在Microsoft Windows 2000伺服器和Cisco裝置之間配置IPSec

目錄

簡介

本文檔演示如何使用預共用金鑰形成IPSec隧道以加入2個專用網路：思科裝置內的專用網路(192.168.l.X)和Microsoft 2000 Server內的專用網路(10.32.50.X)。我們假設從思科裝置內部和2000伺服器內部到Internet（此處由172.18.124.X網路表示）的流量在啟動此組態之前流動。

您可以在Microsoft網站上找到有關配置Microsoft Windows 2000伺服器的詳細資訊：http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

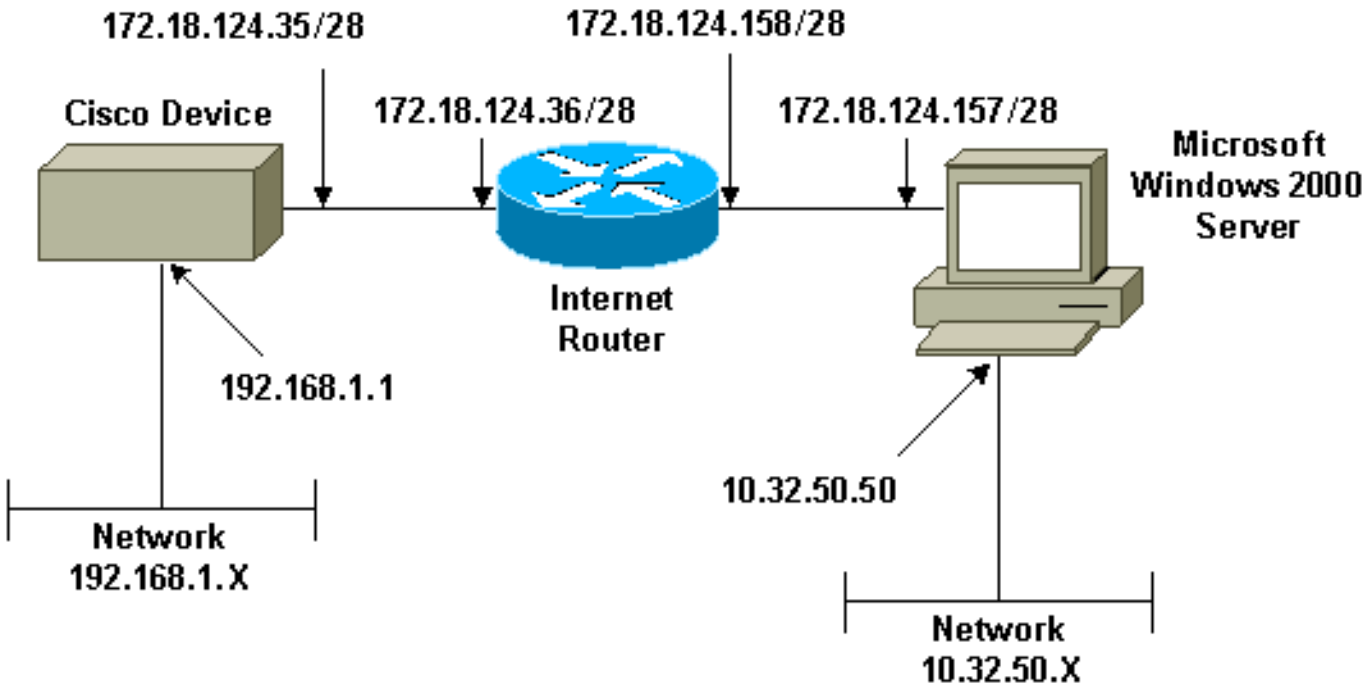
這些配置使用下面的軟體和硬體版本進行開發和測試。

- Microsoft Windows 2000 Server 5.00.2195
- 採用Cisco IOS®軟體版本c3640-ik2o3s-mz.121-5.T.bin的Cisco 3640路由器
- 採用PIX軟體版本5.2.1的Cisco安全PIX防火牆
- 採用VPN 3000集中器軟體版本2.5.2.F的Cisco VPN 3000集中器
- 採用VPN 5000集中器軟體的Cisco VPN 5000集中器版本5.2.19

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

網路圖表

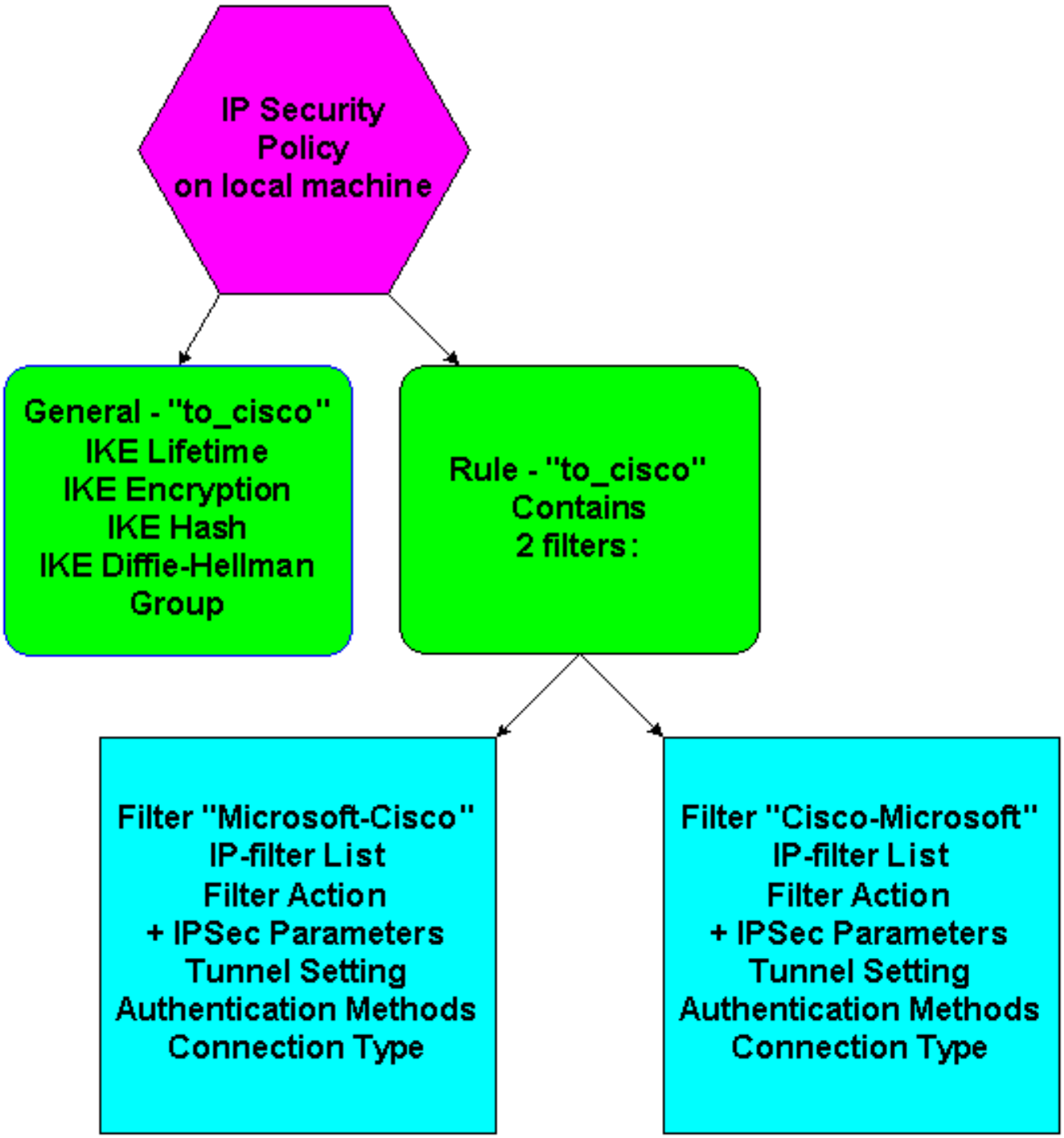
本文檔使用下圖所示的網路設定。



配置Microsoft Windows 2000 Server以使用思科裝置

已執行的任務

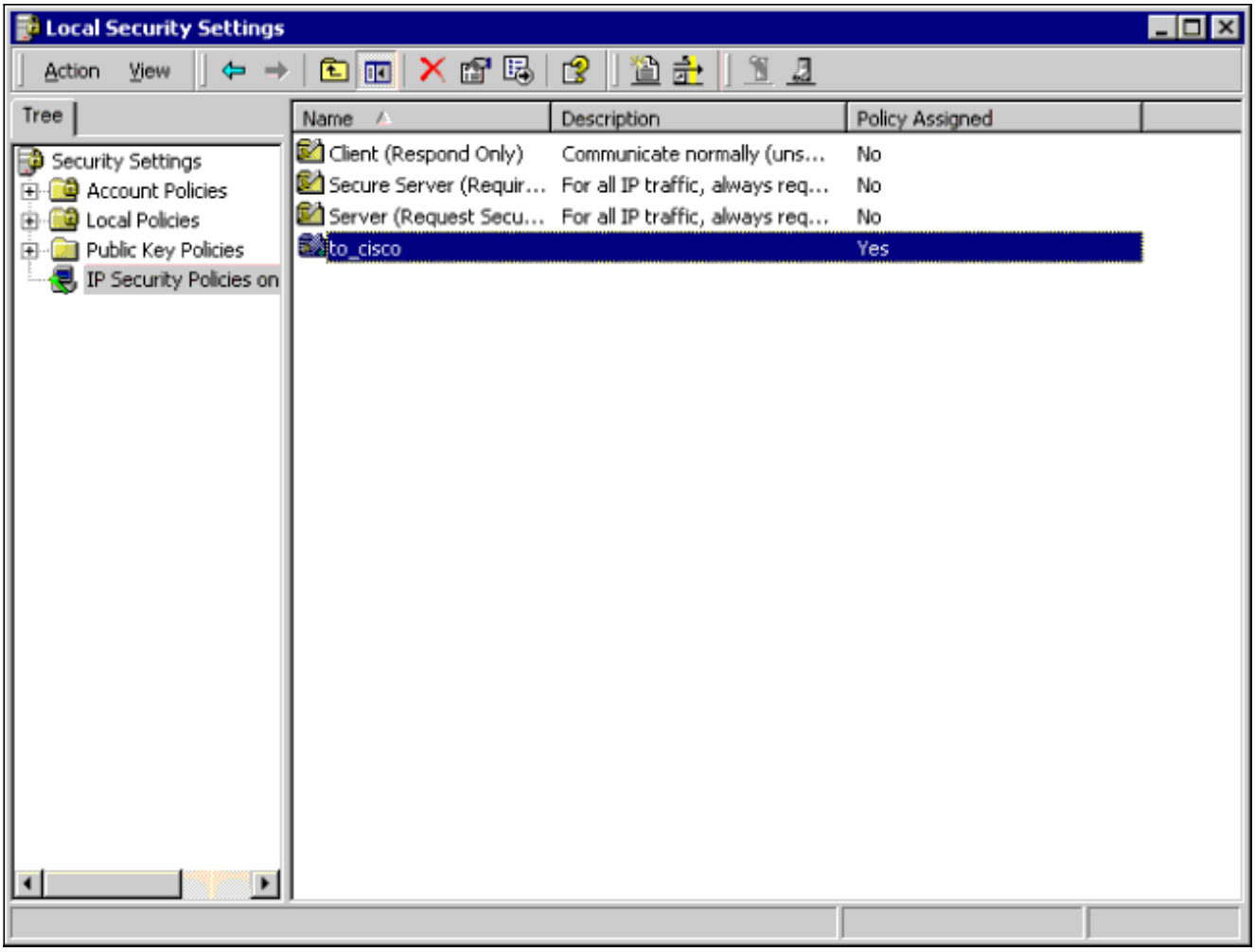
此圖顯示了在Microsoft Windows 2000伺服器配置中執行的任務：



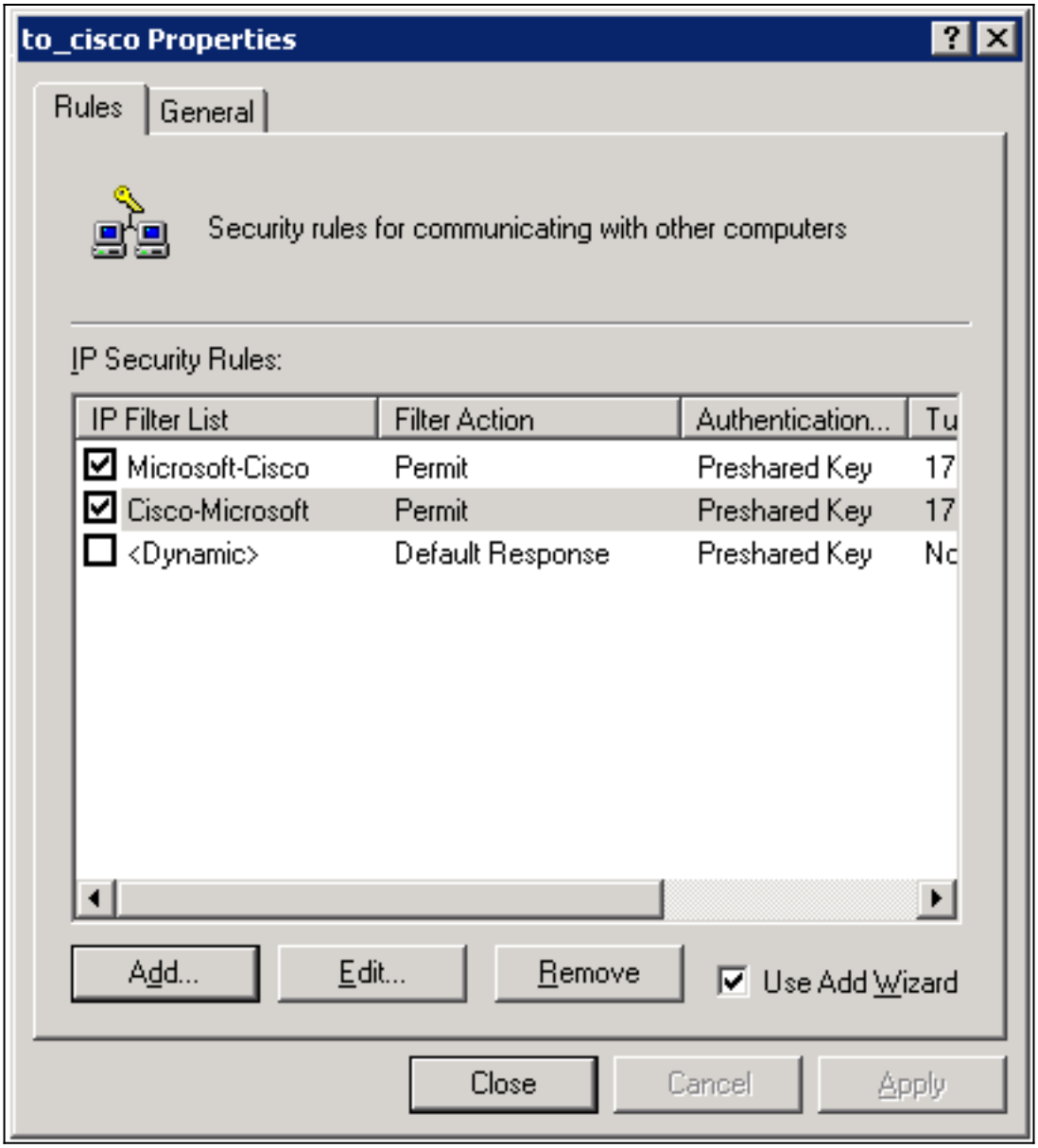
逐步說明

按照Microsoft網站上的配置說明 ，使用以下步驟驗證您的配置是否可以與思科裝置配合使用。評論和更改會隨螢幕截圖註明。

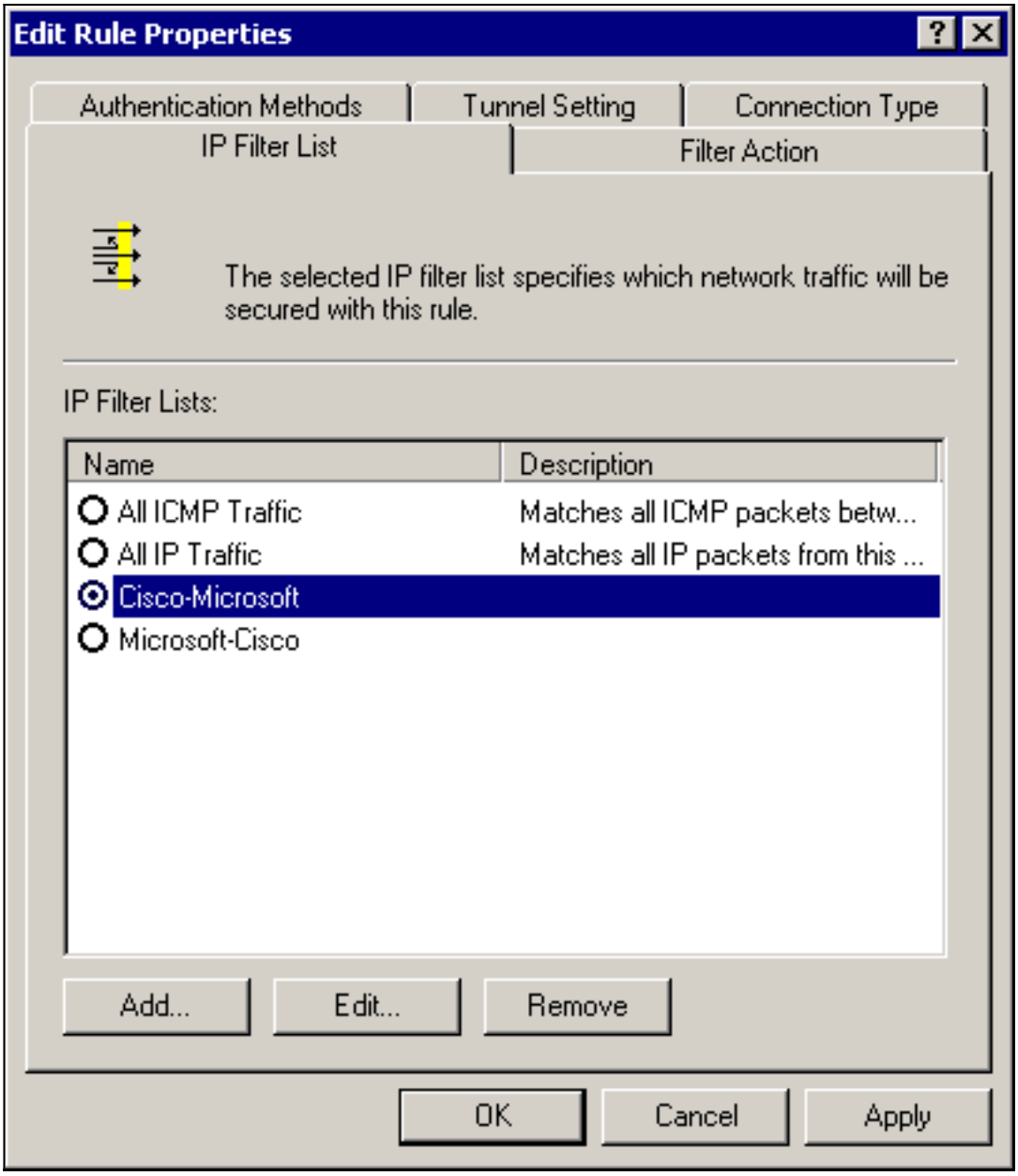
1. 在Microsoft Windows 2000 Server上按一下**Start > Run > secpol.msc**，並在以下螢幕上驗證資訊。使用Microsoft網站上的說明配置2000伺服器之後，將顯示以下隧道資訊。**注意：**示例規則稱為「to_cisco」。



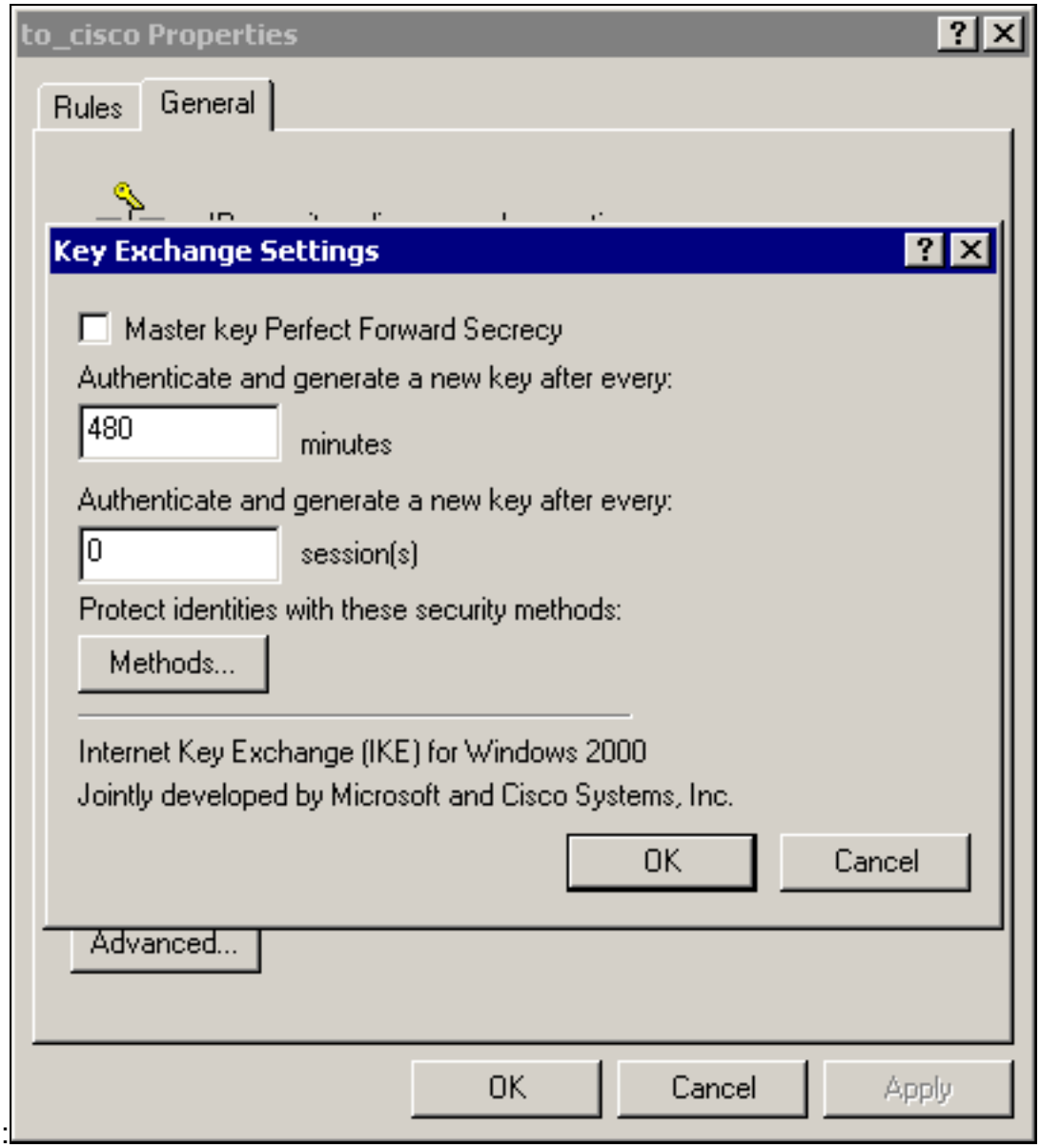
2. 此示例規則包含兩個篩選器：Microsoft-Cisco和Cisco-Microsoft。



3. 選擇Cisco-Microsoft IP安全規則，然後按一下**Edit**以檢視/新增/編輯IP過濾器清單。

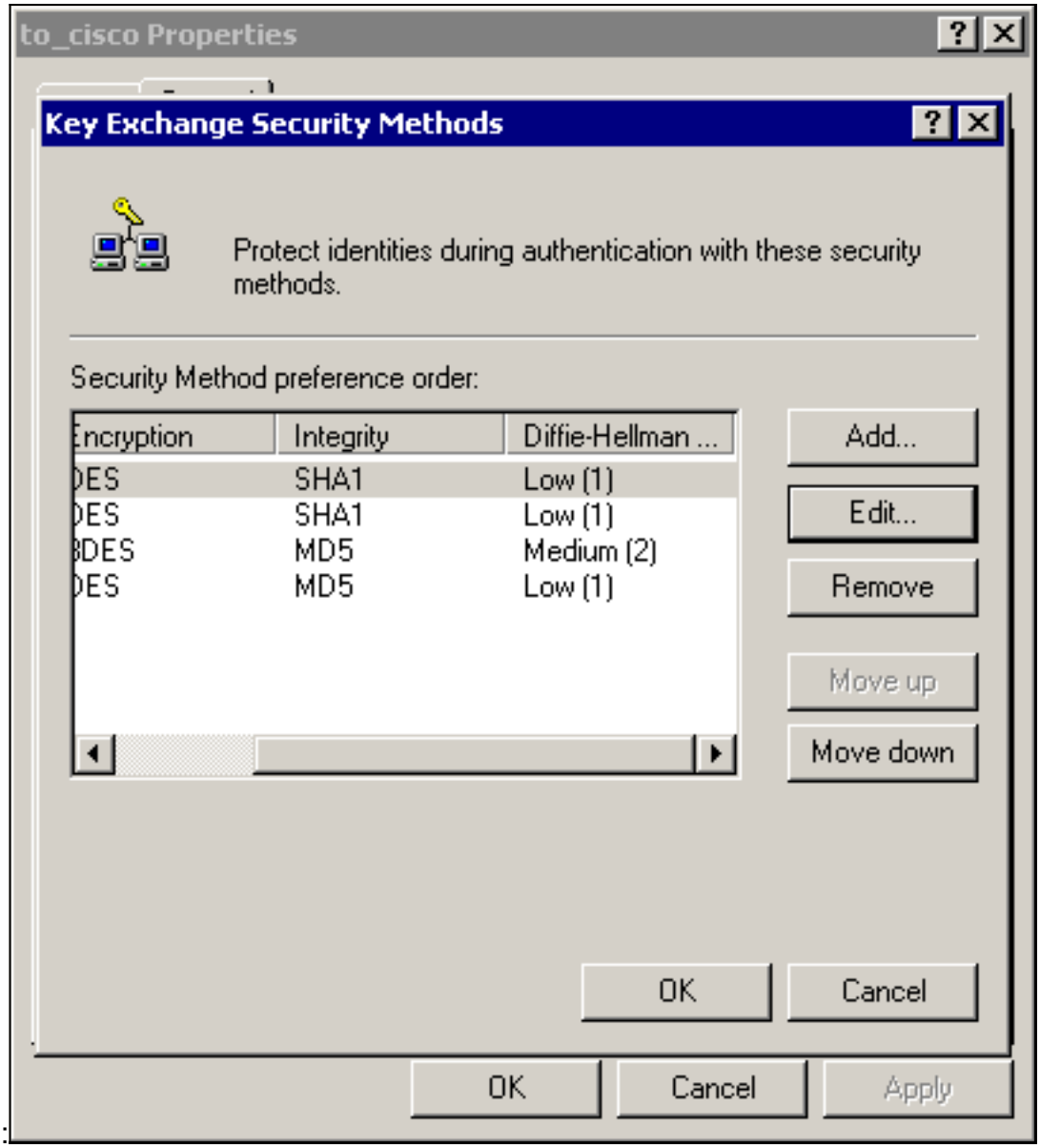


4. 規則的**General > Advanced**頁籤具有**IKE lifetime**(480分鐘= 28800秒



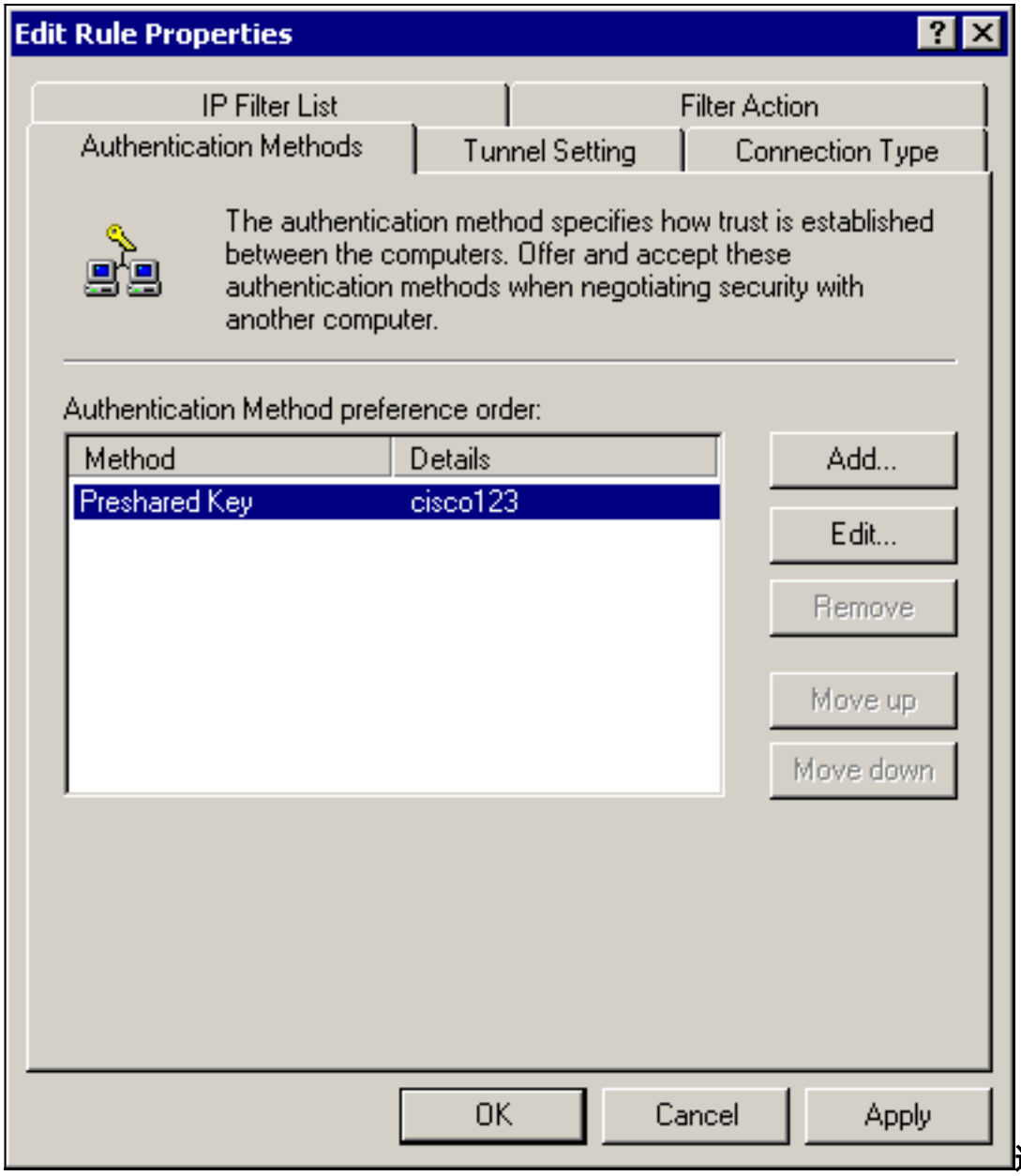
):

5. 規則的**General > Advanced > Methods**頁籤具有**IKE加密方法**(DES)、**IKE雜湊**(SHA1)和**Diffie-Helman組**

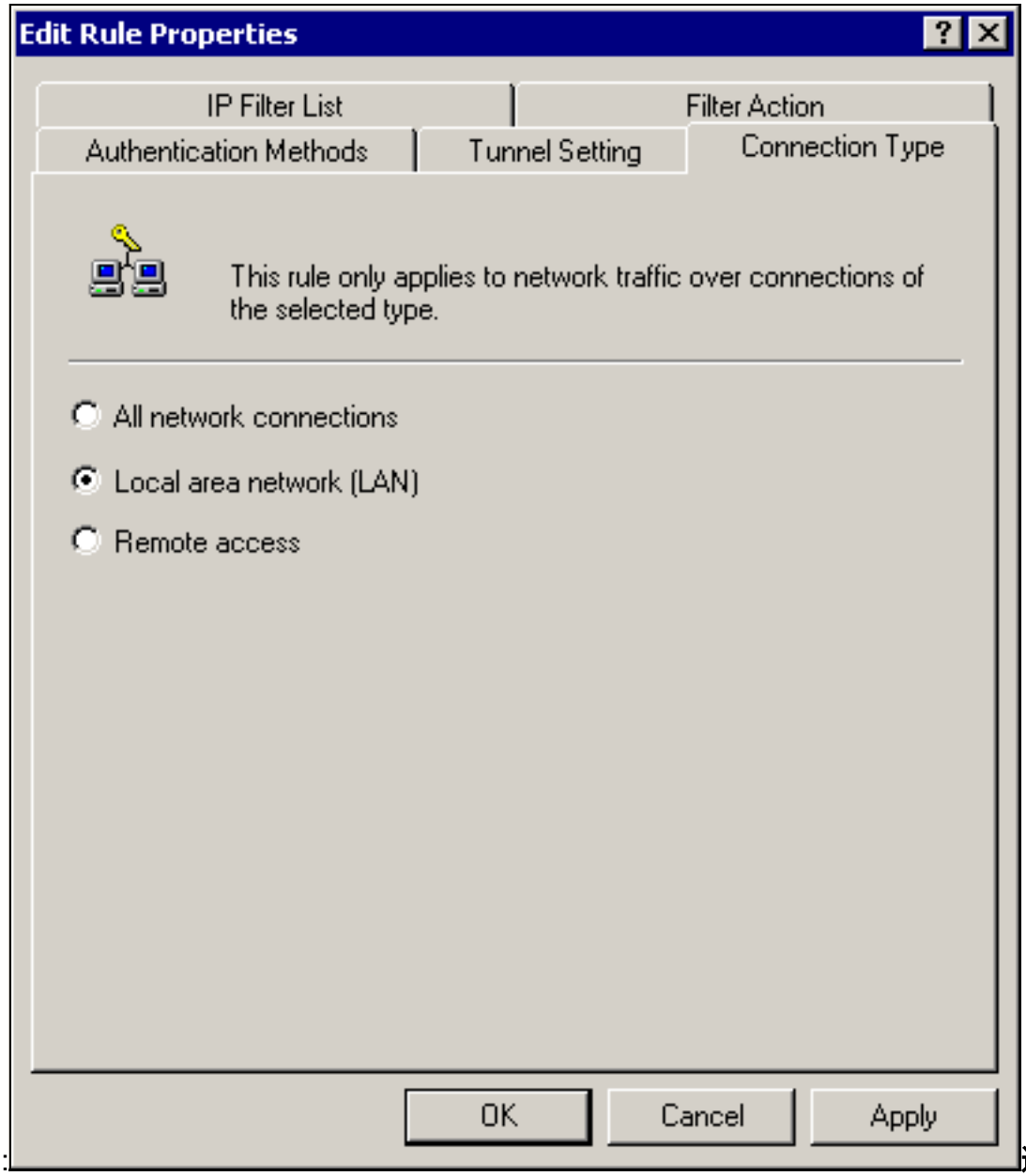


(Low(1)):

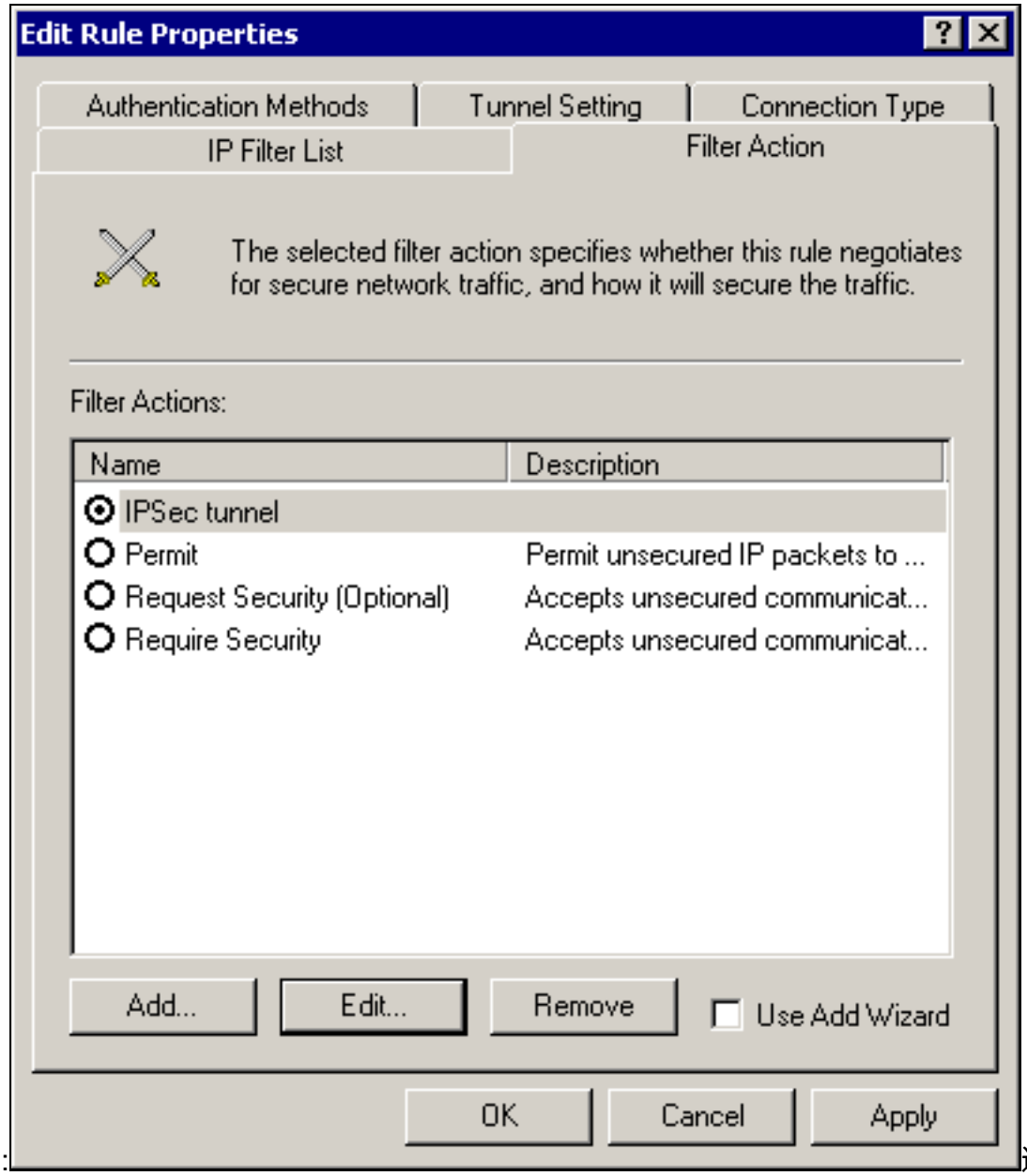
6. 每個過濾器有5個頁籤：**驗證方**法（Internet金鑰交換[IKE]的預共用金鑰


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

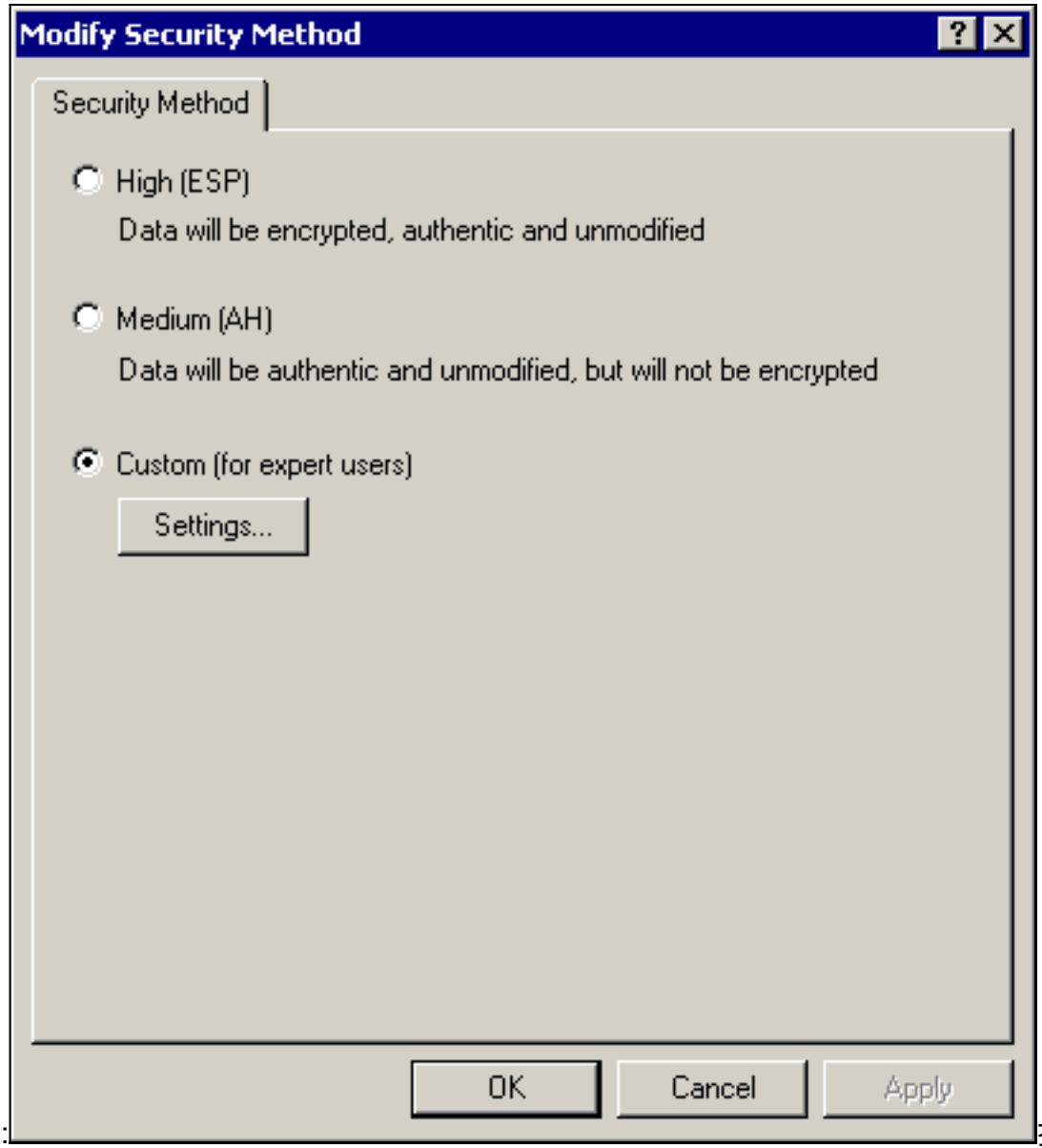
) : **連線類型**


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

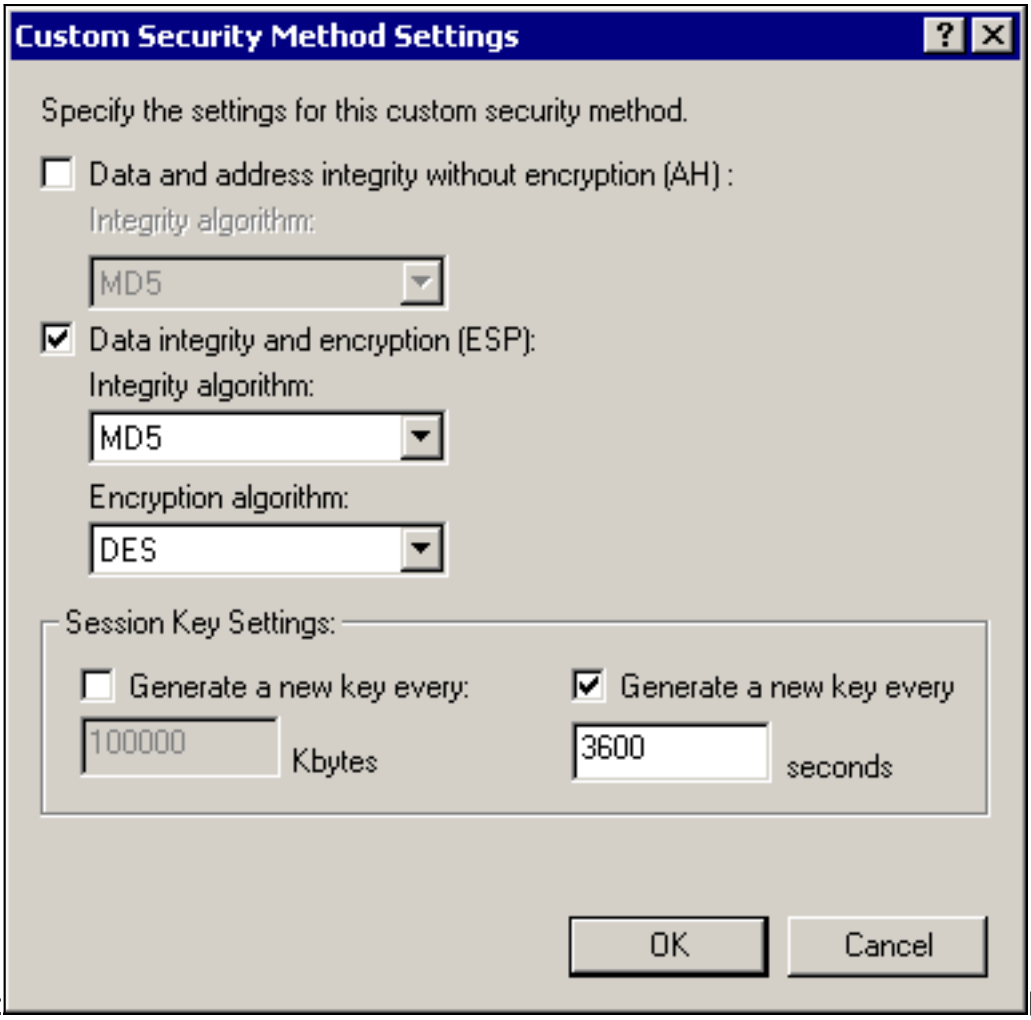
(LAN)：過濾器操



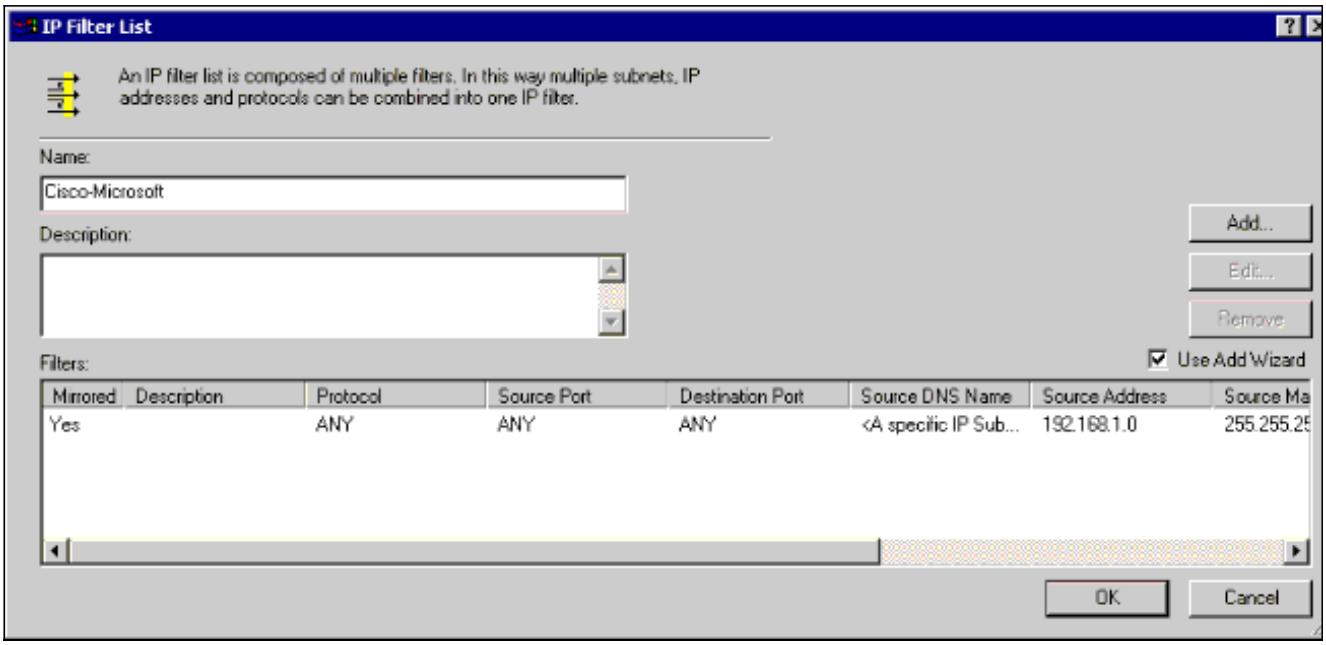
作(IPSec):選擇 **Filter Action > IPSec tunnel > Edit > Edit**，然後按一下



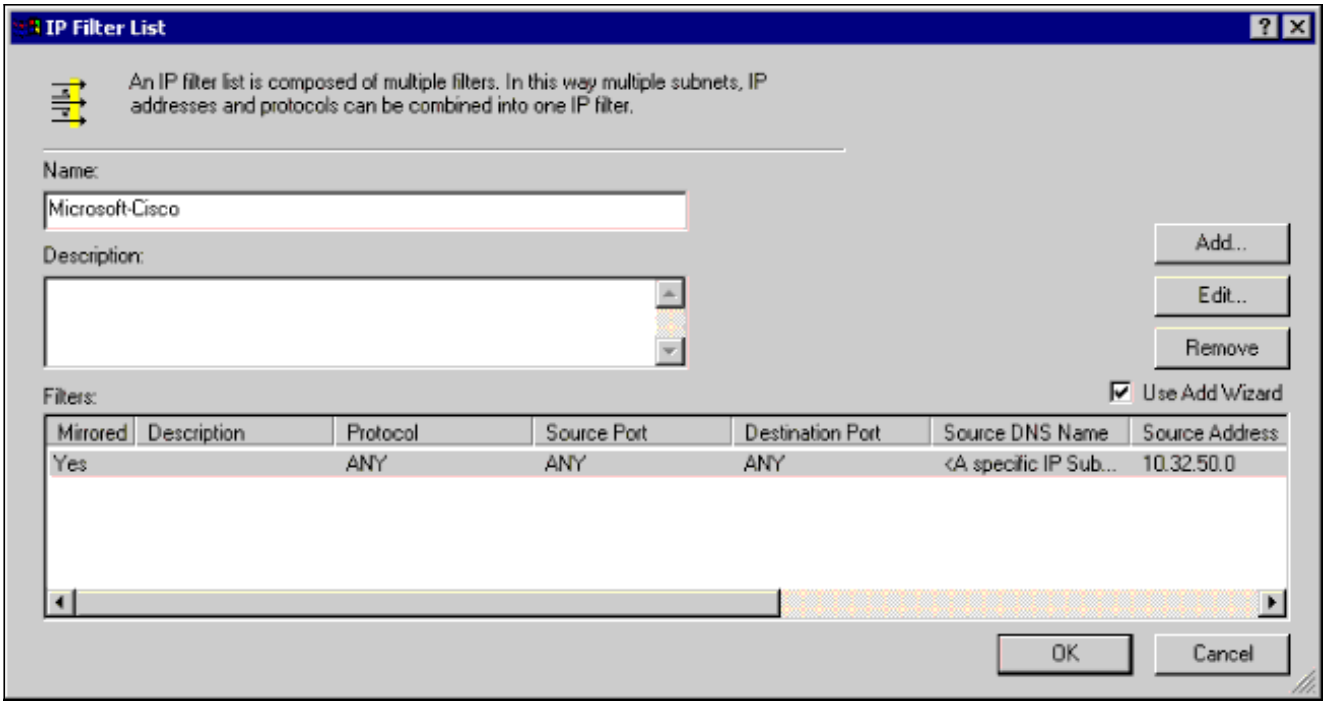
Custom:按一下Settings - IPSec transforms和IPSec



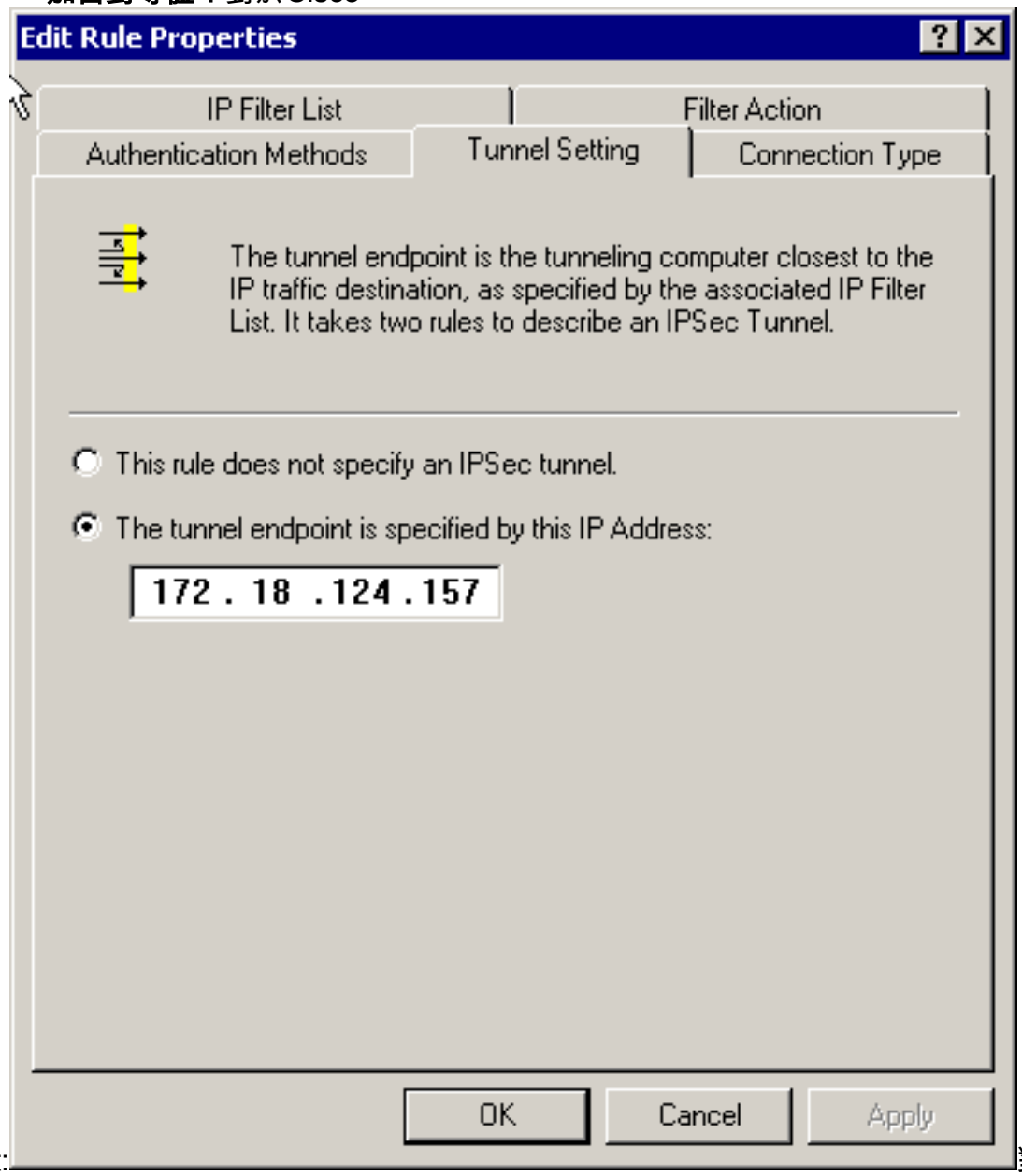
lifetime: **IP過濾器清單 — 要加密的源網路和目標網路：對於Cisco-Microsoft:**



對於Microsoft-Cisco:

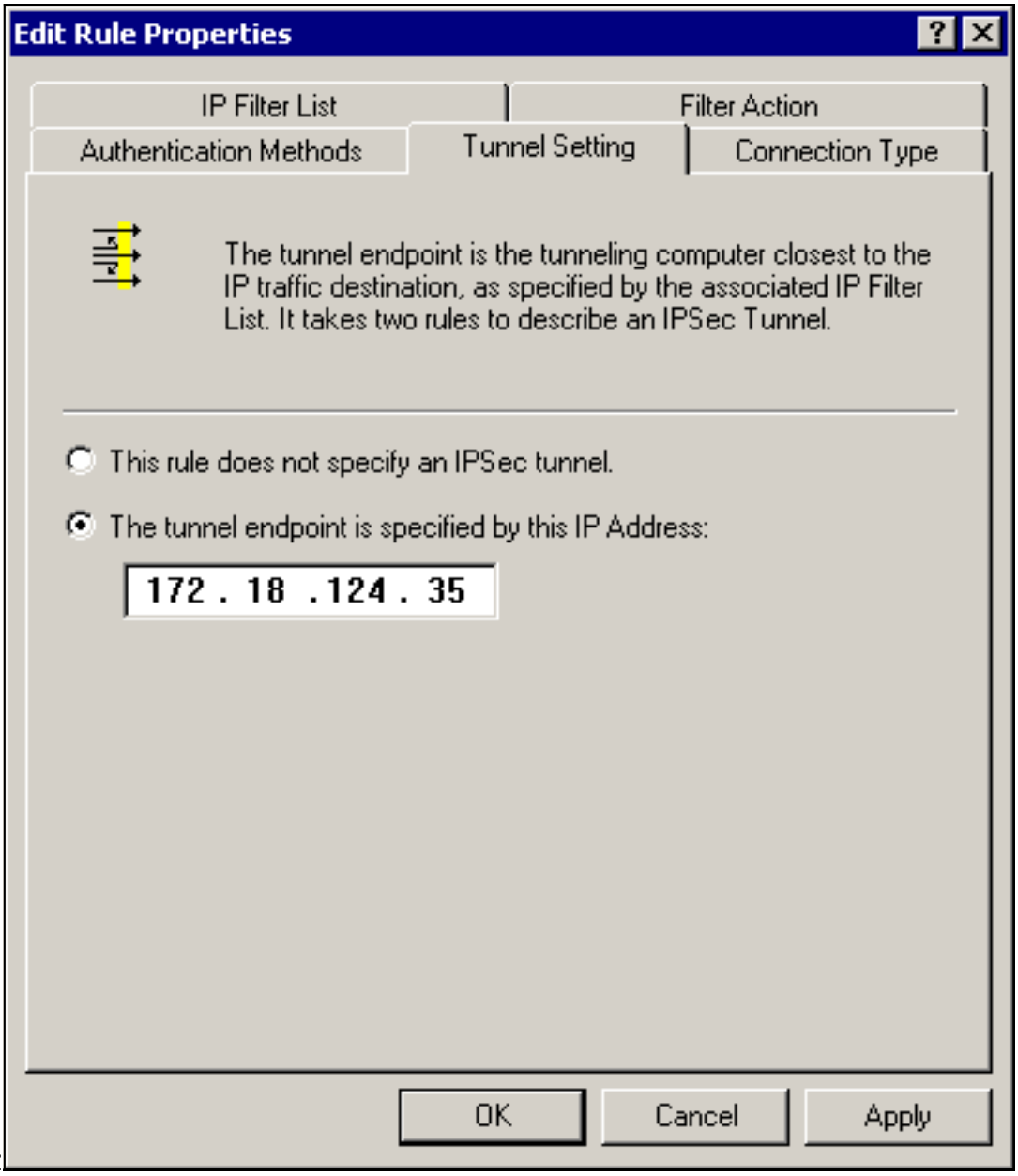


通道設定 — 加密對等體：對於Cisco-



Microsoft:對於

Microsoft-Cisco:



配置思科裝置

如下例所示，配置Cisco路由器、PIX和VPN集中器。

- 思科3640路由器
- PIX
- VPN 3000 Concentrator
- VPN 5000 Concentrator

配置Cisco 3640路由器

思科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

根據需要，使用下列選單選項和引數配置VPN集中器。

- 要新增IKE提議，請選擇**Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Add a proposals**。
  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
- 要定義LAN到LAN隧道，請選擇**Configuration > System > Tunneling Protocols > IPSec LAN-to-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

- 要修改安全關聯，請選擇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 Concentrator

```
[ 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.
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對配置進行故障排除。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出**debug指令之前，請先參閱**有關Debug指令的重要資訊。

思科3640路由器

- **debug crypto engine** — 顯示有關執行加密和解密的加密引擎的調試消息。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。
- **debug crypto ipsec** — 顯示IPSec事件。
- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE安全關聯(SA)。
- **show crypto ipsec sa** — 顯示當前安全關聯使用的設定。
- **clear crypto isakmp** — （從配置模式）清除所有活動的IKE連線。
- **clear crypto sa** — （從配置模式）刪除所有IPSec安全關聯。

PIX

- **debug crypto ipsec** — 顯示第2階段的IPSec協商。
- **debug crypto isakmp** — 顯示第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- **debug crypto engine** — 顯示加密的流量。
- **show crypto ipsec sa** — 顯示第2階段安全關聯。
- **show crypto isakmp sa** — 顯示第1階段安全關聯。
- **clear crypto isakmp** — （從配置模式）清除網際網路金鑰交換(IKE)安全關聯。
- **clear crypto ipsec sa** — （從配置模式）清除IPSec安全關聯。

VPN 3000 Concentrator

- — 通過選擇**Configuration > System > Events > Classes > Modify**(Severity to Log=1-13, Severity to Console=1-3)啟動VPN 3000 Concentrator調試：IKE、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE
- — 可以通過選擇**Monitoring > Event Log**來清除或檢索事件日誌。
- — 可在**Monitoring > Sessions**中監控LAN到LAN通道流量。
- — 可在**管理>管理會話> LAN到LAN會話>操作 — 註銷**中清除隧道。

VPN 5000 Concentrator

- **vpn trace dump all** — 顯示有關所有匹配的VPN連線的資訊，包括有關時間、VPN編號、對等體的實際IP地址、已運行哪些指令碼的資訊，以及在發生錯誤的情況下顯示發生錯誤的軟體代碼的常式和行號。
- **show vpn statistics** — 顯示使用者、合作夥伴的以下資訊以及兩者的總計。（對於模組化型號，顯示屏包括每個模組插槽的部分。）當前活動 — 當前活動的連線。在Negot中 — 當前正在協商的連線。高水位線 — 自上次重新啟動以來併發活動連線的最大數量。Running Total — 自上次重新啟動後成功的連線總數。Tunnel Starts — 隧道啟動次數。Tunnel OK — 沒有錯誤的通道數。Tunnel Error — 發生錯誤的通道數。
- **show vpn statistics verbose** — 顯示ISAKMP協商統計資訊以及更多活動連線統計資訊。

相關資訊

- Cisco VPN 5000系列集中器銷售終止公告
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定
- 技術支援 - Cisco Systems