Cisco и другими Устройствами IPSec является Пересмотром Обмена ключами. Гарантируйте, что установка для обмена IKE на маршрутизаторе Cisco является точно тем же как настроенным на NG CheckpointTM.**Примечание:** Актуальное значение этого параметра зависит от вашей определенной политики корпоративной безопасности.В данном примере конфигурация IKE на маршрутизаторе была установлена в 30 минут с **командой lifetime 1800**. То же значение должно быть установлено на NG CheckpointTM.Для установки этого значения на NG CheckpointTM выберите **Manage Network Object**, затем выберите объект CheckpointTM NG и нажмите **Edit**. Затем выберите **VPN** и отредактируйте IKE. Выберите **Advance** и настройте параметры смены ключа. После того, как вы настраиваете обмен ключами для объекта Сети NG CheckpointTM, выполняете одинаковую конфигурацию Пересмотра Обмена ключами для сетевого объекта Cisco_Router.**Примечание:** Гарантируйте, что вам выбрали корректную Группу Диффи-Хеллмана для соответствия, который настроил на маршрутизаторе.



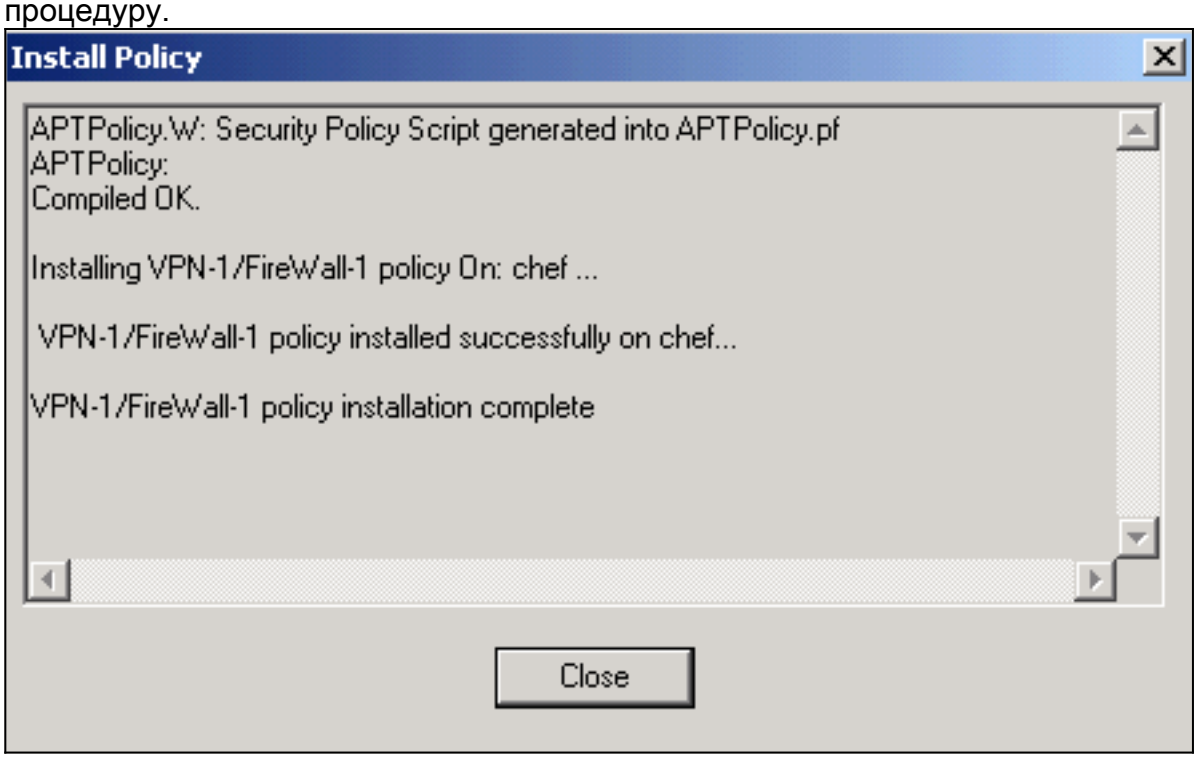
10. Конфигурация политики завершена. Сохраните политику и выберите **Policy> Install** для включения
его.



Замечания о ходе работы показов окна установки как политика скомпилированы.



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



Проверка

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

Проверьте маршрутизатор Cisco

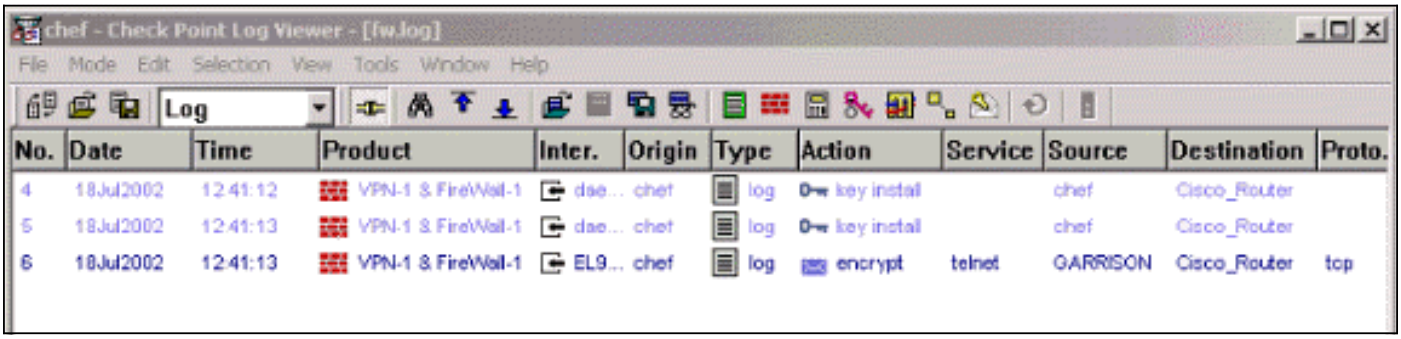
Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику

выходных данных команды show.

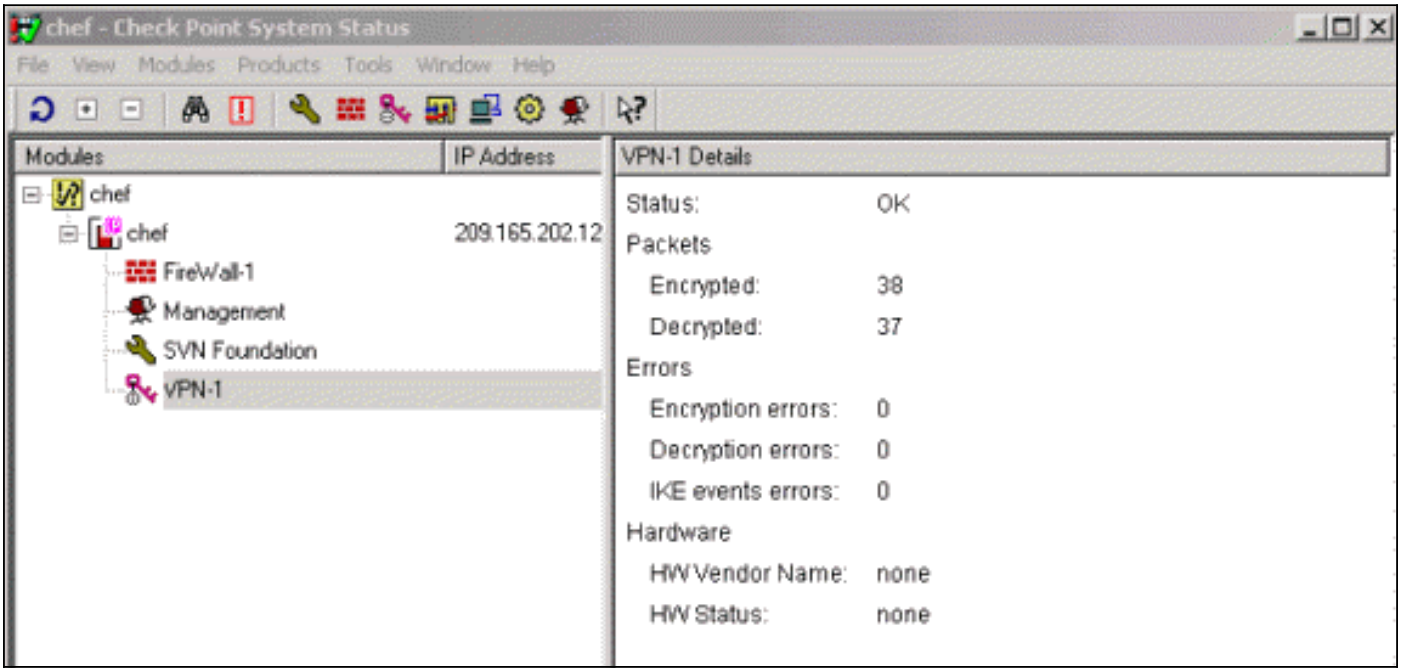
- **show crypto isakmp sa – отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле.**
- **show crypto ipsec sa — отображает настройки, используемые текущими SA.**

Проверьте контрольную точку NG

Для просмотра журналов выберите **Window> Log Viewer**.



Для просмотра состояния системы выберите **Window> System Status**.



Устранение неполадок

Маршрутизатор Cisco

В этом разделе описывается процесс устранения неполадок конфигурации.

Для дополнительных сведений об устранении проблем, см. Устранение проблем системы безопасности IP - Понимание и Использование команд отладки.

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

- **debug crypto engine** сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.
- **debug crypto isakmp – отображает сообщения о событиях IKE.**
- **debug crypto ipsec– показывает события IPSec.**
- **clear crypto isakmp** все соединения активного предложения IKE.
- **clear crypto sa** все КОНТЕКСТЫ БЕЗОПАСНОСТИ IPSEC.

Успешный Вывод лога отладки

```
18:05:32: ISAKMP (0:0): received packet from
   209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
   but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
   against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
   message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
   matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
   MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
   MM_KEY_EXCH
```

```
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
   IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
   message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
   message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
   with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
   IKE_PHASE1_COMPLETE
```

Old State = IKE_P1_COMPLETE New State = IKE_P1_COMPLETE 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): processing HASH payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing SA payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): Checking IPSec proposal 1 18:05:33: ISAKMP: transform 1, ESP_3DES 18:05:33: ISAKMP: attributes in transform: 18:05:33: ISAKMP: SA life type in seconds 18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10 18:05:33: ISAKMP: authenticator is HMAC-MD5 18:05:33: ISAKMP: encaps is 1 18:05:33: ISAKMP (0:1): atts are acceptable. 18:05:33: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_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= 0x4 18:05:33: ISAKMP (0:1): processing NONCE payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): processing ID payload. message ID = -1335371103 18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA from 209.165.202.226 to 209.165.202.129 for prot 3 18:05:33: ISAKMP: received ke message (2/1) 18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2 18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:33: ISAKMP (0:1): Creating IPSec SAs 18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226 (proxy 192.168.10.0 to 172.16.15.0) 18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4 18:05:33: lifetime of 3600 seconds 18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129 (proxy 172.16.15.0 to 192.168.10.0) 18:05:33: has spi -2006413528 and conn_id 201 and flags C 18:05:33: lifetime of 3600 seconds 18:05:33: ISAKMP (0:1): deleting node -1335371103 error FALSE reason "quick mode done (await()" 18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH **Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE** 18:05:33: IPSEC(key_engine): got a queue event... 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) INBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0, flags= 0x4 18:05:33: IPSEC(initialize_sas): , (key eng. msg.) OUTBOUND local= 209.165.202.226, remote=209.165.202.129, local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4), remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-3des esp-md5-hmac , lifedur= 3600s and 0kb, spi=

0x88688F28(2288553768), conn_id= 201, keysize= 0, flags= 0xC 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.226, sa_prot= 50, sa_spi= 0x800022D3(2147492563), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200 18:05:33: IPSEC(create_sa): sa created, (sa) sa_dest= 209.165.202.129, sa_prot= 50, sa_spi= 0x88688F28(2288553768), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201 18:05:34: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 18:05:34: ISAKMP (0:1): received packet from 209.165.202.129 (R) QM_IDLE 18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate of a previous packet. 18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2 18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2 node marked dead -1335371103 sv1-6#**show crypto isakmp sa** dst src state conn-id slot 209.165.202.226 209.165.202.129 QM_IDLE 1 0 sv1-6#**show crypto ipsec sa** interface: Ethernet0/0 Crypto map tag: aptmap, local addr. 209.165.202.226 local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0) current_peer: 209.165.202.129 PERMIT, flags={origin_is_acl,} **#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21 #pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24** #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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129 path mtu 1500, media mtu 1500 current outbound spi: 88688F28 inbound esp sas: spi: 0x800022D3(2147492563) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3559) IV size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi: 0x88688F28(2288553768) transform: esp-3des esp-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap sa timing: remaining key lifetime (k/sec): (4607997/3550) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas: sv1-6#**show crypto engine conn act** ID Interface IP- Address State Algorithm Encrypt Decrypt 1 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 0 200 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C 0 **24** 201 Ethernet0/0 209.165.202.226 set HMAC_MD5+3DES_56_C **21** 0

Дополнительные сведения

- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems