在 Microsoft Windows 2000 服务器与 Cisco 设备之间配置 IPSec

目录

简介

本文档演示如何使用预共享密钥形成IPSec隧道以加入2个专用网络：思科设备内的专用网络(192.168.l.X)和Microsoft 2000服务器内的专用网络(10.32.50.X)。在开始此配置之前，我们假设从思科设备内部和2000服务器内部到Internet（以172.18.124.X网络表示）的流量正在流动。

您可以在Microsoft网站上找到有关配置Microsoft Windows 2000服务器的详细信息：http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

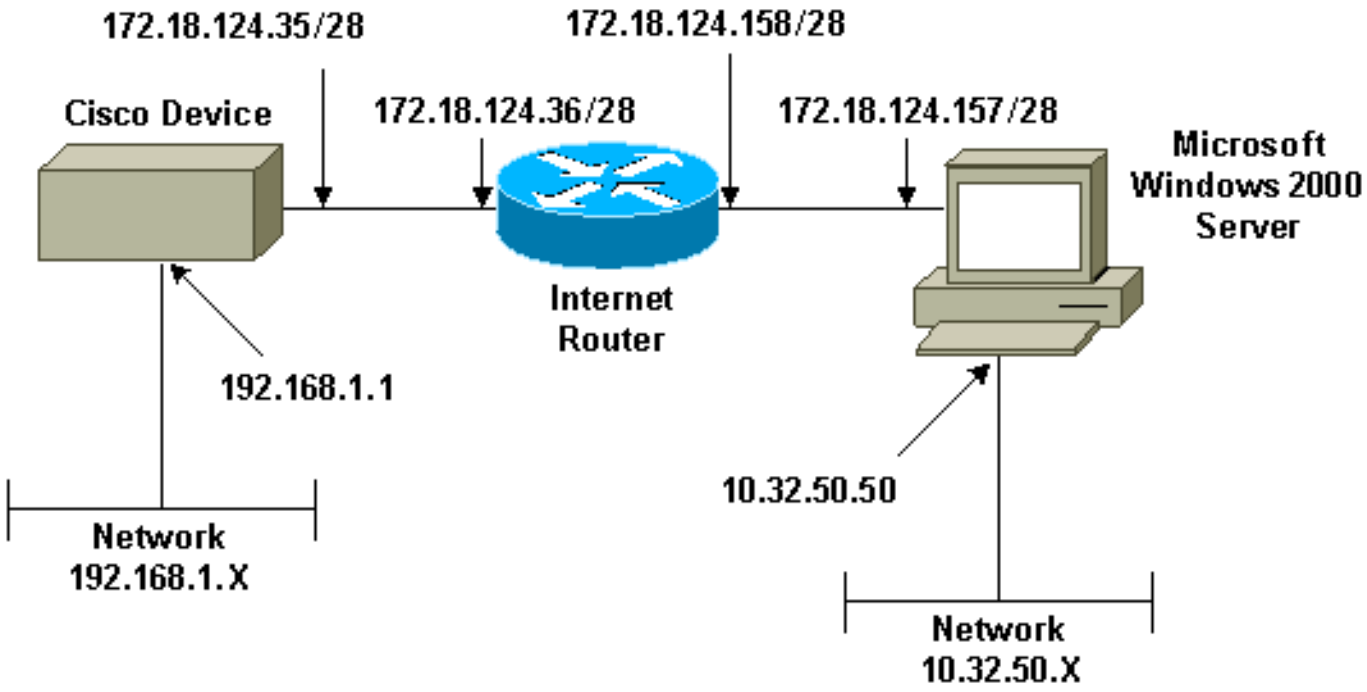
这些配置是使用以下软件和硬件版本开发和测试的。

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640路由器，带Cisco IOS®软件版本c3640-ik2o3s-mz.121-5.T.bin
- 带PIX软件版本5.2.1的思科安全PIX防火墙
- 带VPN 3000集中器软件版本2.5.2.F的Cisco VPN 3000集中器
- 带VPN 5000集中器软件版本5.2.19的Cisco VPN 5000集中器

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

网络图

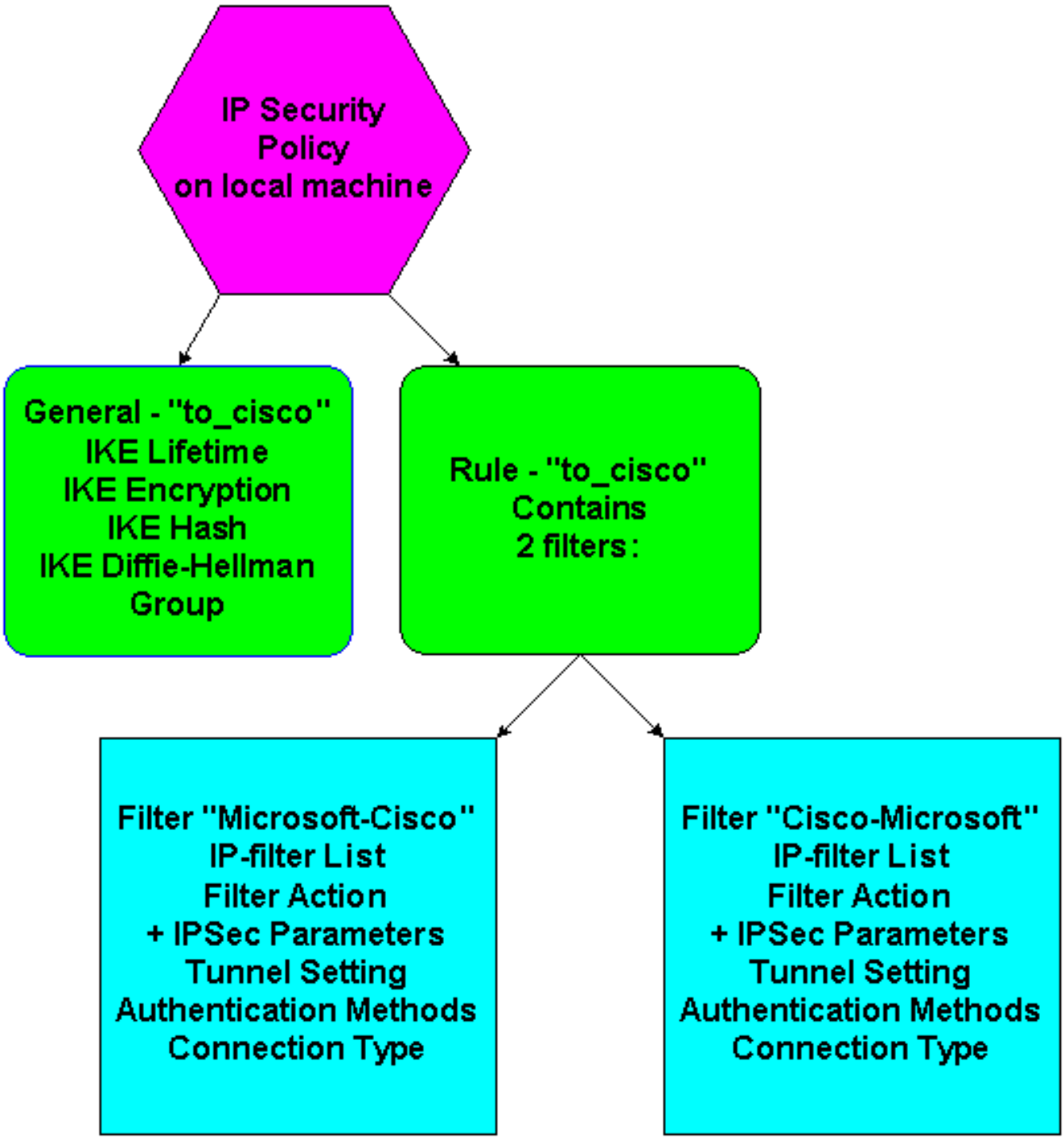
本文档使用下图所示的网络设置。



配置 Microsoft Windows 2000 服务器与 Cisco 设备一起运作

执行的任务

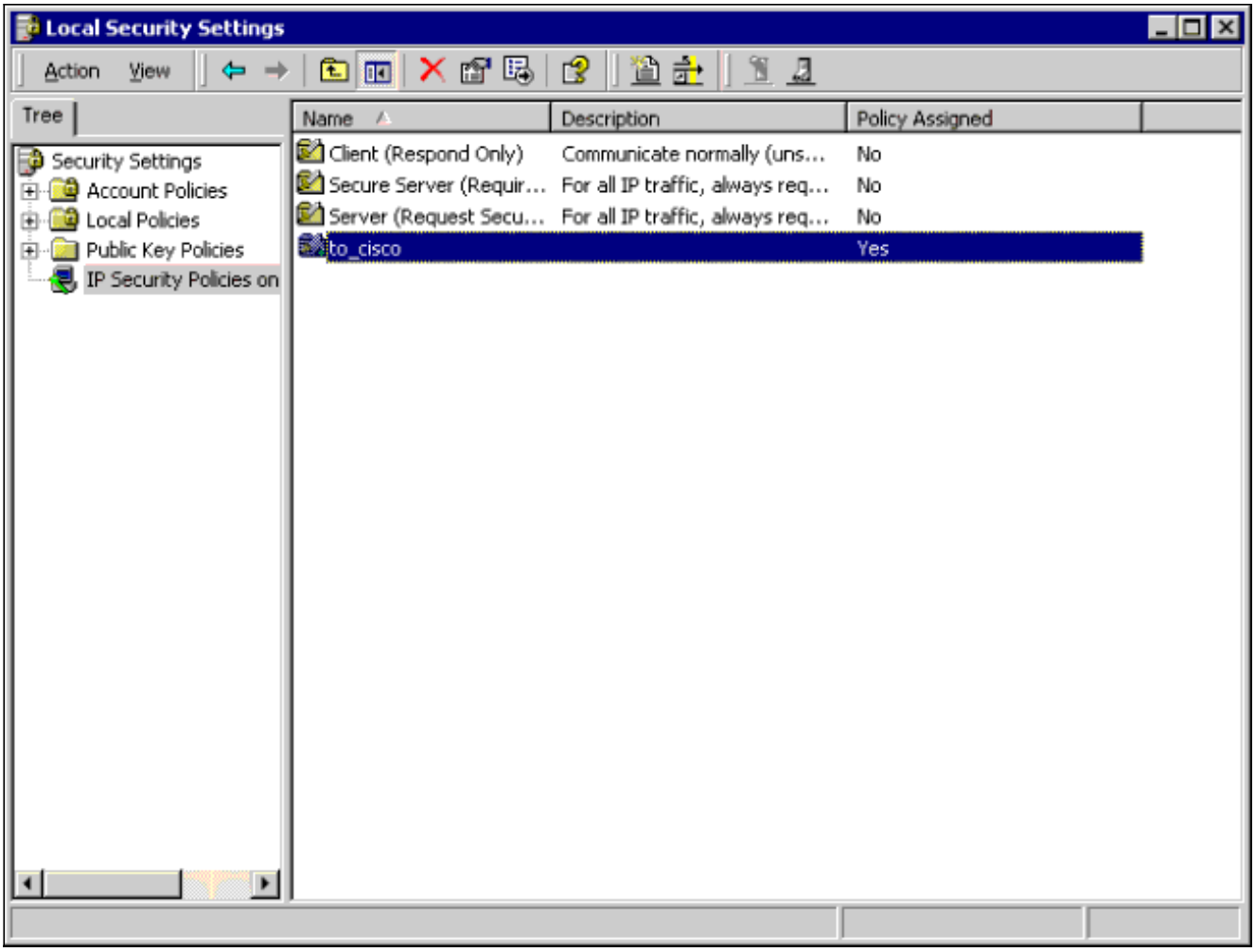
此图显示了在Microsoft Windows 2000服务器配置中执行的任务：



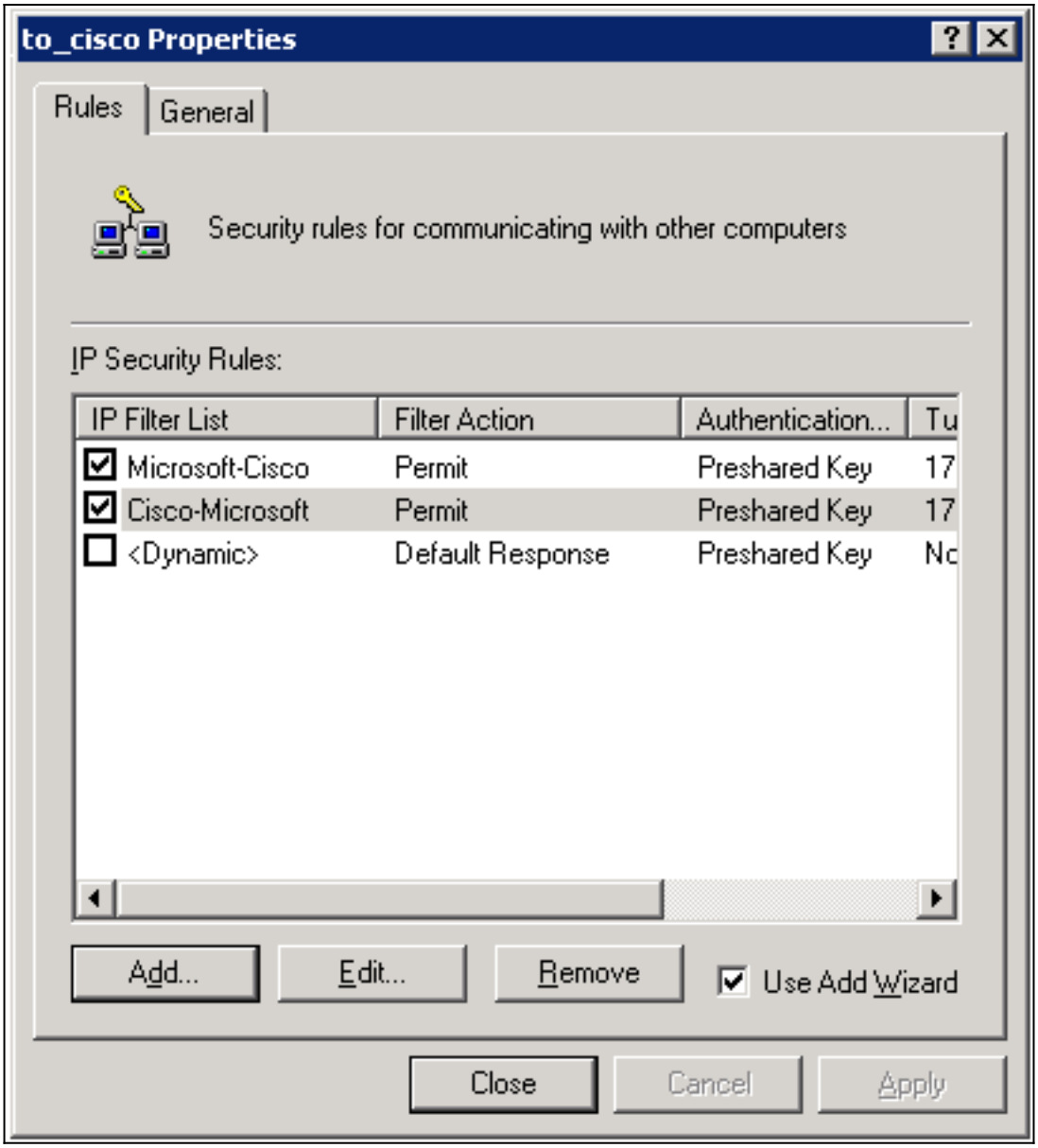
逐步指导

在Microsoft网站上按照 配置说明操作后，请使用以下步骤验证您的配置是否可以与Cisco设备配合使用。注释和更改会与屏幕截图一起记录。

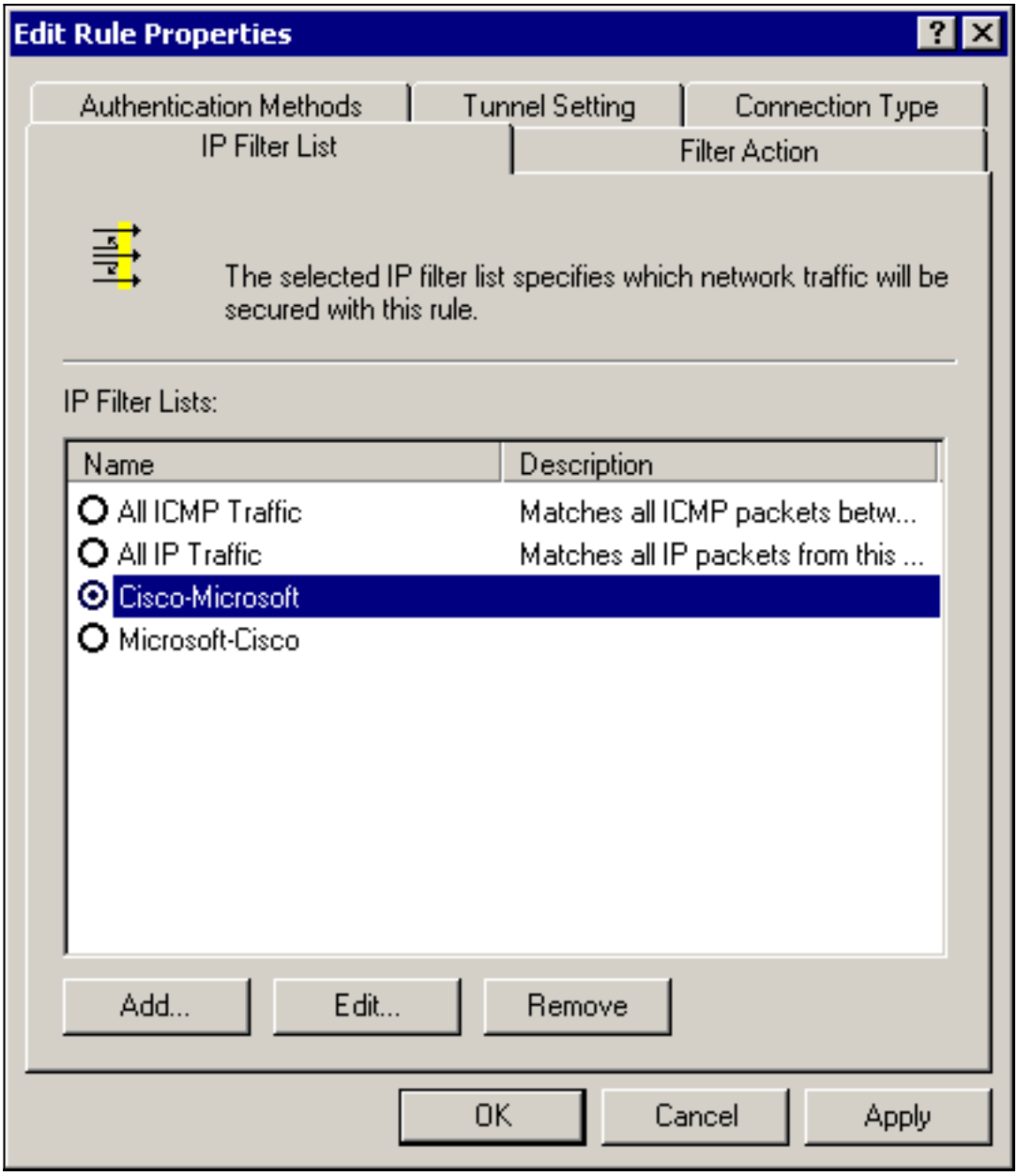
1. 在Microsoft Windows 2000 Server上单击**开始>运行> secpol.msc**，然后验证以下屏幕上的信息。使用Microsoft网站上的说明配置2000服务器后，将显示以下隧道信息。**注意：**示例规则称为“to_cisco”。



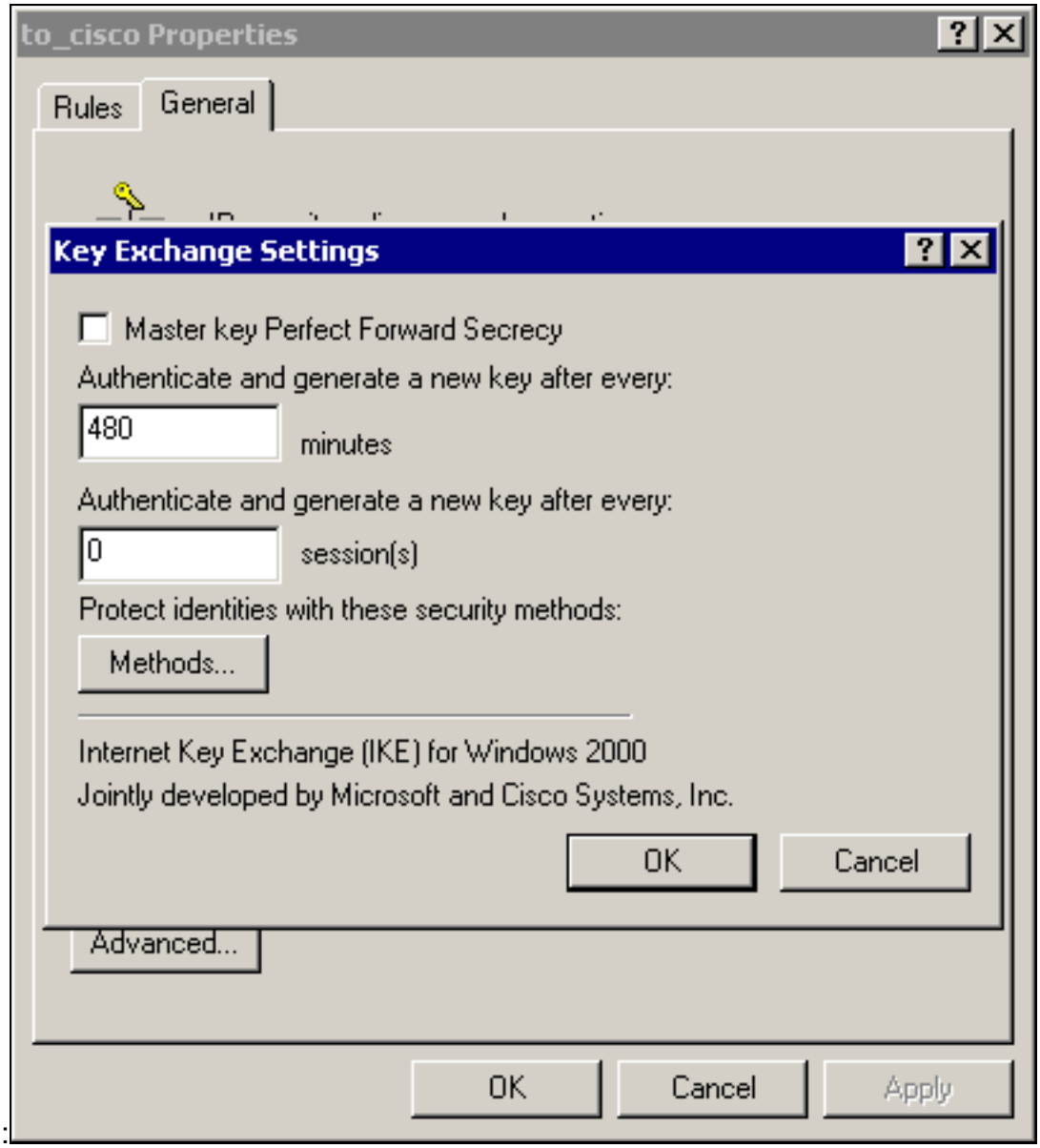
2. 此示例规则包含两个过滤器：Microsoft-Cisco和Cisco-Microsoft。



3. 选择Cisco-Microsoft IP Security Rule，然后单击**Edit**查看/添加/编辑IP过滤器列表。

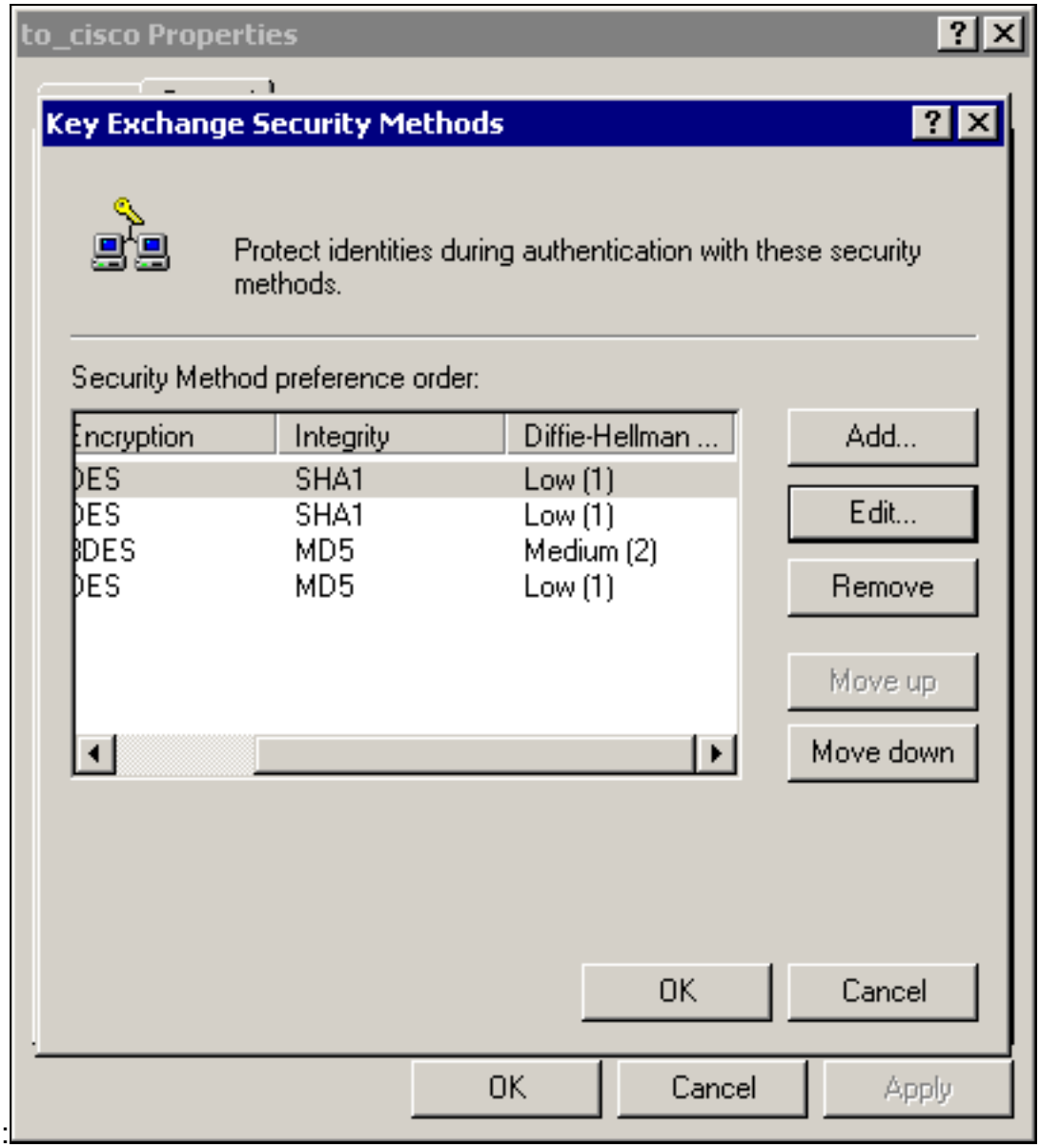


4. 规则的General **> Advanced**选项卡具**有IKE生**命期(480分钟= 28800秒



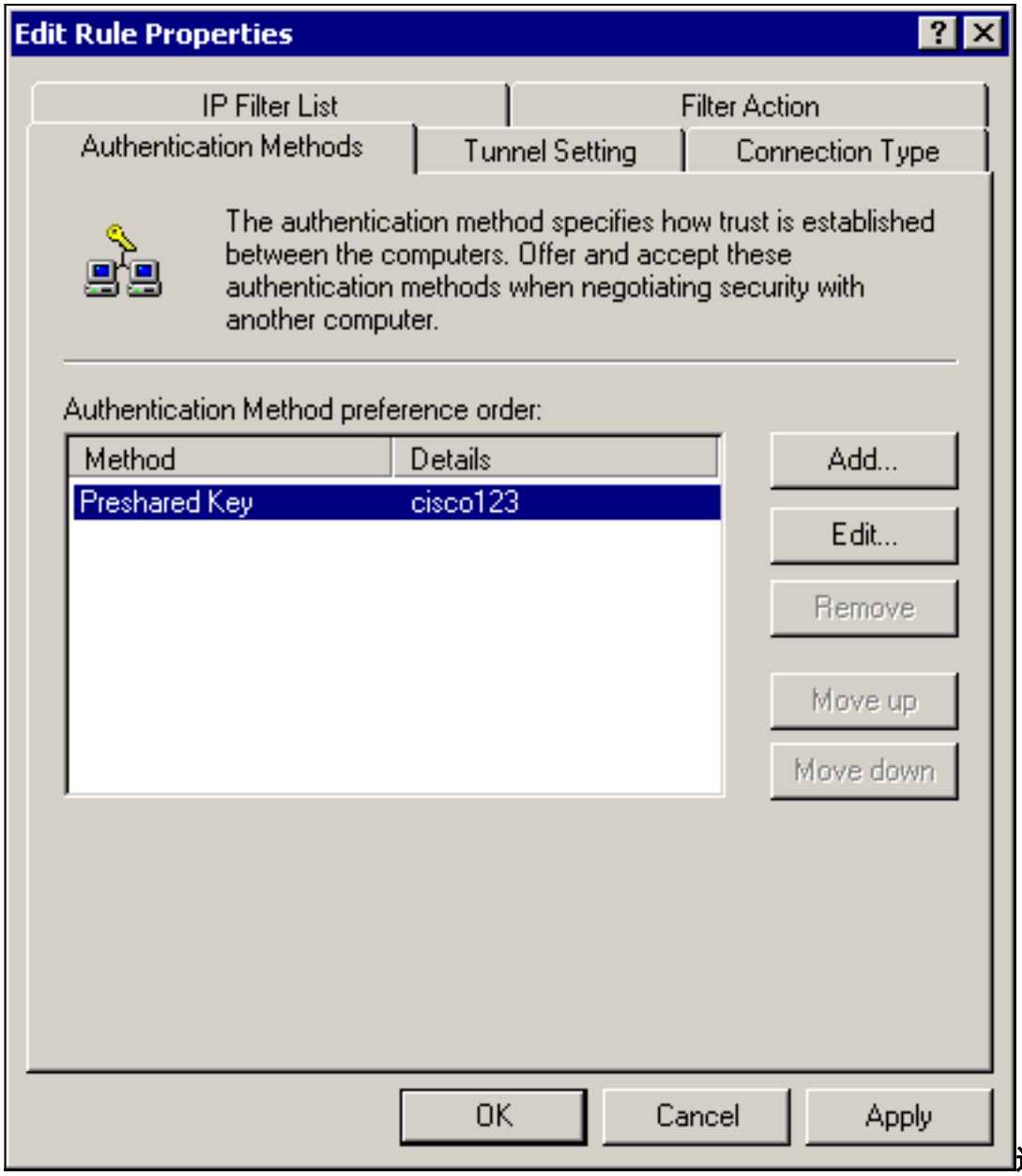
):

5. 规则的**General > Advanced > Methods**选项**卡具有IKE加密方法**(DES)、**IKE散列**(SHA1)和**Diffie-Helman组**(低

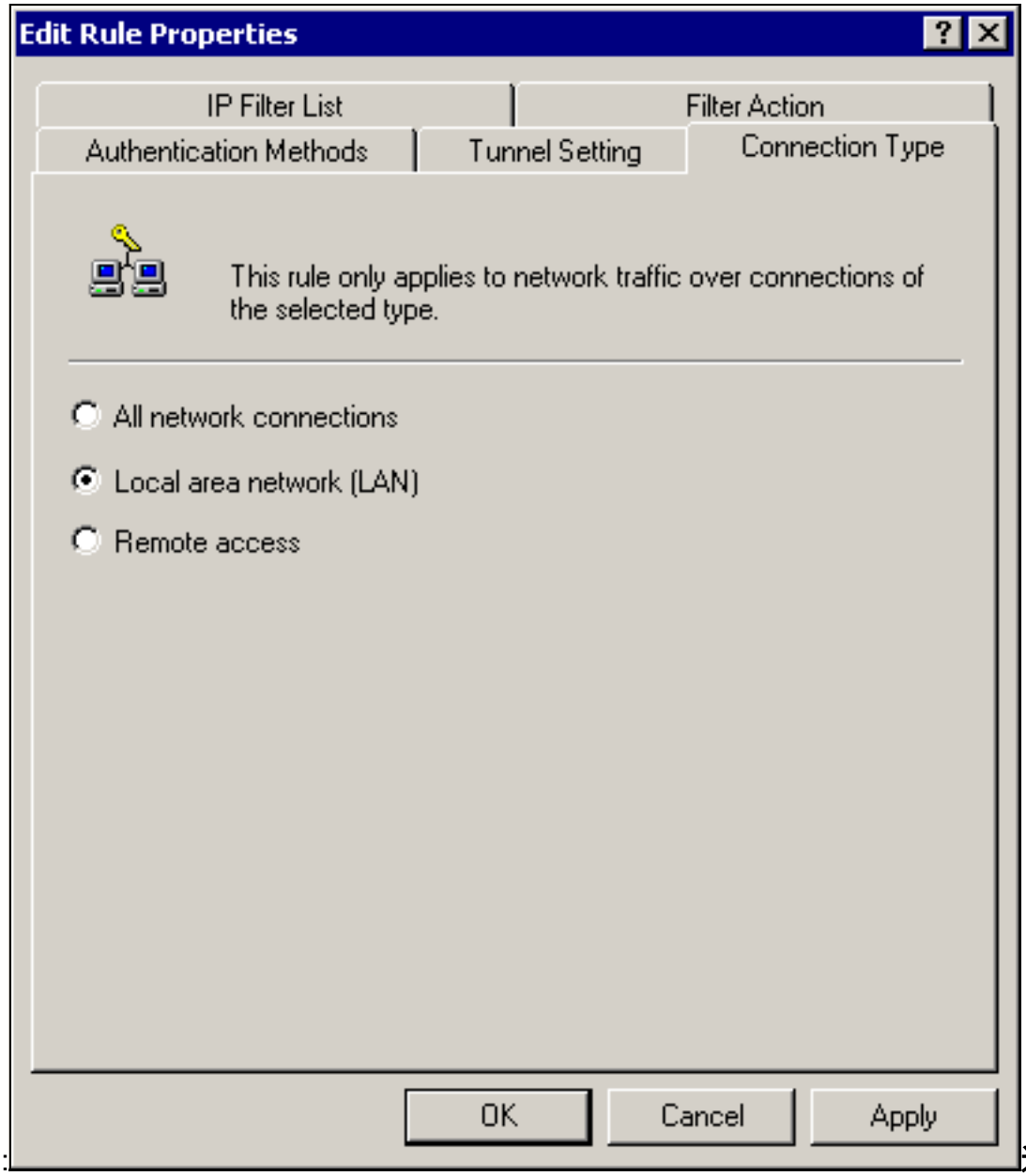


(1)):

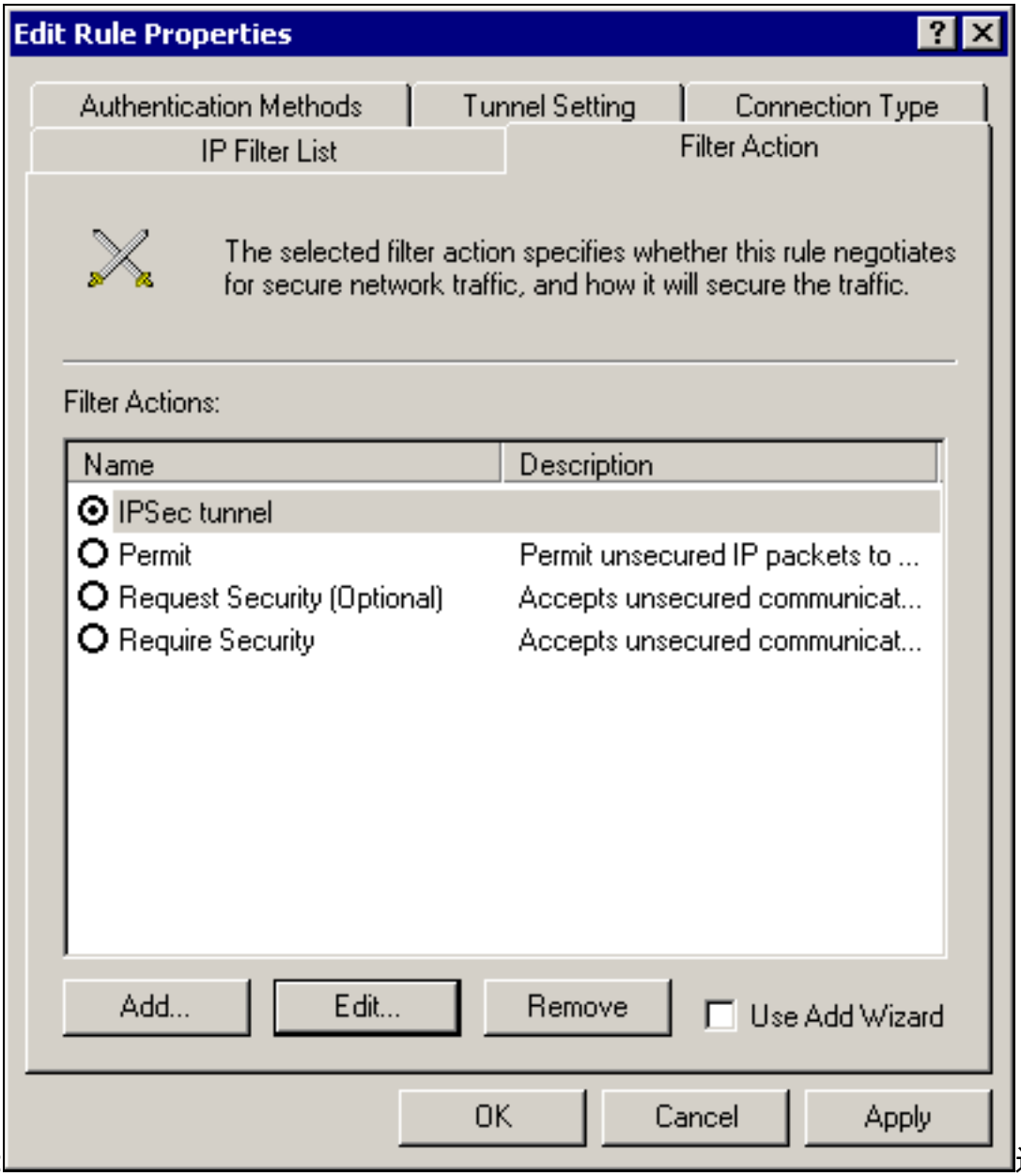
6. 每个过滤器有5个选项卡：**身份验证**方法（Internet密钥交换[IKE]的预共享密钥


Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method preference order:
Method
Details
Preshared Key
cisco123
Add...
Edit...
Remove
Move up
Move down
OK
Cancel
Apply

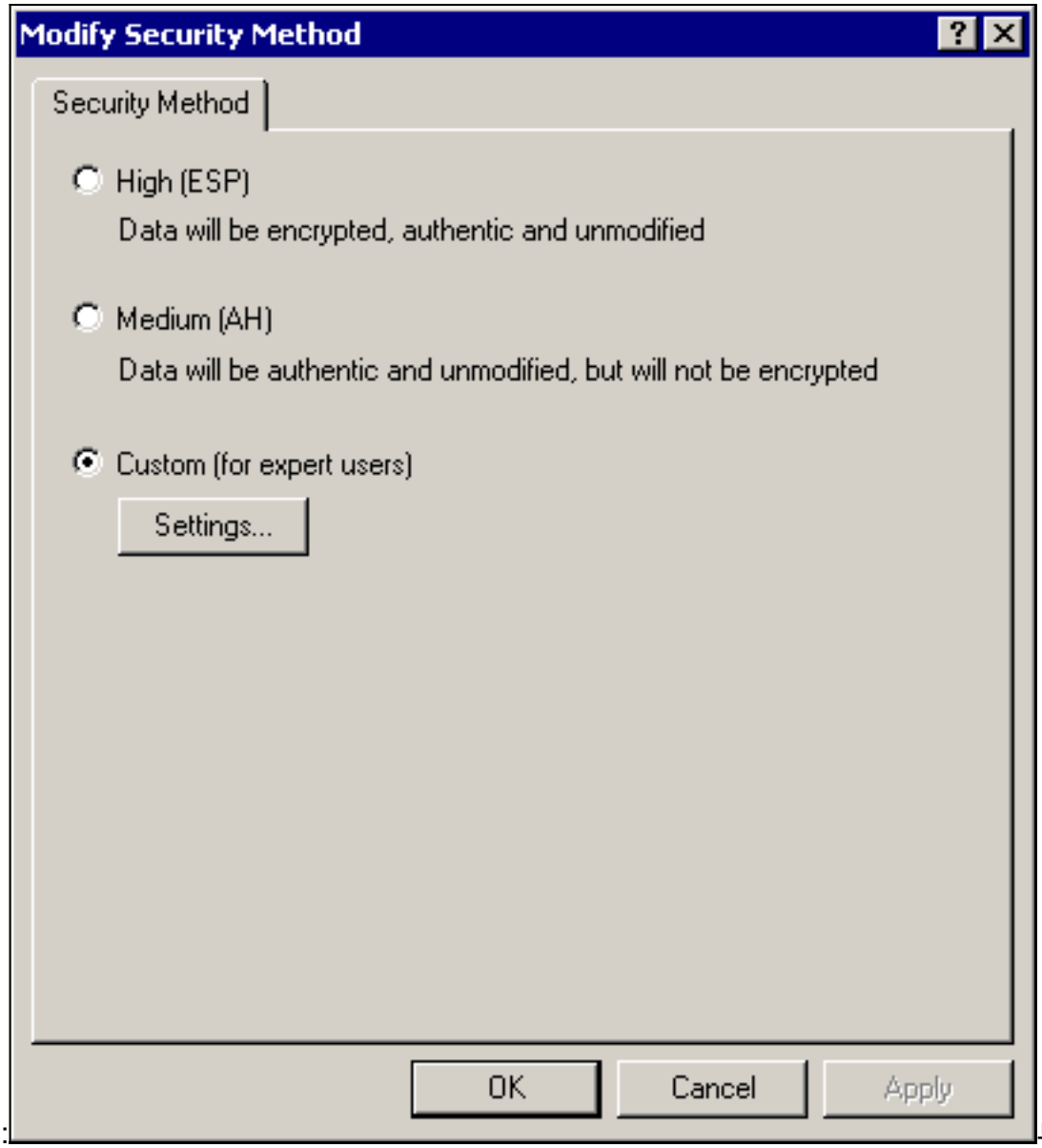
) : **连接类型**


Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
This rule only applies to network traffic over connections of the selected type.
All network connections
Local area network (LAN)
Remote access
OK
Cancel
Apply

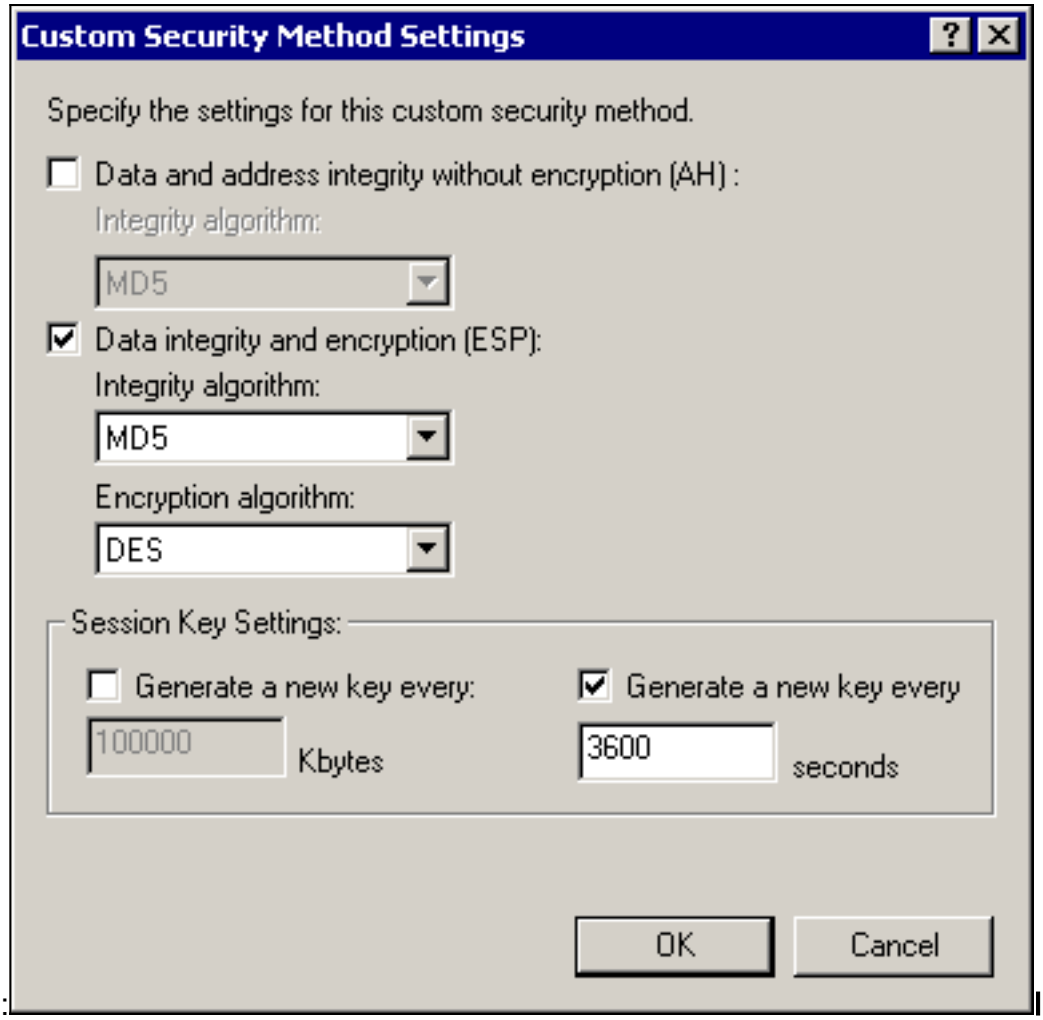
(LAN):**过滤器操**



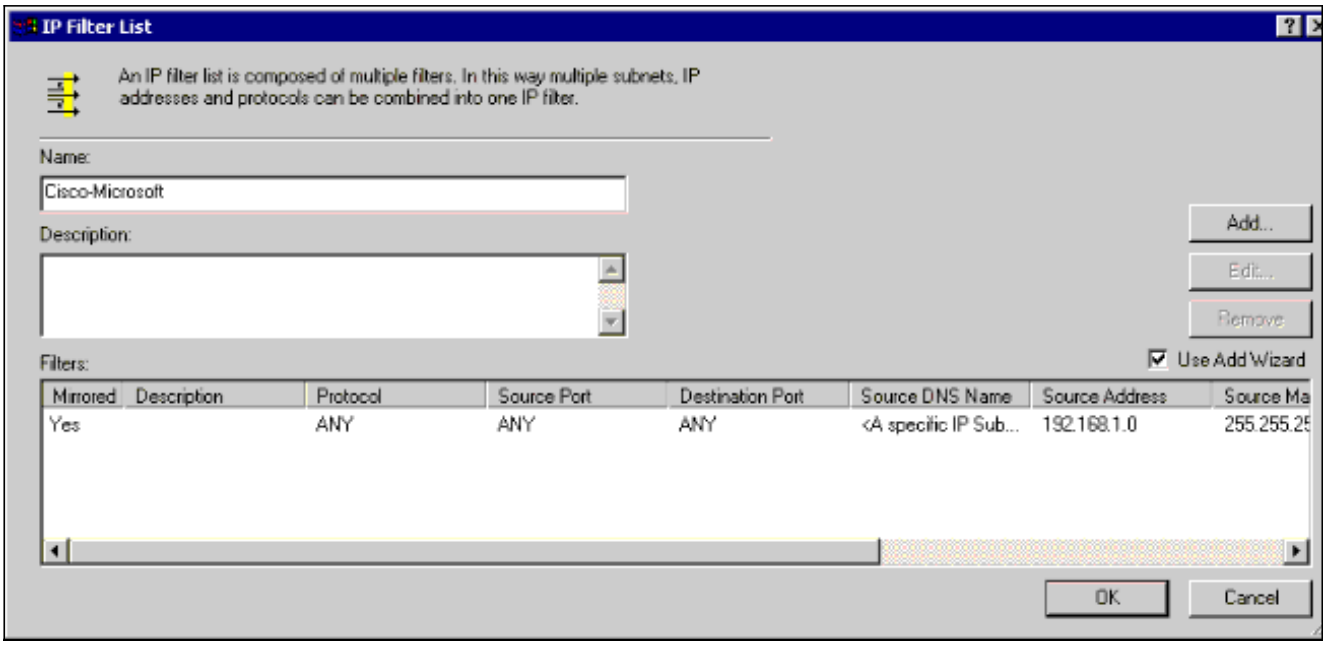
作(IPSec):选择 **Filter Action > IPSec tunnel > Edit > Edit，然后单击**



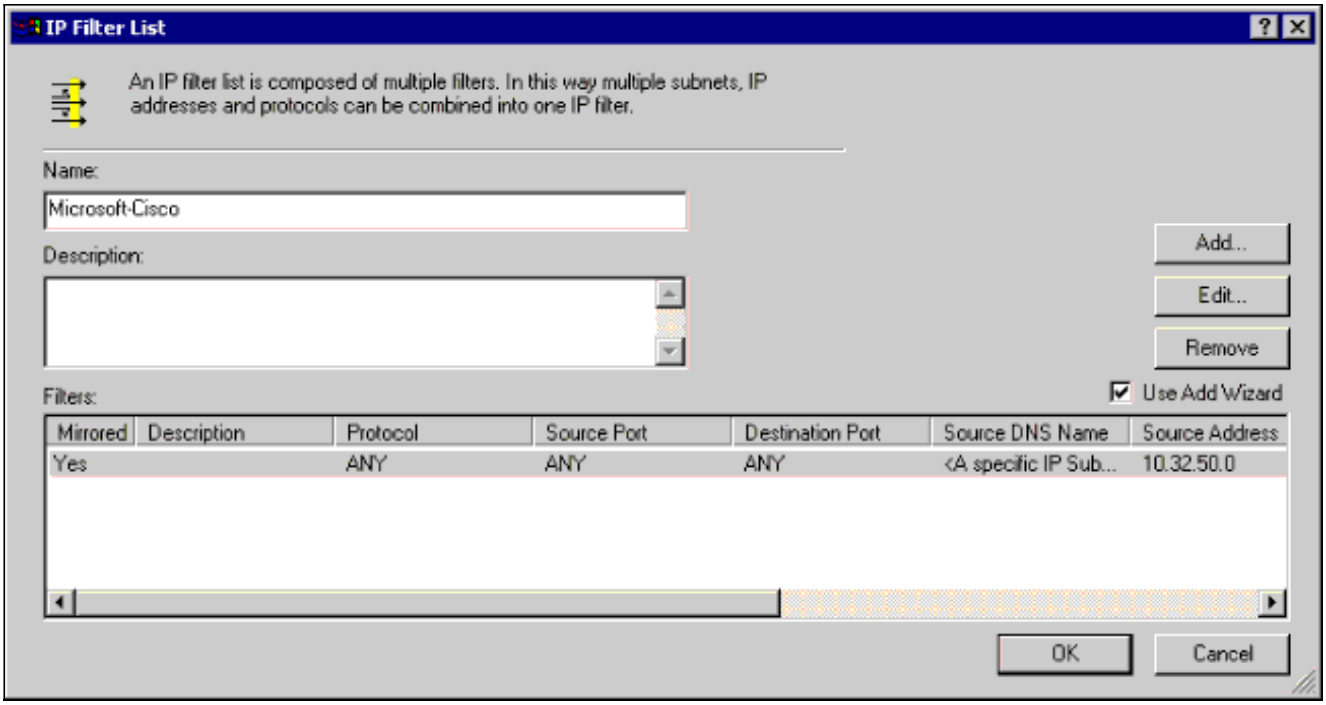
Custom:单击Settings - IPSec转换和IPSec有效期



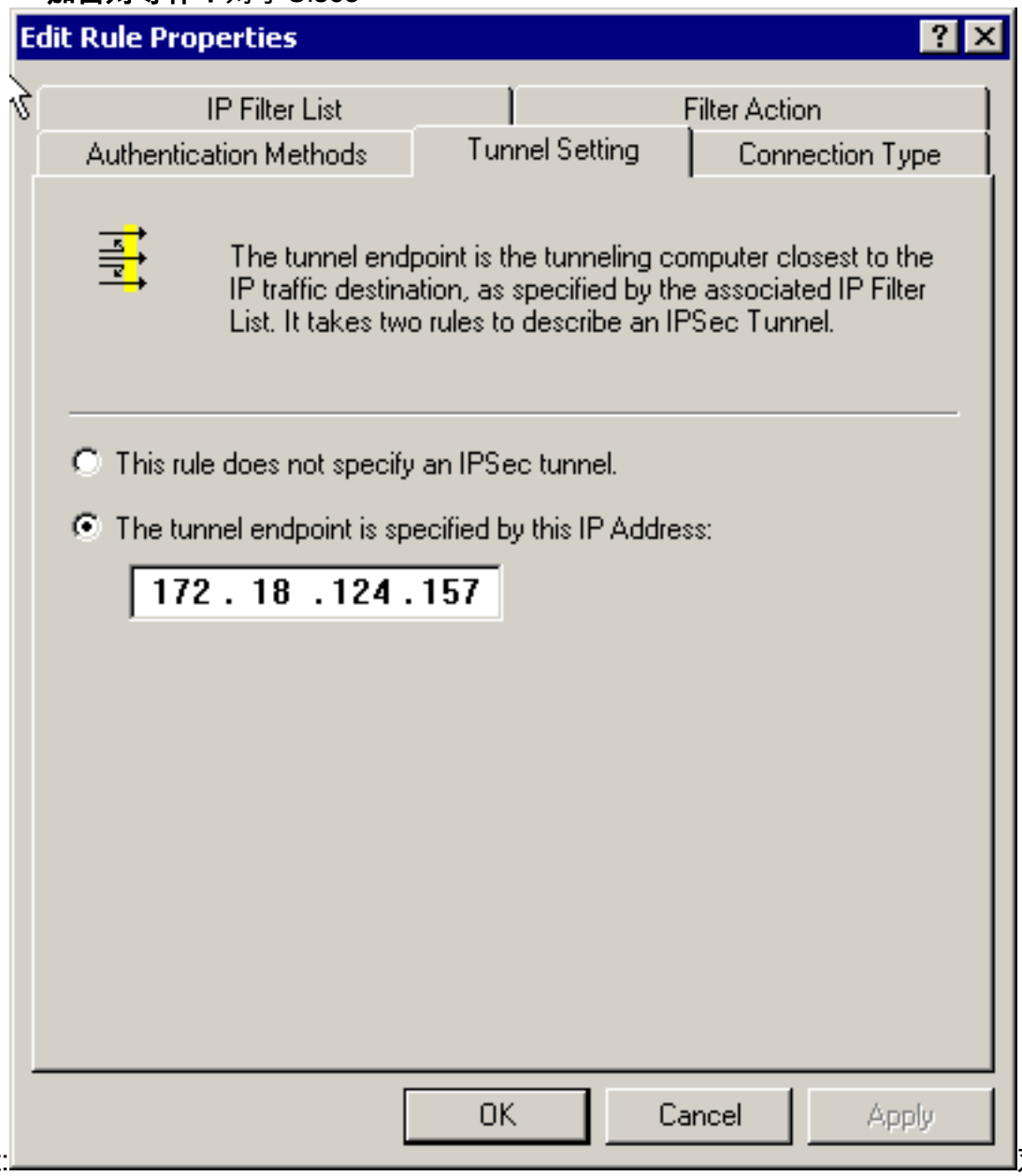
:**IP过滤器列表 — 要加密的源和目标网络：对于Cisco-Microsoft:**



对于Microsoft-Cisco:

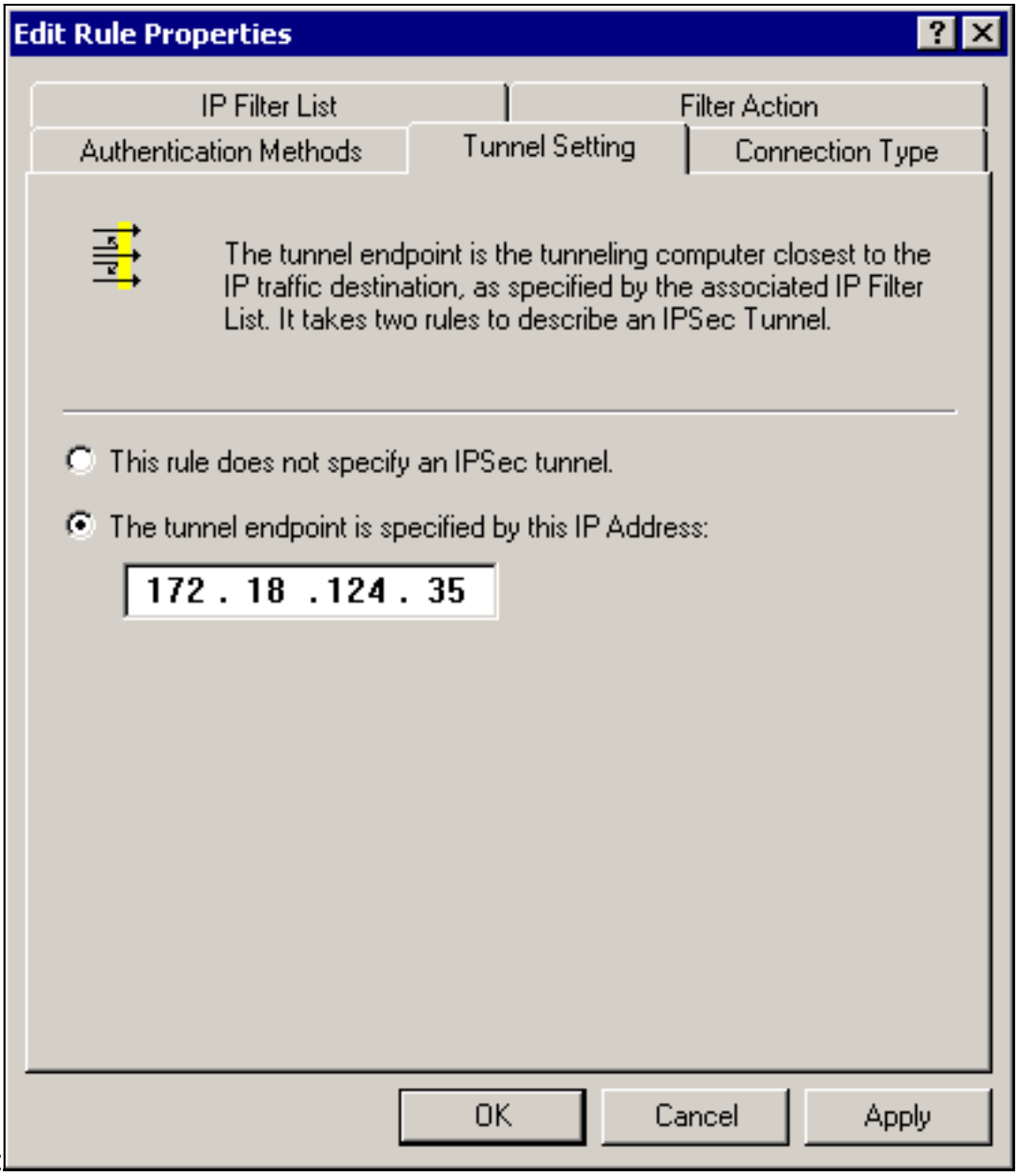


隧道设置 — 加密对等体：对于Cisco-



Microsoft:对于

Microsoft-Cisco:



配置 Cisco 设备

配置Cisco路由器、PIX和VPN集中器，如以下示例所示。

- Cisco 3640 路由器
- PIX
- VPN 3000 集中器
- VPN 5000 集中器

配置 Cisco 3640 路由器

Cisco 3640 路由器
Current configuration : 1840 bytes ! version 12.1 no service single-slot-reload-enable service timestamps debug uptime

```
service timestamps log uptime
no service password-encryption
!
hostname moss
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
crypto isakmp policy 1
!--- The following are IOS defaults so they do not
appear: !--- IKE encryption method encryption des !---
IKE hashing hash sha !--- Diffie-Hellman group group 1
!--- Authentication method authentication pre-share
!--- IKE lifetime lifetime 28800
!--- encryption peer crypto isakmp key cisco123 address
172.18.124.157
!
!--- The following is the IOS default so it does not
appear: !--- IPSec lifetime crypto ipsec security-
association lifetime seconds 3600 ! !--- IPSec
transforms crypto ipsec transform-set rtpset esp-des
esp-md5-hmac
!
crypto map rtp 1 ipsec-isakmp
!--- Encryption peer set peer 172.18.124.157
set transform-set rtpset
!--- Source/Destination networks defined match address
115
!
call rsvp-sync
!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface Ethernet0/1
ip address 172.18.124.35 255.255.255.240
ip nat outside
half-duplex
crypto map rtp
!
ip nat pool INTERNET 172.18.124.35 172.18.124.35 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.36
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
!--- Source/Destination networks defined access-list 115
permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
```

```
line con 0
transport input none
line 65 94
line aux 0
line vty 0 4
!
end
```

配置 PIX

PIX

```
PIX Version 5.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
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
!--- Source/Destination networks defined 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
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 10baset
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
!--- Except Source/Destination from Network Address
Translation (NAT): nat (inside) 0 access-list 115
route outside 0.0.0.0 0.0.0.0 172.18.124.36 1
timeout xlate 3:00:00
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
sysopt connection permit-ipsec
no sysopt route dnat
!--- IPSec transforms crypto ipsec transform-set myset
esp-des esp-md5-hmac
!--- IPSec lifetime crypto ipsec security-association
lifetime seconds 3600
crypto map rtpmap 10 ipsec-isakmp
!--- Source/Destination networks crypto map rtpmap 10
match address 115
!--- Encryption peer crypto map rtpmap 10 set peer
172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap interface outside
isakmp enable outside
!--- Encryption peer isakmp key ******** address
172.18.124.157 netmask 255.255.255.240
isakmp identity address
!--- Authentication method isakmp policy 10
authentication pre-share
!--- IKE encryption method isakmp policy 10 encryption
des
!--- IKE hashing isakmp policy 10 hash sha
!--- Diffie-Hellman group isakmp policy 10 group 1
!--- IKE lifetime isakmp policy 10 lifetime 28800
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:c237ed11307abea7b530bbd0c2b2ec08
: end
```

配置 VPN 3000 集中器

使用如下所示的菜单选项和参数根据需要配置VPN集中器。

- 要添加IKE建议，请选择**Configuration > System > Tunneling Protocols > IPSec > IKE Proposas > Add a proposal**。
  Proposal Name = DES-SHA
  !--- Authentication method Authentication Mode = Preshared Keys *!--- IKE hashing*
  Authentication Algorithm = SHA/HMAC-160 *!--- IKE encryption method* Encryption Algorithm =
  DES-56 *!--- Diffie-Hellman group* Diffie Hellman Group = Group 1 (768-bits) Lifetime
  Measurement = Time Date Lifetime = 10000 *!--- IKE lifetime* Time Lifetime = 28800
- 要定义LAN到LAN隧道，请选择**Configuration > System > Tunneling Protocols > IPSec LAN到LAN**。
  Name = to_2000
  Interface = Ethernet 2 (Public) 172.18.124.35/28
  !--- Encryption peer Peer = 172.18.124.157 *!--- Authentication method* Digital Certs = none
  (Use Pre-shared Keys) Pre-shared key = cisco123 *!--- IPSec transforms* Authentication =
  ESP/MD5/HMAC-128 Encryption = DES-56 *!--- Use the IKE proposal* IKE Proposal = DES-SHA
  Autodiscovery = off *!--- Source network defined* Local Network Network List = Use IP
  Address/Wildcard-mask below IP Address 192.168.1.0 Wildcard Mask = 0.0.0.255 *!---*
  Destination network defined Remote Network Network List = Use IP Address/Wildcard-mask below
  IP Address 10.32.50.0 Wildcard Mask 0.0.0.255

- 要修改安全关联，请选择**Configuration > Policy Management > Traffic Management > Security Associations > Modify**。

```
SA Name = L2L-to_2000
Inheritance = From Rule
IPSec Parameters
!--- IPSec transforms Authentication Algorithm = ESP/MD5/HMAC-128 Encryption Algorithm =
DES-56 Encapsulation Mode = Tunnel PFS = Disabled Lifetime Measurement = Time Data Lifetime
= 10000 !--- IPSec lifetime Time Lifetime = 3600 Ike Parameters !--- Encryption peer IKE
Peer = 172.18.124.157 Negotiation Mode = Main !--- Authentication method Digital Certificate
= None (Use Preshared Keys) !--- Use the IKE proposal IKE Proposal DES-SHA
```

配置 VPN 5000 集中器

VPN 5000 集中器

```
[ IP Ethernet 1:0 ]
Mode = Routed
SubnetMask = 255.255.255.240
IPAddress = 172.18.124.35

[ General ]
IPSecGateway = 172.18.124.36
DeviceName = "cisco"
EthernetAddress = 00:00:a5:f0:c8:00
DeviceType = VPN 5002/8 Concentrator
ConfiguredOn = Timeserver not configured
ConfiguredFrom = Command Line, from Console

[ IP Ethernet 0:0 ]
Mode = Routed
SubnetMask = 255.255.255.0
IPAddress = 192.168.1.1

[ Tunnel Partner VPN 1 ]
 !--- Encryption peer Partner = 172.18.124.157 !---
IPSec lifetime KeyLifeSecs = 3600 BindTo = "ethernet
1:0" !--- Authentication method SharedKey = "cisco123"
KeyManage = Auto !--- IPSec transforms Transform =
esp(md5,des) Mode = Main !--- Destination network
defined Peer = "10.32.50.0/24" !--- Source network
defined LocalAccess = "192.168.1.0/24" [ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1 [ IP VPN 1 ] Mode =
Routed Numbered = Off [ IKE Policy ] !--- IKE hashing,
encryption, Diffie-Hellman group Protection = SHA_DES_G1
Configuration size is 1088 out of 65500 bytes.
```

验证

当前没有可用于此配置的验证过程。

故障排除

本节提供可用于排除配置故障的信息。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

注意：在发出debug**命**令之前，请参阅有关Debug命令的重要信息。

Cisco 3640 路由器

- **debug crypto engine** — 显示有关执行加密和解密的加密引擎的调试消息。
- **debug crypto isakmp** — 显示有关IKE事件的消息。
- **debug crypto ipsec** — 显示IPSec事件。
- **show crypto isakmp sa - 显示对等体上的所有当前 IKE 安全关联 (SA)。**
- **show crypto ipsec sa** — 显示当前安全关联使用的设置。
- **clear crypto isakmp** —（从配置模式）清除所有活动IKE连接。
- **clear crypto sa** —（从配置模式）删除所有IPSec安全关联。

PIX

- **debug crypto ipsec - 显示第 2 阶段的 IPSec 协商。**
- **debug crypto isakmp - 显示第 1 阶段的 Internet 安全连接和密钥管理协议 (ISAKMP) 协商。**
- **debug crypto engine - 显示加密的流量。**
- **show crypto ipsec sa - 显示第 2 阶段的安全关联。**
- **show crypto isakmp sa** — 显示第1阶段安全关联。
- **clear crypto isakmp** —（从配置模式）清除互联网密钥交换(IKE)安全关联。
- **clear crypto ipsec sa** —（从配置模式）清除IPSec安全关联。

VPN 3000 集中器

- — 通过选择**Configuration > System > Events > Classes > Modify**(Severity to Log=1-13, Severity to Console=1-3)启动VPN 3000集中器调试：IKE、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE
- — 通过选择Monitoring > Event Log，可以清除或检**索事件日志。**
- — 可在Monitoring > Sessions中监控LAN到LAN隧道**流量。**
- — 隧道可以在**Administration > Administer Sessions > LAN-to-LAN sessions > Actions - Logout中清除。**

VPN 5000 集中器

- **vpn trace dump all** — 显示有关所有匹配VPN连接的信息，包括有关时间、VPN编号、对等体的实际IP地址、已运行脚本以及发生错误时的软件代码的例程和行号。
- **show vpn statistics** — 显示用户、合作伙伴和两者的合计的以下信息。（对于模块化型号，显示器包括每个模块插槽的部分。）当前活动 — 当前活动连接。在Negot中 — 当前协商连接。High Water — 自上次重新启动以来并发活动连接的最大数量。Running Total — 自上次重新启动以来成功连接的总数。Tunnel Starts — 隧道启动数。隧道正常 — 没有错误的隧道数。隧道错误 — 有错误的隧道数。
- **show vpn statistics verbose** — 显示ISAKMP协商统计信息和更多活动连接统计信息。

相关信息

- Cisco VPN 5000 系列集中器终止销售公告
- 配置 IPSec 网络安全
- 配置 Internet 密钥交换安全协议
- 技术支持 - Cisco Systems