# Настройка IPSec между системой Microsoft Windows 2000 Server и устройством Cisco

## Содержание



## Введение

Этот документ демонстрирует формирование туннеля IPSec с предварительными общими ключами для подключения к двум частным сетям: частной сети (192.168.l. X) в устройства Cisco и частной сети (10.32.50. X) в Microsoft 2000 Server. Мы полагаем, что трафик из устройства Cisco и из 2000 Server в Интернет (представленный здесь сетями 172.18.124.X) идет до начала этой конфигурации.

Подробные сведения о настройке можно найти на сервере Windows 2000 server на веб-узле компании Майкрософт: http://support.microsoft.com/support/kb/articles/Q252/7/35. ASP

## Перед началом работы

### Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

## Предварительные условия

Для данного документа отсутствуют предварительные условия.

## Используемые компоненты

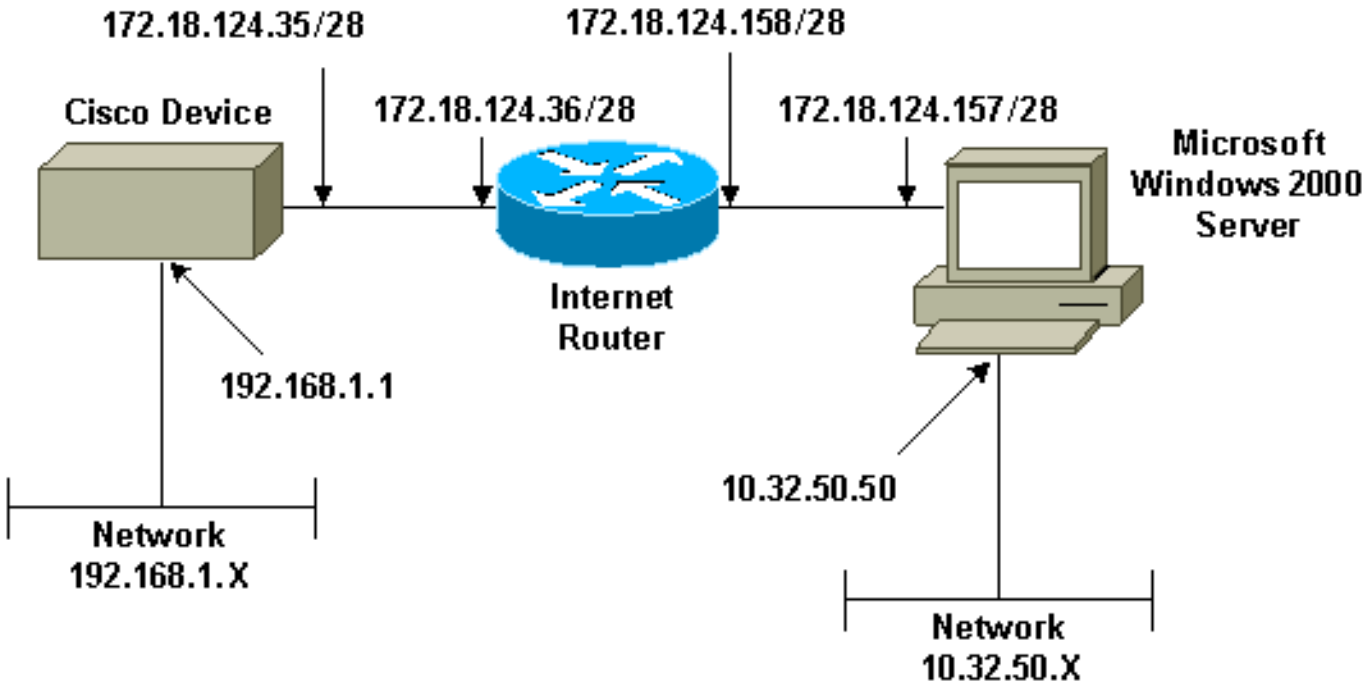
При разработке и тестировании этих конфигураций использовались следующие версии программного и аппаратного обеспечения.

- Сервер Microsoft Windows 2000 5.00.2195
- Маршрутизатор Cisco 3640 с операционной системой Cisco IOS® выпуска c3640-ik2o3s-mz.121-5.T.bin
- Брандмауэр Cisco Secure PIX с ПО PIX выпуска 5.2.1
- Концентратор Cisco VPN 3000 с программным обеспечением VPN 3000 Concentrator версии 2.5.2.F
- Концентратор Cisco VPN 5000 с программным обеспечением для концентратора VPN 5000 версии 5.2.19

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

## Схема сети

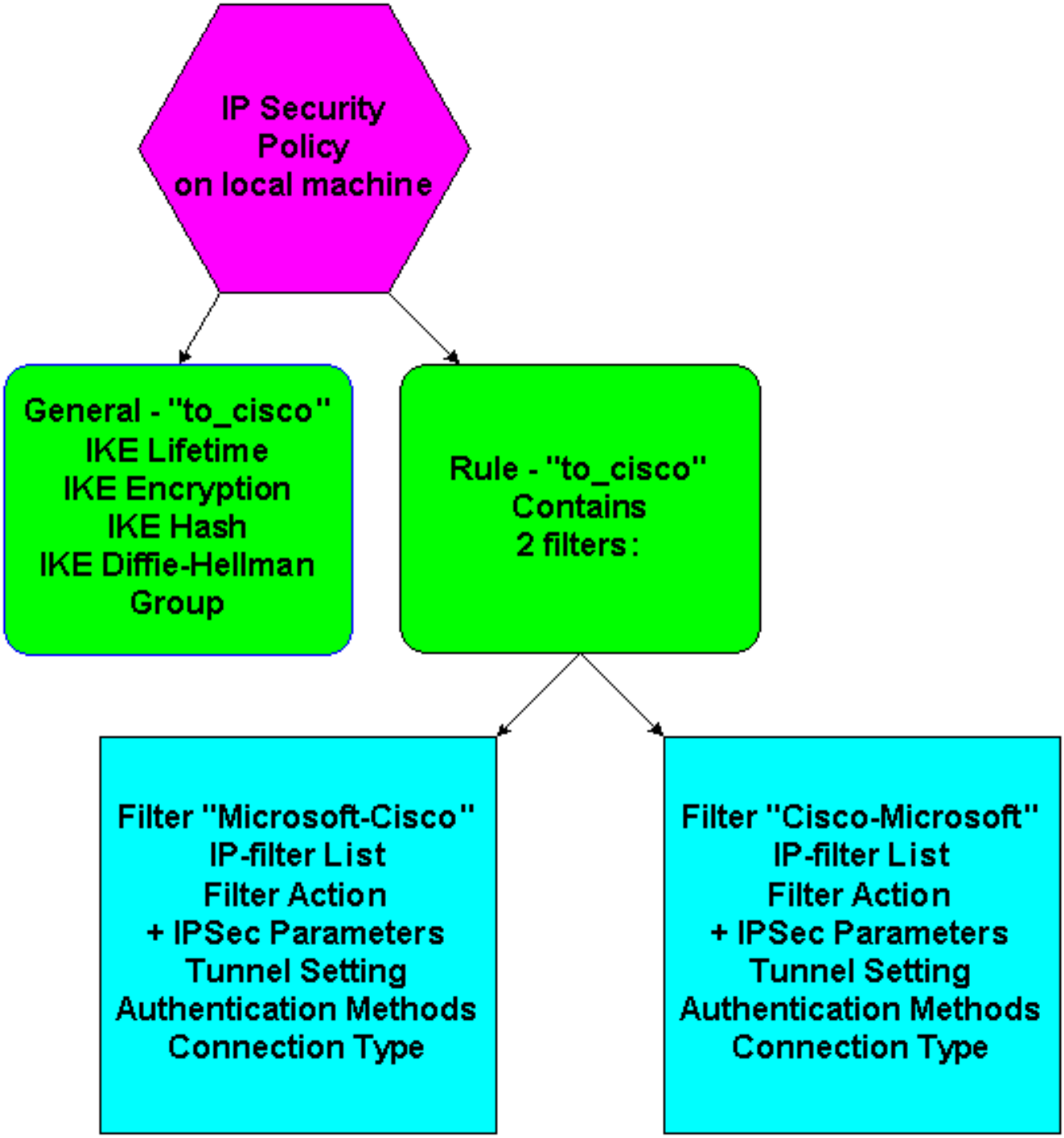
В данном документе используется сетевая установка, показанная на следующей схеме.




# Настройка сервера Microsoft Windows 2000 для работы с устройствами Cisco

## Выполненные задачи

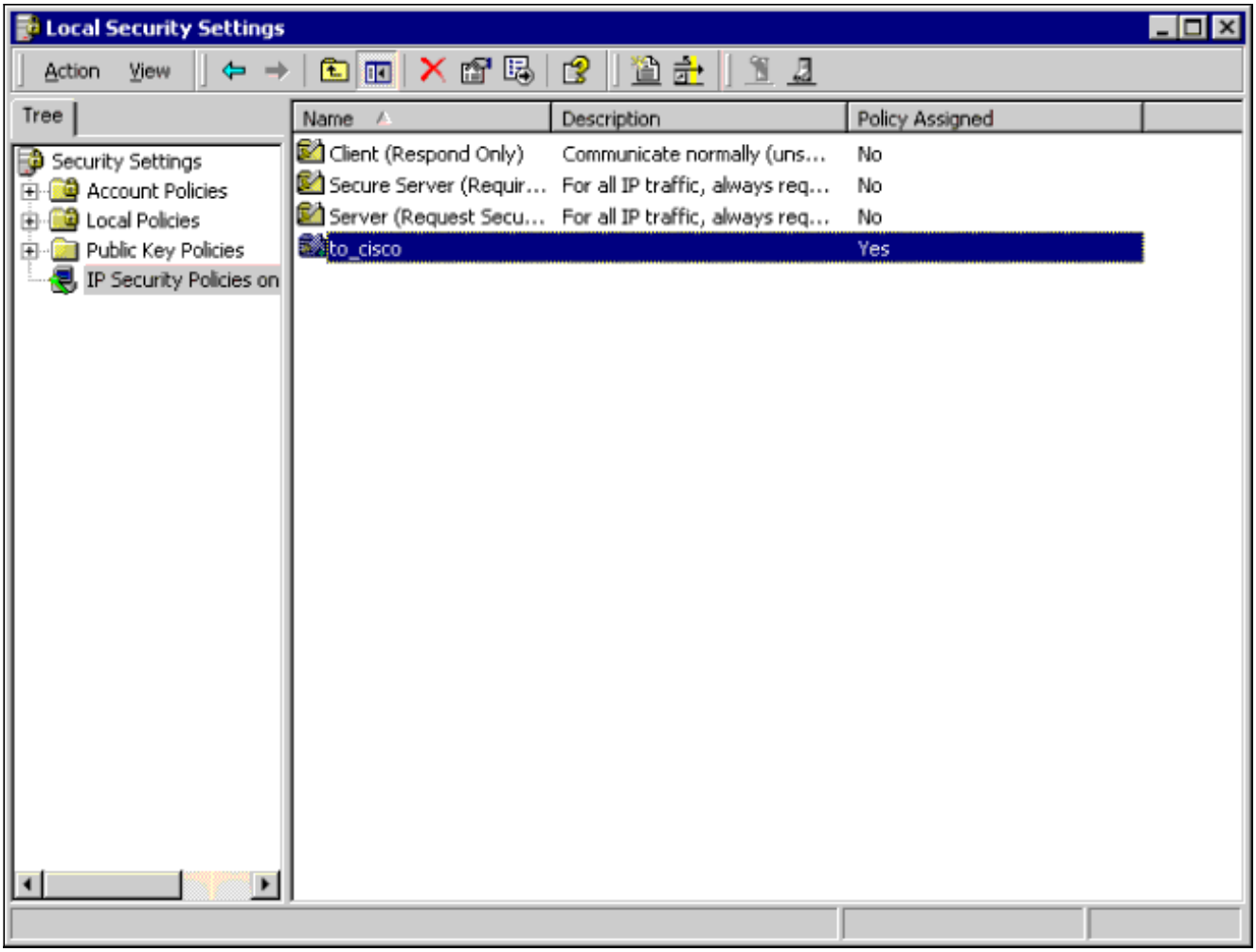
На схеме показаны задачи, которые выполняются в конфигурации сервера Microsoft Windows 2000:



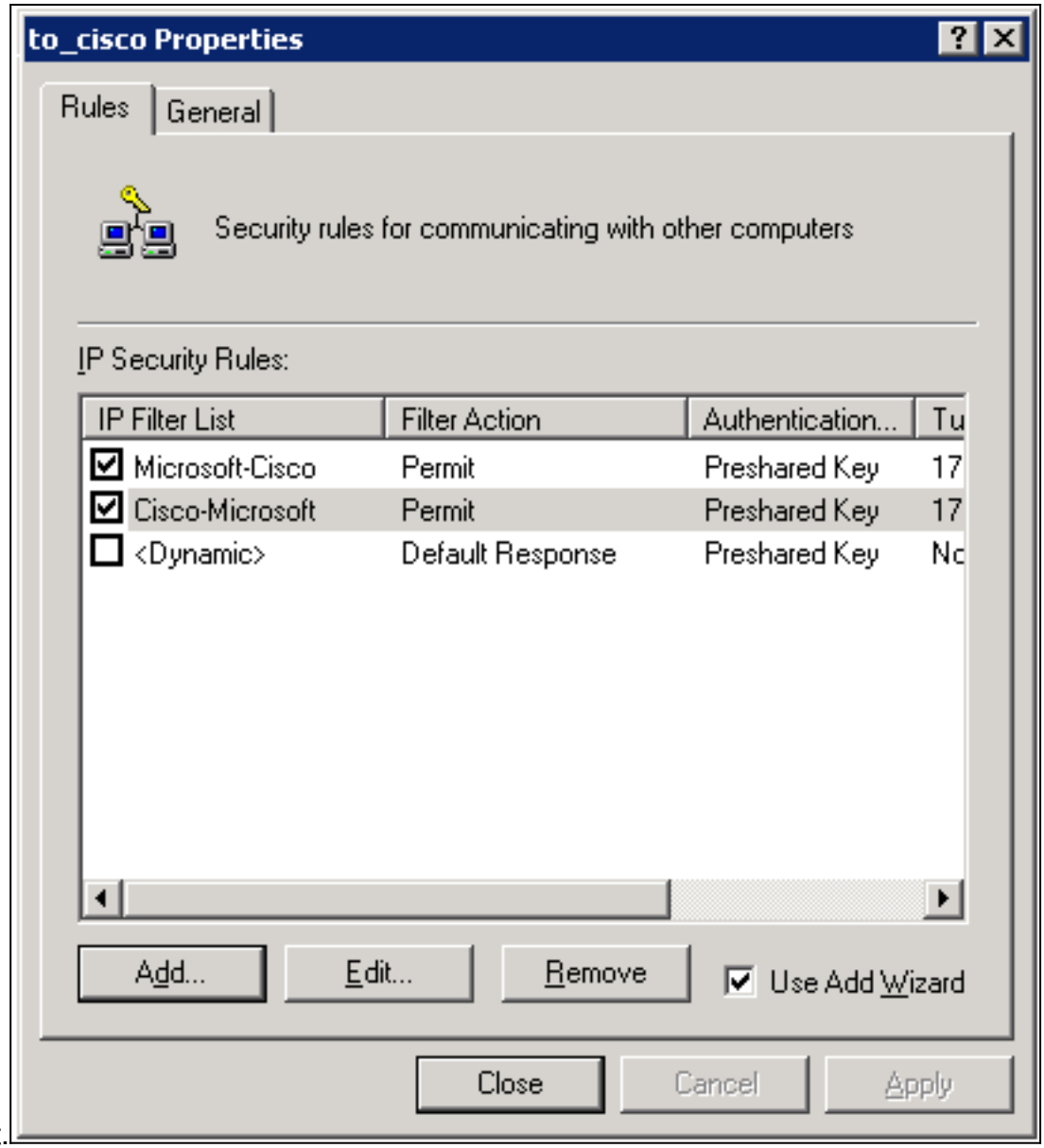

## Пошаговые инструкции

Как только вы начали следовать инструкциям по настройке на сайте Microsoft, используйте следующие шаги для проверки того, что ваша конфигурация может работать с устройствами Cisco. Комментарии и изменения указаны со снимками экрана.

1. **Нажмите кнопку Start > Run > secpol.msc в Microsoft Windows 2000 Server и проверьте данные на следующих экранах.**После того, как инструкции по узлу Веб-узла Microsoft использовались для настройки сервера 2000, следующие сведения о туннеле были отображены.**Примечание:** Пример правила назван «to_cisco».

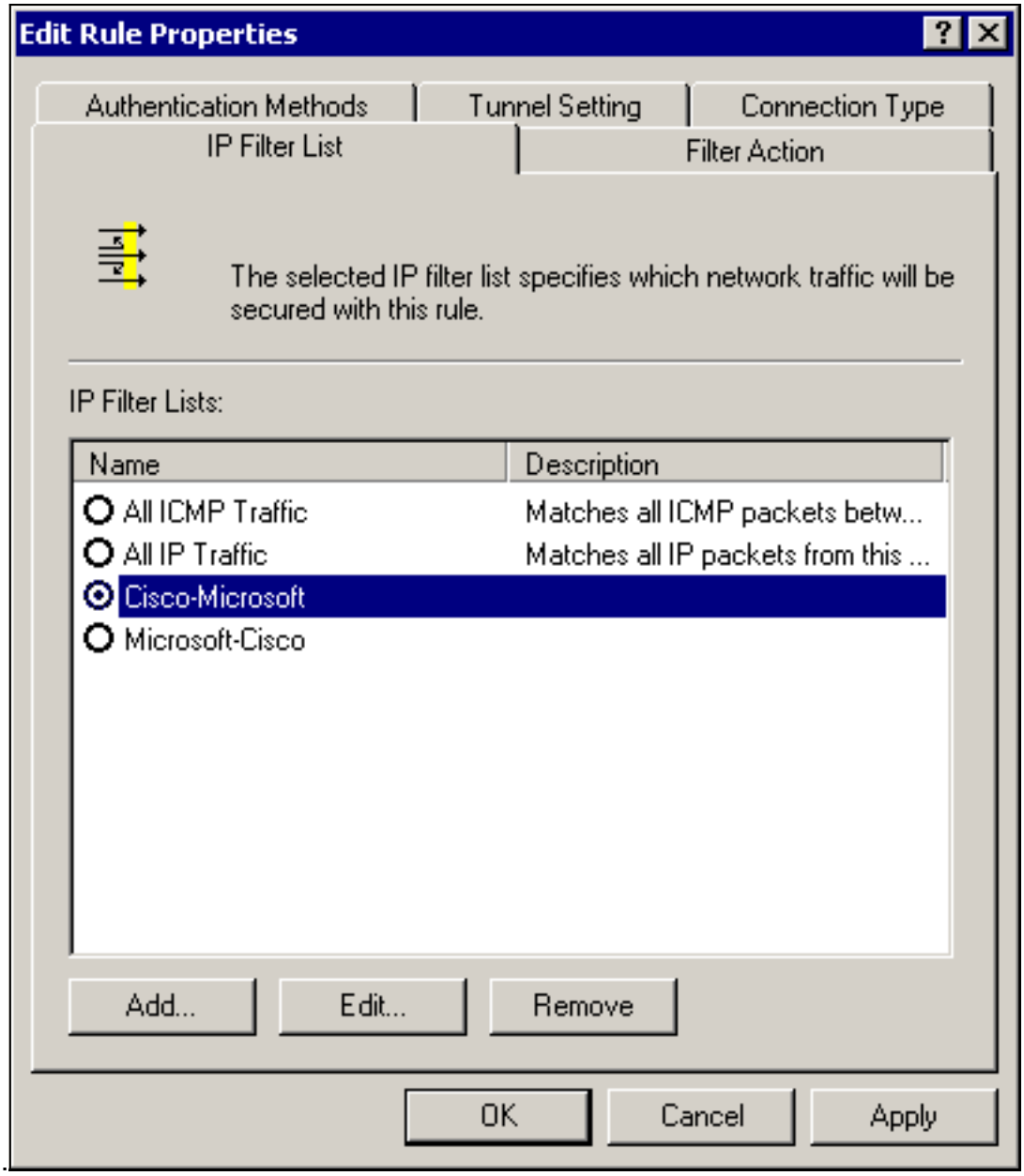



2. Правило данного примера содержит два фильтра: Microsoft-Cisco и Cisco-



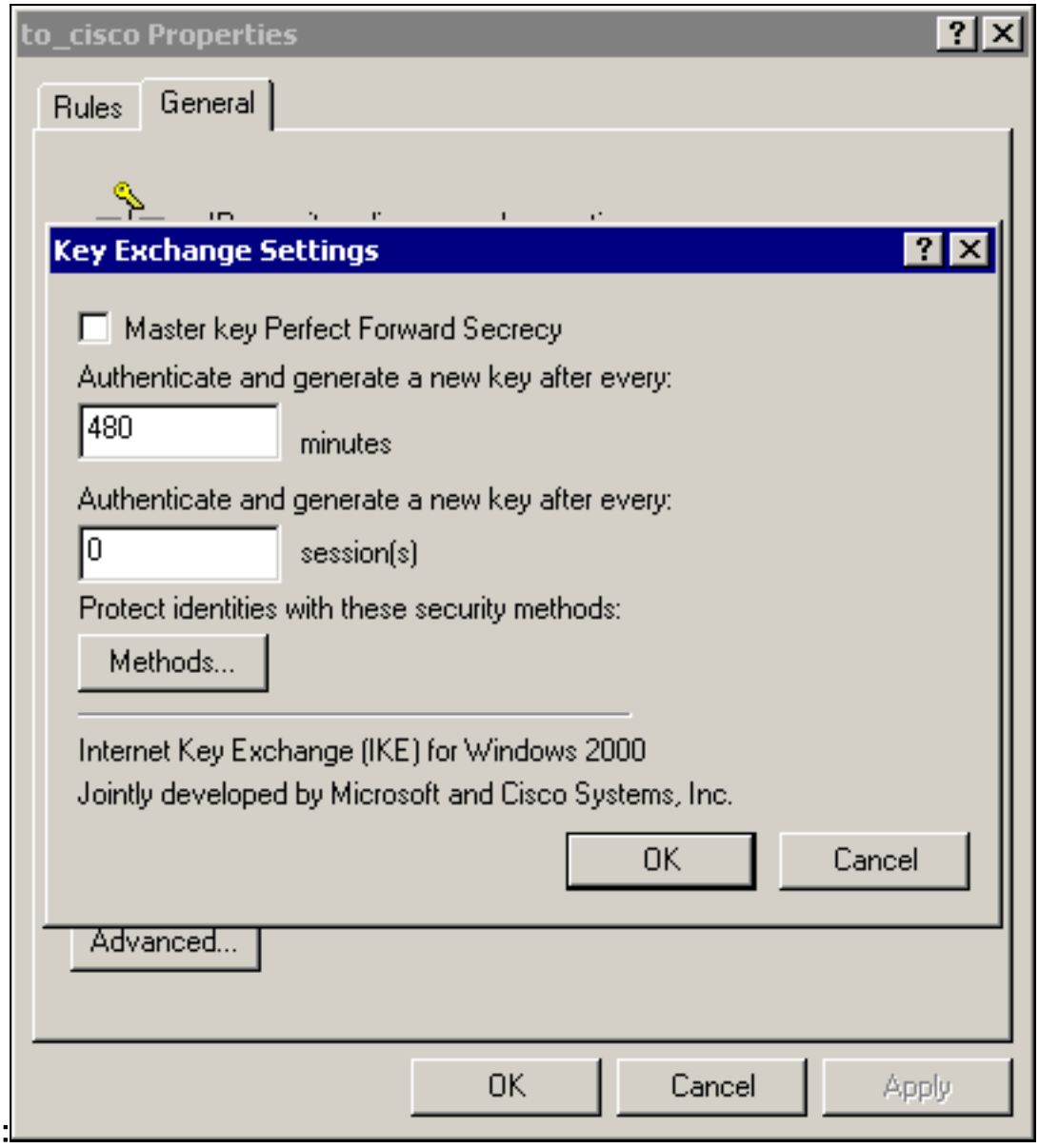

Microsoft.

3. Выберите Cisco-Microsoft IP Security Rule, затем нажмите **Edit** для просмотра Списков



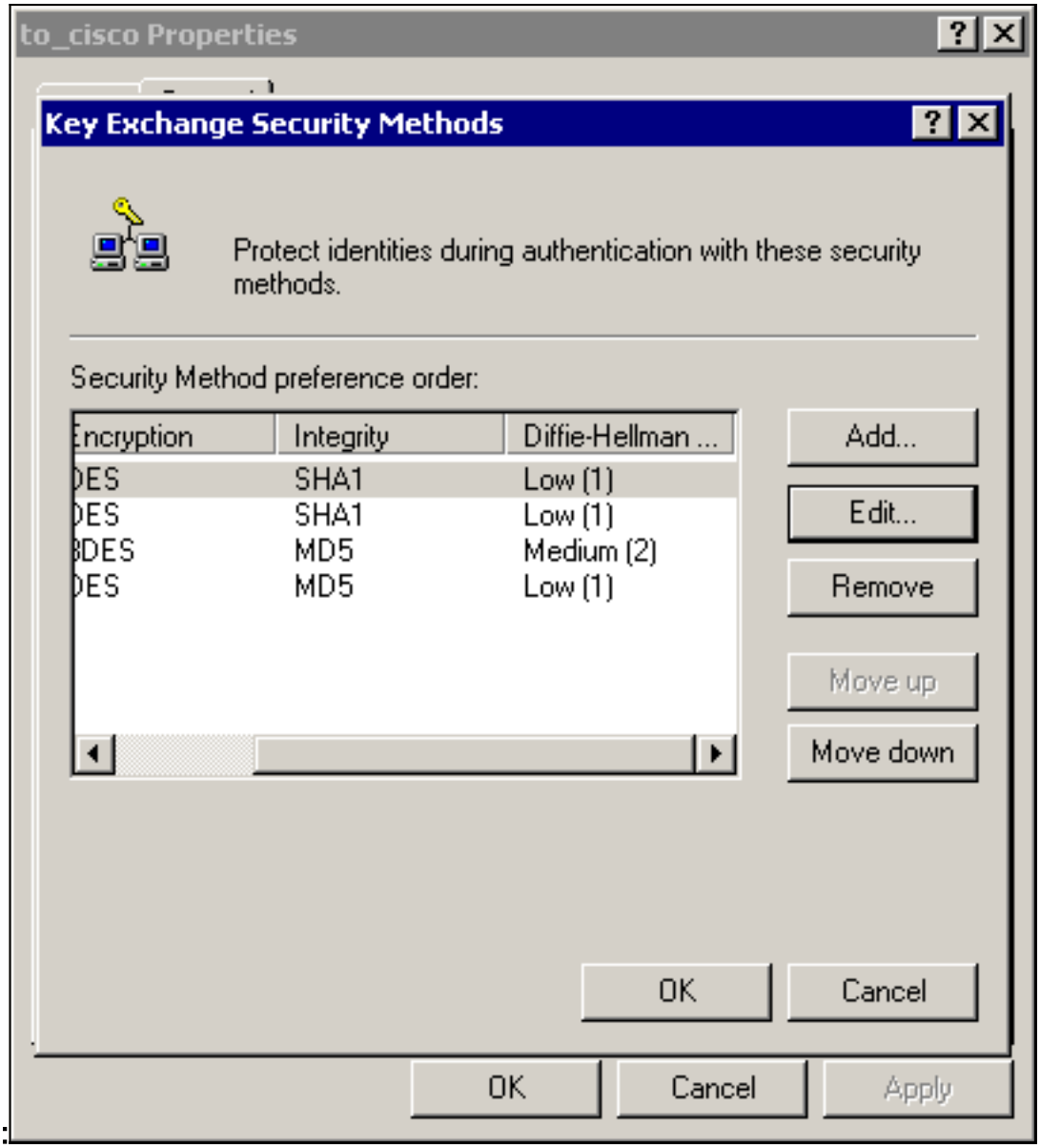

Фильтра IP.

4. **На вкладке "Общее > Расширенное" для этого правила указано время существования IKE (480 минут = 28800**



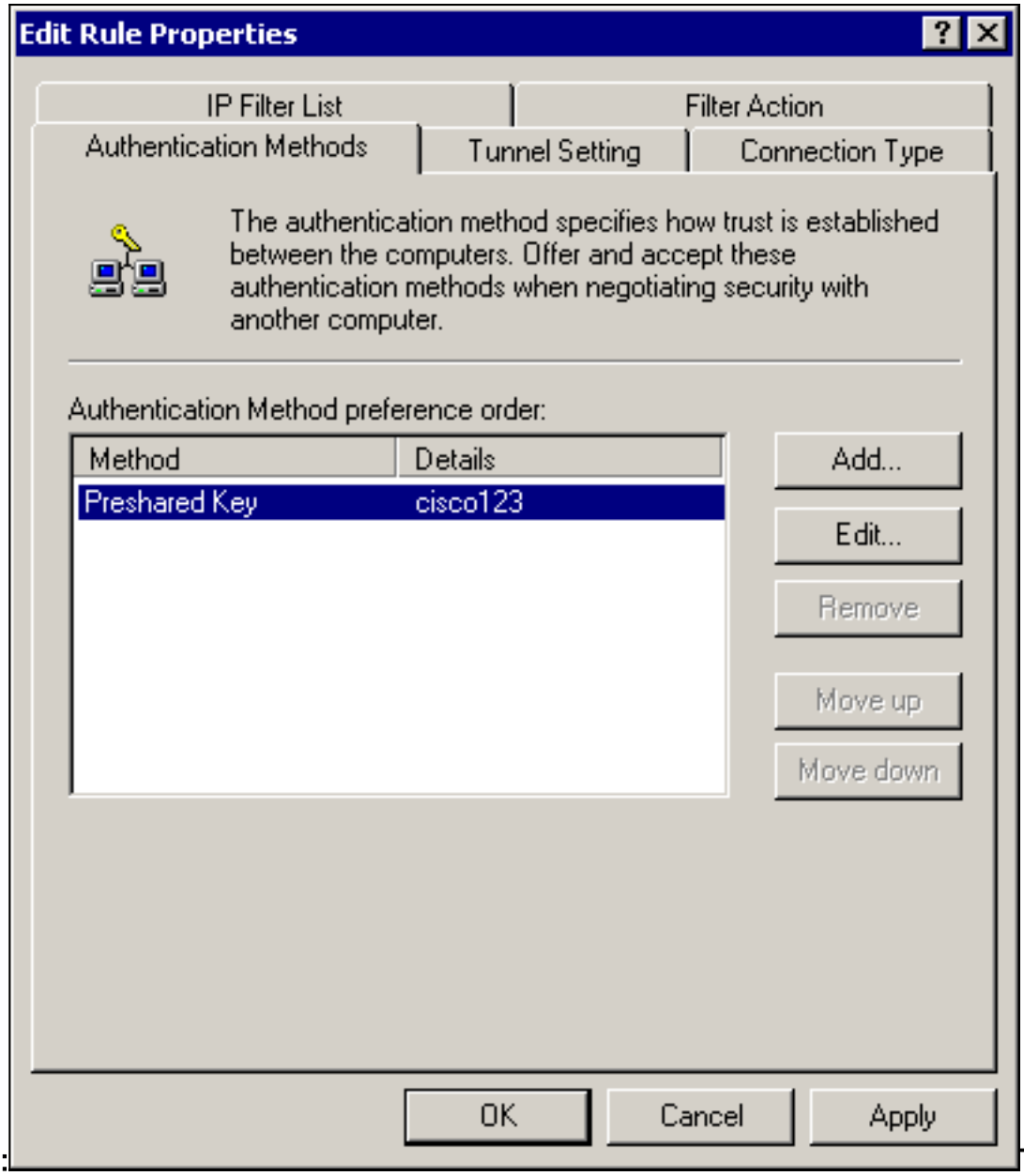

секунд):

5. На вкладке правил General > Advanced > Methods (Общие > Дополнительно > Методы) имеется метод IKE-шифрования (DES), IKE-хеширования (SHA1) и группировки Диффи-Хермана

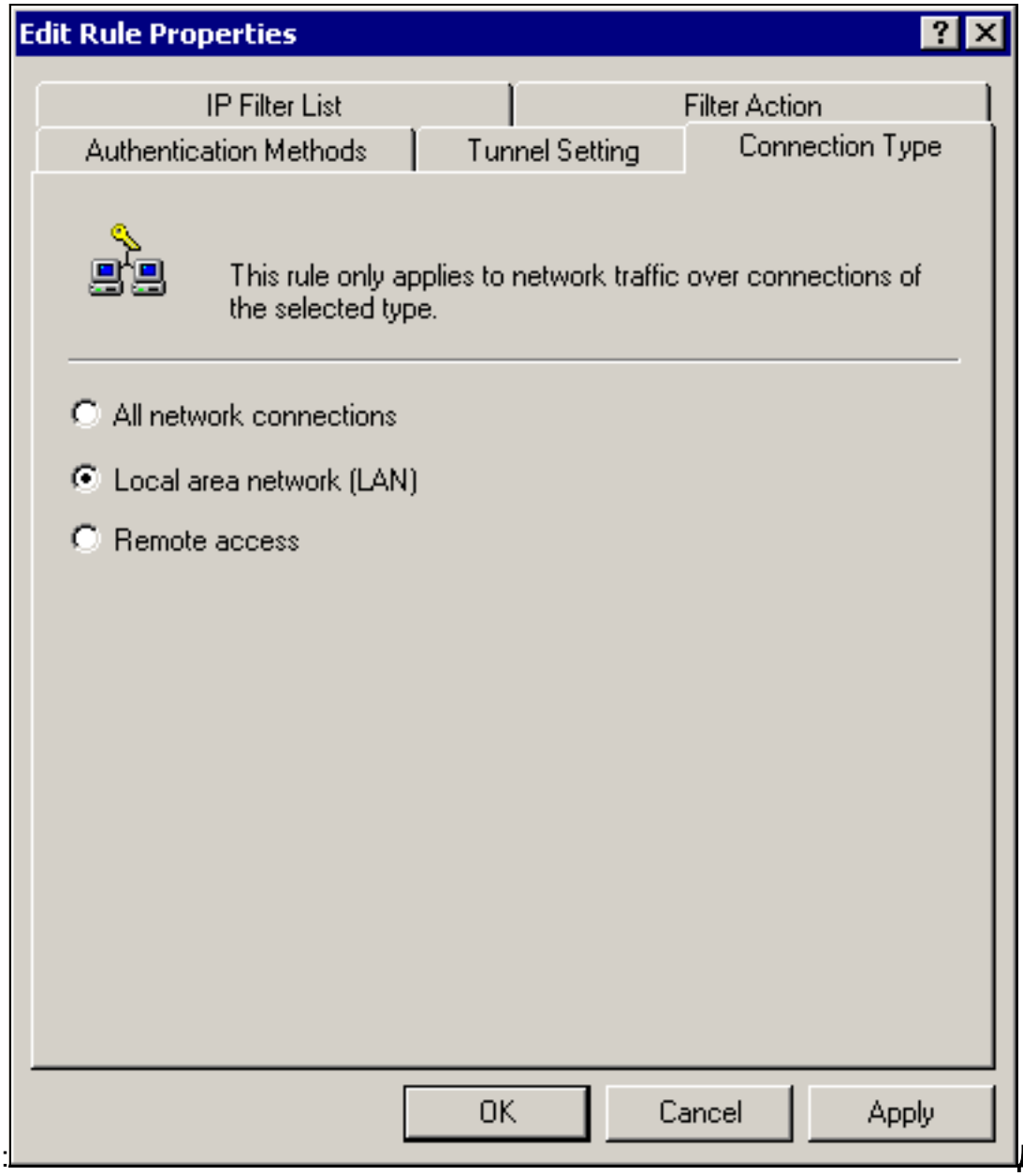



(Low(1)):

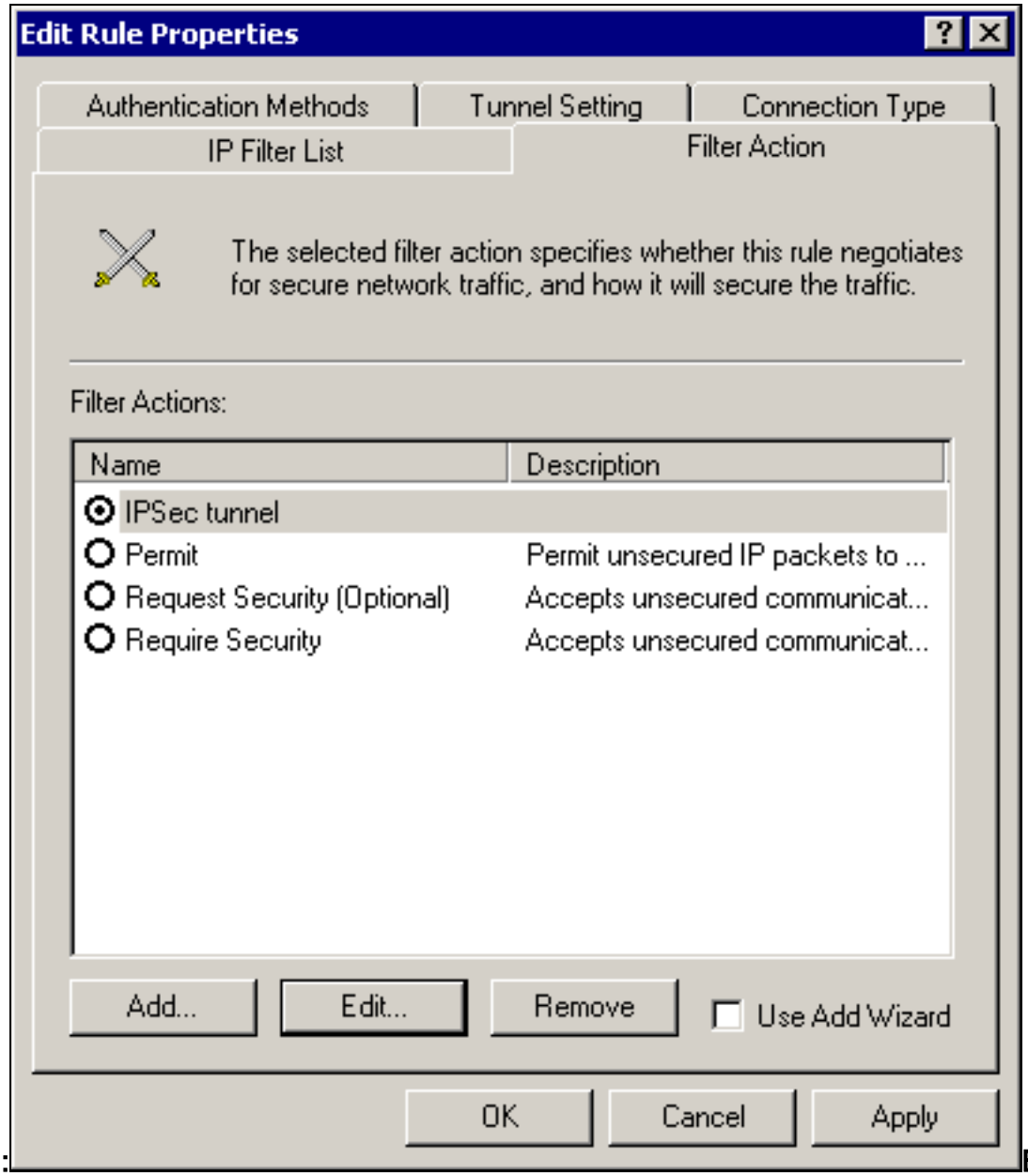
6. Каждый фильтр имеет 5 вкладок:**Способы проверки подлинности (Предварительно разрешенные для общего доступа ключи для обмена ключами по Интернету**



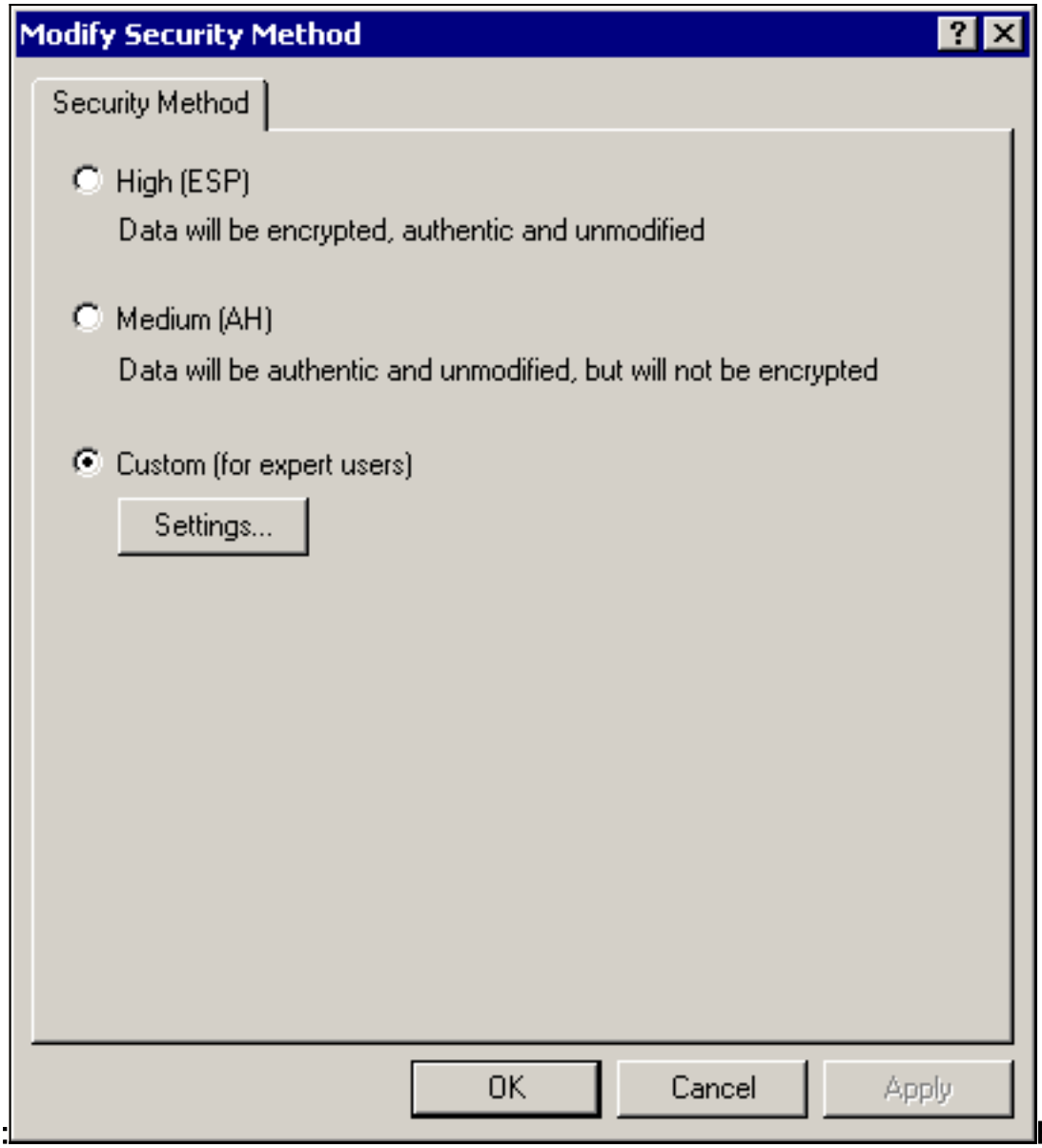

**[IKE]): Тип соединения**



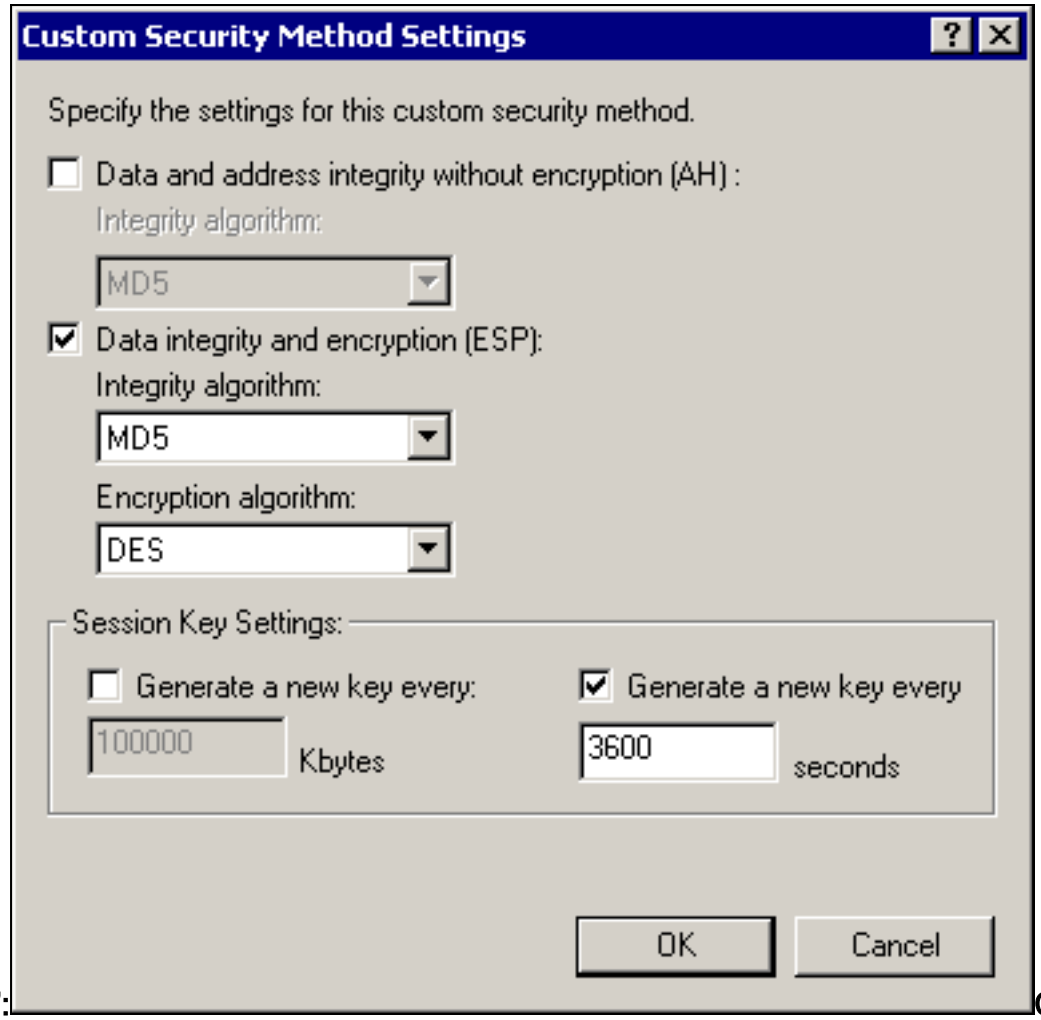

(LAN):**Действие фильтра**



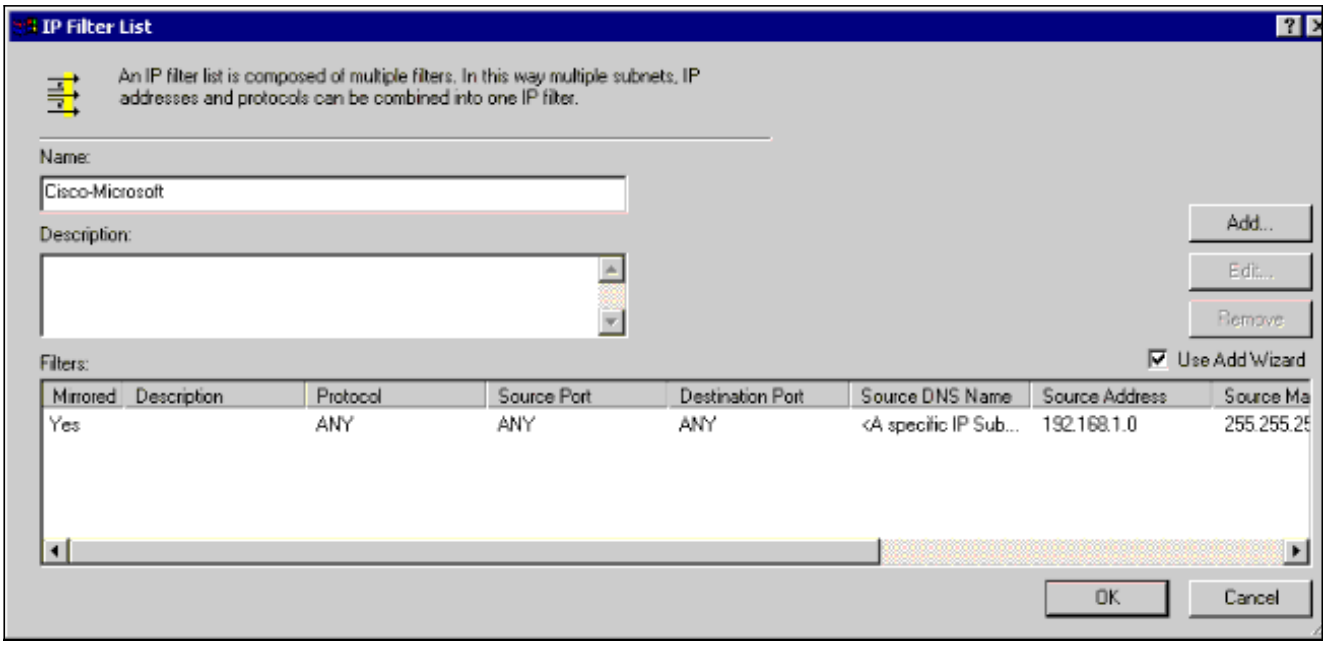

(IPSec): Выберите Filter Action > IPSec tunnel > Edit > Edit (Действие фильтрации > Туннель IPSec > Правка > Правка) и нажмите Custom



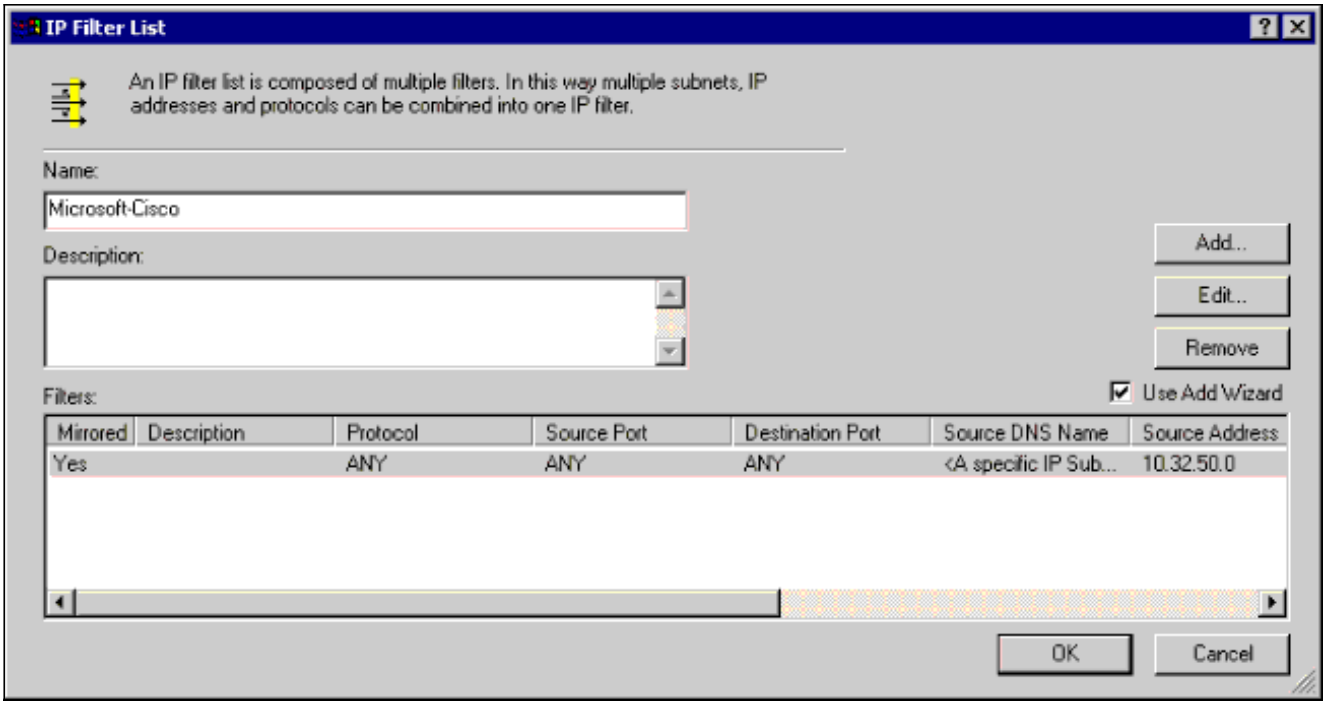

(Заказной): Выберите "Настройки" - "Преобразования IPSec и срок существования



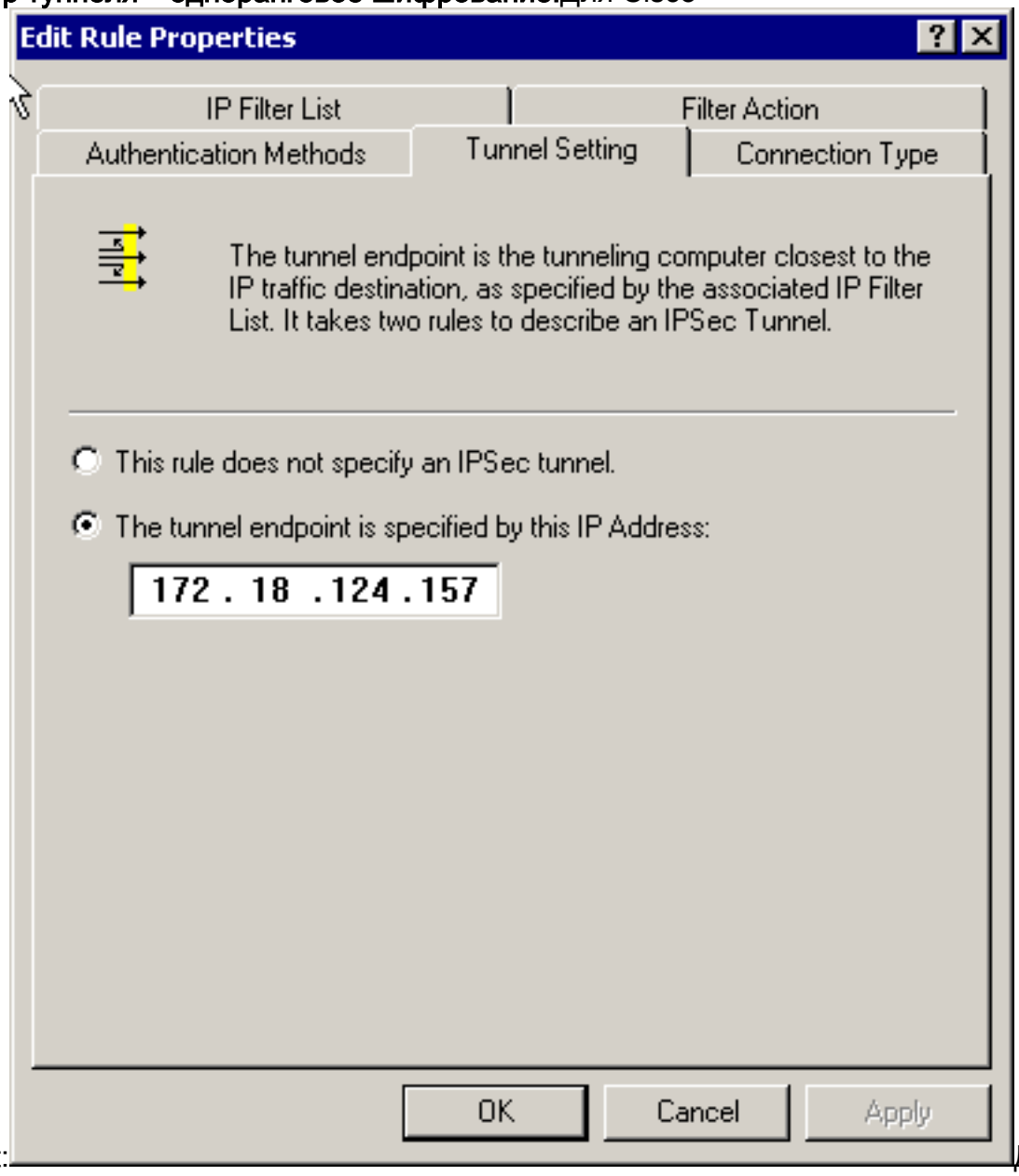

**IPSec":** **Список Фильтра IP - источник** и **сети назначения**, которые будут зашифрованы:Для Cisco-Microsoft:




Для Microsoft-Cisco:

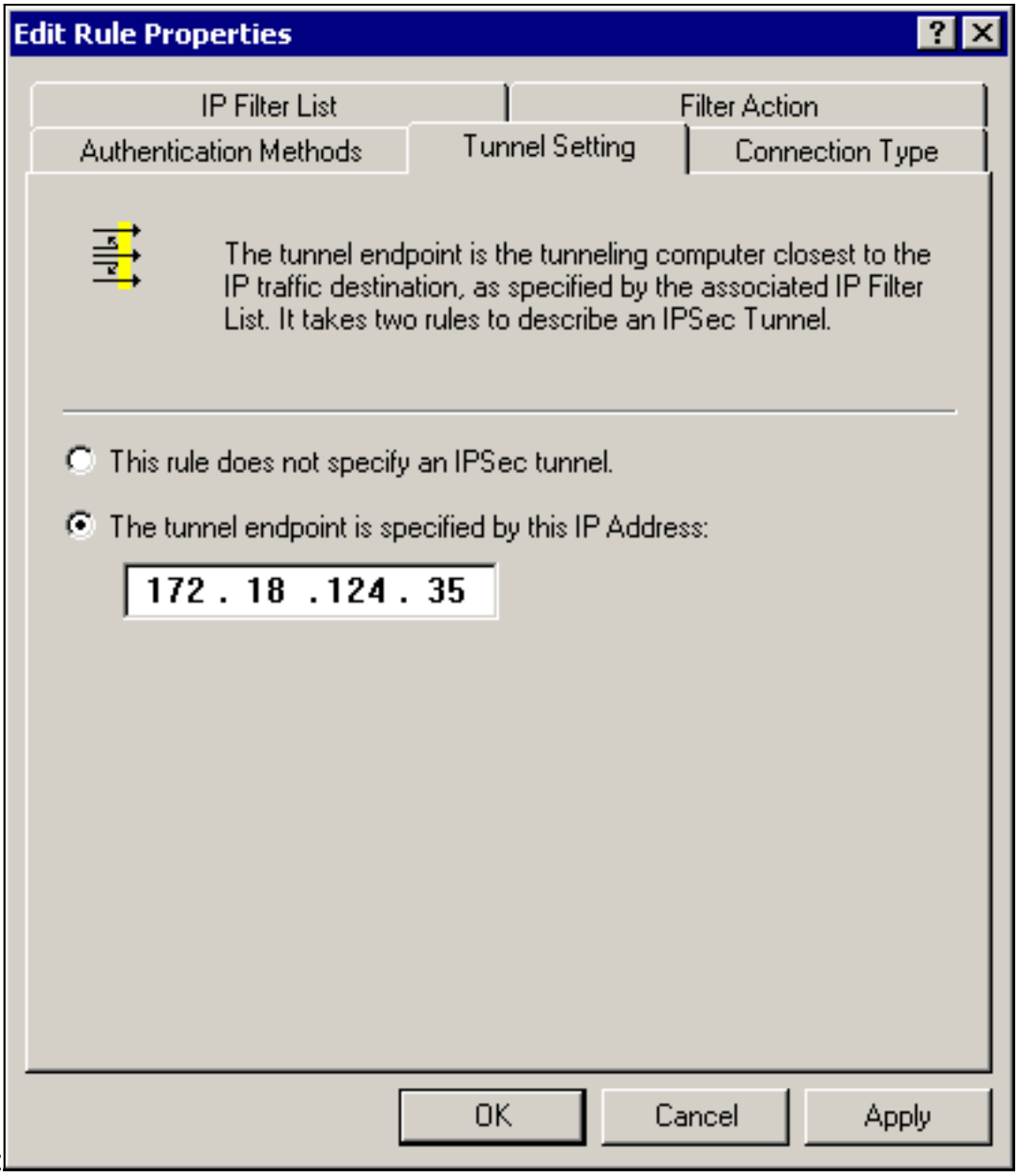



**Параметр туннеля – одноранговое шифрование:**Для Cisco-Microsoft:




Для

Microsoft-Cisco:




## Конфигурация устройств Cisco

Настройте маршрутизатор Cisco, PIX и Концентраторы VPN как показано в примерах ниже.

- Маршрутизатор Cisco 3640
- PIX
- Концентратор VPN 3000
- Концентратор VPN 5000

### Настройка маршрутизатора Cisco 3640

| Маршрутизатор Cisco 3640 |
| --- |
| Current configuration : 1840 bytes!version 12.1no service single-slot-reload-enableservice timestamps debug uptimeservice timestamps log uptimeno service password-encryption!hostname moss!logging rate-limit console 10 except errors!ip subnet-zero!no ip finger!ip audit notify logip audit po max-events 100!**crypto isakmp** |

```
policy 1!--- The following are IOS defaults so they do
not appear: !--- IKE encryption methodencryption des!---
IKE hashinghash sha!--- Diffie-Hellman groupgroup 1!---
Authentication methodauthentication pre-share!--- IKE
lifetimelifetime 28800!--- encryption peercrypto isakmp
key cisco123 address 172.18.124.157!!--- The following
is the IOS default so it does not appear: !--- IPSec
lifetimecrypto ipsec security-association lifetime
seconds 3600!!--- IPSec transformscrypto ipsec
transform-set rtpset esp-des esp-md5-hmac !crypto map
rtp 1 ipsec-isakmp !--- Encryption peerset peer
172.18.124.157set transform-set rtpset !---
Source/Destination networks definedmatch address
115!call rsvp-sync!interface Ethernet0/0ip address
192.168.1.1 255.255.255.0ip nat insidehalf-
duplex!interface Ethernet0/1ip address 172.18.124.35
255.255.255.240ip nat outsidehalf-duplexcrypto map
rtp!ip nat pool INTERNET 172.18.124.35 172.18.124.35
netmask 255.255.255.240ip nat inside source route-map
nonat pool INTERNETip classlessip route 0.0.0.0 0.0.0.0
172.18.124.36no ip http server!access-list 101 deny ip
192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255access-list
101 permit ip 192.168.1.0 0.0.0.255 any!---
Source/Destination networks definedaccess-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255access-list 115 deny ip 192.168.1.0 0.0.0.255
anyroute-map nonat permit 10match ip address 101!line
con 0transport input noneline 65 94line aux 0line vty 0
4!end
```

## Настройка PIX

**PIX**

```
PIX Version 5.2(1)nameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname pixfirewallfixup
protocol ftp 21fixup protocol http 80fixup protocol h323
1720fixup protocol rsh 514fixup protocol smtp 25fixup
protocol sqlnet 1521fixup protocol sip 5060names!---
Source/Destination networks definedaccess-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 24logging onno logging
timestampno logging standbyno logging consoleno logging
monitorno logging bufferedno logging trapno logging
historylogging facility 20logging queue 512interface
ethernet0 autointerface ethernet1 10basetmtu outside
1500mtu inside 1500ip address outside 172.18.124.35
255.255.255.240ip address inside 192.168.1.1
255.255.255.0ip audit info action alarmip audit attack
action alarmno failoverfailover timeout 0:00:00failover
poll 15failover ip address outside 0.0.0.0failover ip
address inside 0.0.0.0arp timeout 14400!--- Except
Source/Destination from Network Address Translation
(NAT):nat (inside) 0 access-list 115route outside
0.0.0.0 0.0.0.0 172.18.124.36 1timeout xlate
3:00:00timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h323 0:05:00sip 0:30:00 sip_media
0:02:00timeout uauth 0:05:00 absoluteaaa-server TACACS+
protocol tacacs+ aaa-server RADIUS protocol radius no
snmp-server locationno snmp-server contactsnmp-server
```

```
community publicno snmp-server enable trapsfloodguard
enablesysopt connection permit-ipsecno sysopt route
dnat!--- IPSec transformscrypto ipsec transform-set
myset esp-des esp-md5-hmac !--- IPSec lifetimecrypto
ipsec security-association lifetime seconds 3600crypto
map rtpmap 10 ipsec-isakmp!--- Source/Destination
networkscrypto map rtpmap 10 match address 115!---
Encryption peercrypto map rtpmap 10 set peer
172.18.124.157 crypto map rtpmap 10 set transform-set
mysetcrypto map rtpmap interface outsideisakmp enable
outside!--- Encryption peerisakmp key ******** address
172.18.124.157 netmask 255.255.255.240 isakmp identity
address!--- Authentication methodisakmp policy 10
authentication pre-share!--- IKE encryption methodisakmp
policy 10 encryption des!--- IKE hashingisakmp policy 10
hash sha!--- Diffie-Hellman groupisakmp policy 10 group
1!--- IKE lifetimeisakmp policy 10 lifetime 28800telnet
timeout 5ssh timeout 5terminal width
80Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08: end
```

## Настройка концентратора VPN 3000

Используйте опции меню и параметры, которые, как показывают ниже, настраивали Концентратор VPN по мере необходимости.

- **Чтобы добавить предложение IKE, выберите Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Add a proposal.**Proposal Name = DES-SHA!--- Authentication methodAuthentication Mode = Preshared Keys!--- IKE hashingAuthentication Algorithm = SHA/HMAC-160!--- IKE encryption methodEncryption Algorithm = DES-56!--- Diffie-Hellman groupDiffie Hellman Group = Group 1 (768-bits) Lifetime Measurement = TimeDate Lifetime = 10000!--- IKE lifetimeTime Lifetime = 28800
- Для определения туннеля между локальными сетями (LAN-to-LAN) выберите **Configuration> System> Tunneling Protocols> IPSec LAN-to-LAN.**Name = to_2000Interface = Ethernet 2 (Public) 172.18.124.35/28!--- Encryption peerPeer = 172.18.124.157!--- Authentication methodDigital Certs = none (Use Pre-shared Keys)Pre-shared key = cisco123!--- IPSec transformsAuthentication = ESP/MD5/HMAC-128Encryption = DES-56!--- Use the IKE proposalIKE Proposal = DES-SHAAutodiscovery = off!--- Source network definedLocal Network Network List = Use IP Address/Wildcard-mask belowIP Address 192.168.1.0Wildcard Mask = 0.0.0.255!--- Destination network definedRemote NetworkNetwork List = Use IP Address/Wildcard-mask belowIP Address 10.32.50.0 Wildcard Mask 0.0.0.255
- Для изменения сопоставления безопасности выберите **Configuration> Policy Management> Traffic Management> Security Associations> Modify.**SA Name = L2L-to_2000Inheritance = From RuleIPSec Parameters!--- IPSec transformsAuthentication Algorithm = ESP/MD5/HMAC-128Encryption Algorithm = DES-56Encapsulation Mode = TunnelPFS = DisabledLifetime Measurement = TimeData Lifetime = 10000!--- IPSec lifetimeTime Lifetime = 3600Ike Parameters!--- Encryption peerIKE Peer = 172.18.124.157Negotiation Mode = Main!--- Authentication methodDigital Certificate = None (Use Preshared Keys)!--- Use the IKE proposalIKE Proposal DES-SHA

## Настройка концентратора VPN 5000

**Концентратор VPN 5000**

```
[ IP Ethernet 1:0 ]Mode = RoutedSubnetMask =
255.255.255.240IPAddress = 172.18.124.35[ General
]IPSecGateway = 172.18.124.36DeviceName =
"cisco"EthernetAddress = 00:00:a5:f0:c8:00DeviceType =
VPN 5002/8 ConcentratorConfiguredOn = Timeserver not
configuredConfiguredFrom = Command Line, from Console[
```

```
IP Ethernet 0:0 ]Mode = RoutedSubnetMask =
255.255.255.0IPAddress = 192.168.1.1[ Tunnel Partner VPN
1 ]!--- Encryption peerPartner = 172.18.124.157!---
IPSec lifetimeKeyLifeSecs = 3600BindTo = "ethernet
1:0"!--- Authentication methodSharedKey =
"cisco123"KeyManage = Auto!--- IPSec transformsTransform
= esp(md5,des)Mode = Main!--- Destination network
definedPeer = "10.32.50.0/24"!--- Source network
definedLocalAccess = "192.168.1.0/24"[ IP Static
]10.32.50.0 255.255.255.0 VPN 1 1[ IP VPN 1 ]Mode =
RoutedNumbered = Off[ IKE Policy ]!--- IKE hashing,
encryption, Diffie-Hellman groupProtection =
SHA_DES_G1Configuration size is 1088 out of 65500 bytes.
```

# Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

# Устранение неполадок

Этот раздел предоставляет сведения, можно использовать для устранения проблем конфигураций.

## Команды для устранения неполадок

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

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

### Маршрутизатор Cisco 3640

- **debug crypto engine-** Показывает сообщения отладки о ядрах шифрования, которые выполняют шифрование и расшифровку.
- **команда debug crypto isakmp отображает сообщения о событиях IKE.**
- **команда debug crypto ipsec – отображает события IPSec.**
- **show crypto isakmp sa — Показывает все текущие ассоциации безопасности (SA) протокола IKE для узла.**
- **show crypto ipsec sa – отображает текущие настройки связей безопасности.**
- **clear crypto isakmp-** (от режима конфигурации), Очищает все соединения активного предложения IKE.
- **clear crypto sa - (из режима конфигурации) удаляет все сопоставления безопасности IPSec.**

### PIX

- **команда debug crypto ipsec отображает согласование IPSec на втором этапе.**
- **debug crypto isakmp– показывает согласование протокола ISAKMP (протокол**

управления ассоциациями безопасности и ключами в Интернете) на 1-м этапе.
- "debug crypto engine" - отображается зашифрованный трафик.
- команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.
- команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.
- clear crypto isakmp – (из режима конфигурации) Удаляет связи безопасности Internet Key Exchange (IKE).
- clear crypto ipsec sa - (от режима конфигурации), Очищает Сопоставления безопасности IPSec.

[Концентратор VPN 3000]

- Начните отладку концентратора VPN 3000, выбрав пункт Configuration > System > Events > Classes (Severity to Log=1-13, Severity to Console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - Журнал событий может быть очищен с помощью выбора команды Monitoring > Event Log.
- - Туннельный трафик между локальными сетями можно просмотреть в меню Monitoring > Sessions.
- - Туннель может быть очищен на Administration> Administer Sessions>> Actions - Logout сеансов между локальными сетями.

[Концентратор VPN 5000]

- команда vpn trace dump all – отображает сведения о всех соответствующих подключениях VPN, включая сведения о времени, числе VPN, фактический IP-адрес однорангового узла, какие сценарии запущены, а в случае ошибки – в какой подпрограмме и номере строки произошла ошибка.
- команда show vpn statistics отображает следующие данные для пользователей, партнеров и итог для обеих групп. (Для модульных моделей показ включает раздел для каждого модульного слота. Активные – активные в данный момент подключения. In Negot — В настоящий момент подключения согласуются. High Water - наибольшее число одновременных активных подключений с момента последней перезагрузки. Промежуточная сумма – общее число успешных подключений с момента последней перезагрузки. Tunnel Starts – число запускаемых туннелей. Tunnel OK – Количество туннелей, в которых не было ошибок. Tunnel Error – число туннелей с ошибками.
- show vpn statistics verbose: отображает статистику согласования ISAKMP и прочие статистические данные для активных соединений.

## Дополнительные сведения

- Объявление об окончании продажи концентраторов Cisco серии VPN 5000
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Техническая поддержка - Cisco Systems