# Microsoft Windows 2000 サーバとCiscoデバイス間のIPSec 設定

## 内容



## 概要

このドキュメントでは、2 つのプライベート ネットワークに参加するための、事前共有キーを使用した IPSec トンネルを構成する方法を示します。シスコ デバイス内部のプライベート ネットワーク（192.168.l.X）内部および Microsoft 2000 Server 内部のプライベート ネットワーク（10.32.50.X）。シスコ デバイス内部と 2000 Server 内部からのインターネットへのトラフィック（ここでは 172.18.124.X ネットワークで表します）は、この設定を開始する前から流れているものと想定します。

Microsoft Windows 2000 Server 設定に関する詳細情報は、次の Microsoft ウェブ サイトにあります。http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

## はじめに

### 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

## 前提条件

このドキュメントに関しては個別の前提条件はありません。

## 使用するコンポーネント

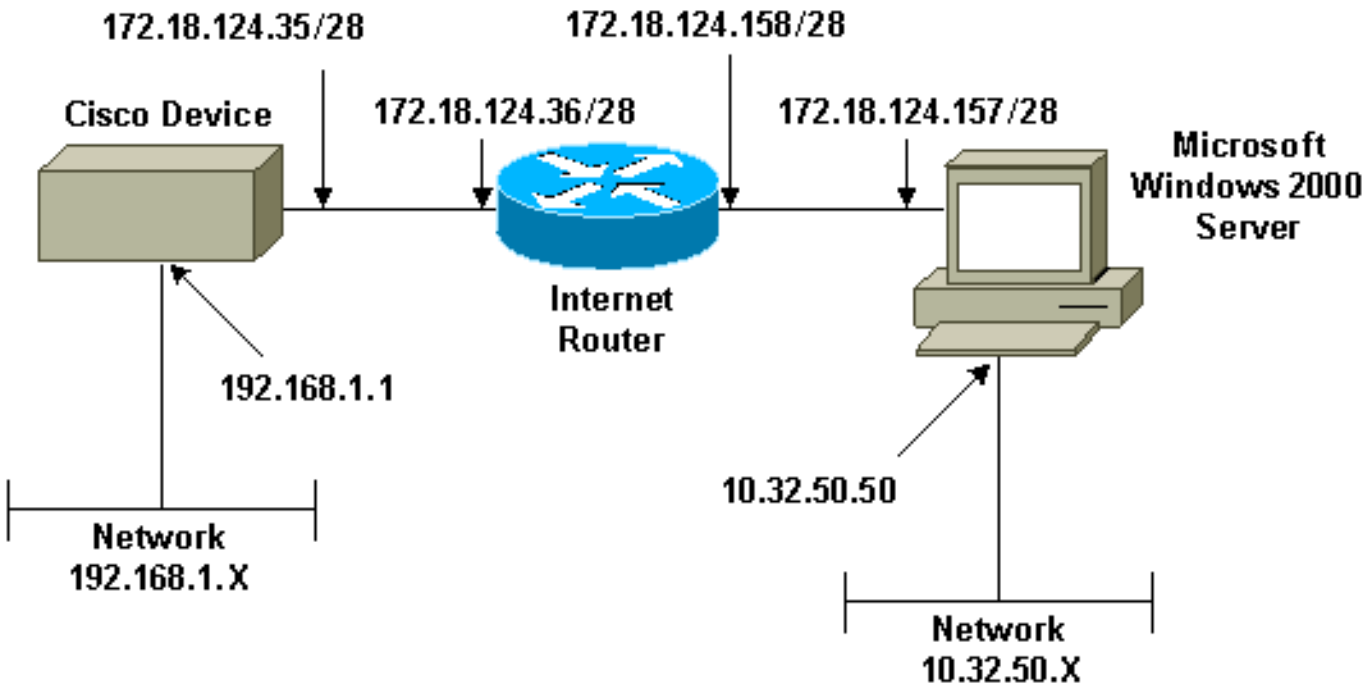
この構成は、次のソフトウェアとハードウェアのバージョンを使用して開発およびテストされています。

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640 ルータと Cisco IOS(R) Software リリース c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall と PIX Software リリース 5.2.1
- Cisco VPN 3000 コンセントレータ と VPN 3000 コンセントレータ ソフトウェア バージョン 2.5.2.F
- Cisco VPN 5000 コンセントレータ と VPN 5000 コンセントレータ ソフトウェア バージョン 5.2.19

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

## ネットワーク図

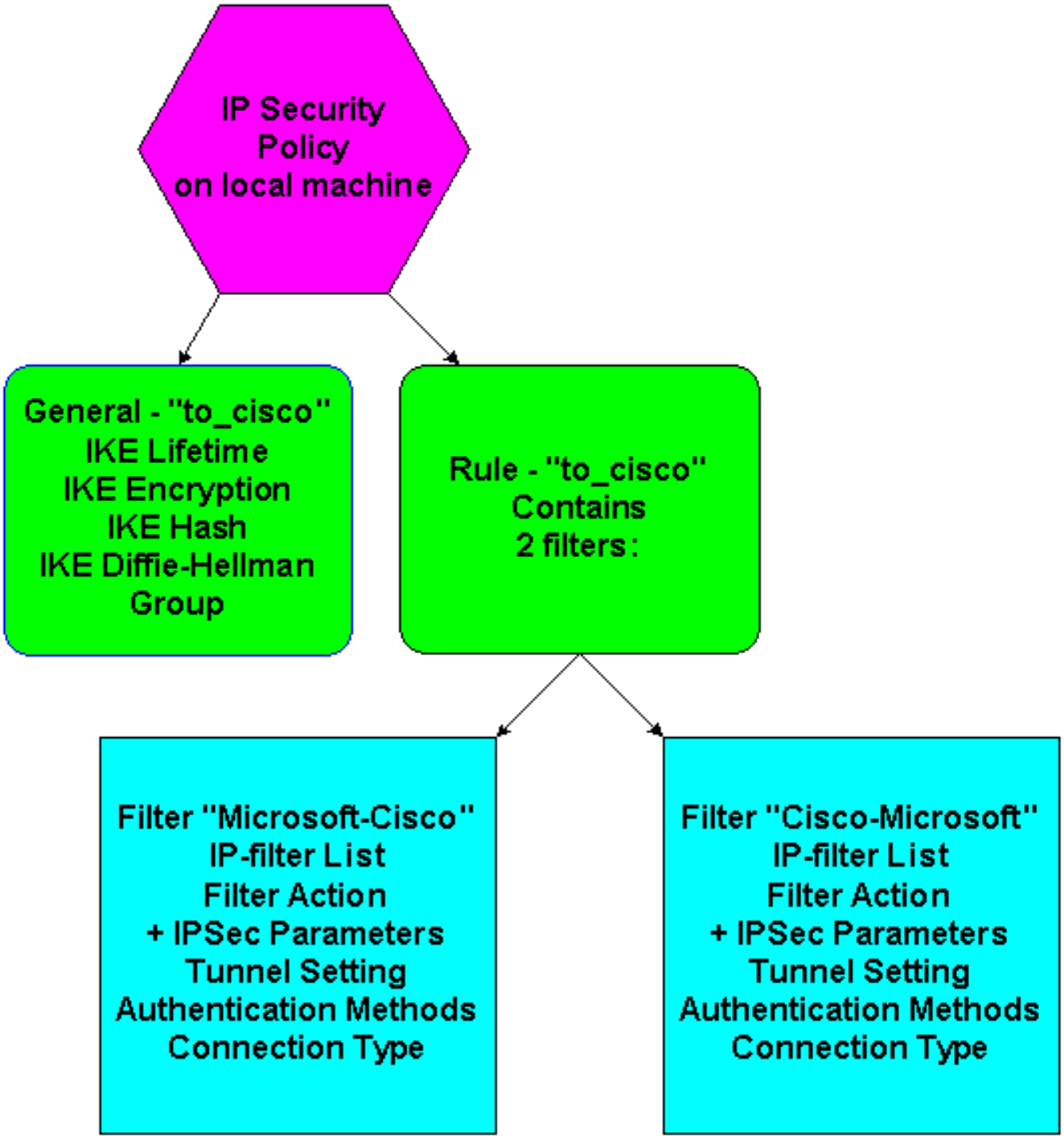
このドキュメントでは次の図に示すネットワーク構成を使用しています。




# Microsoft Windows 2000 Server とシスコ デバイスを連携させるための設定

## 実行されるタスク

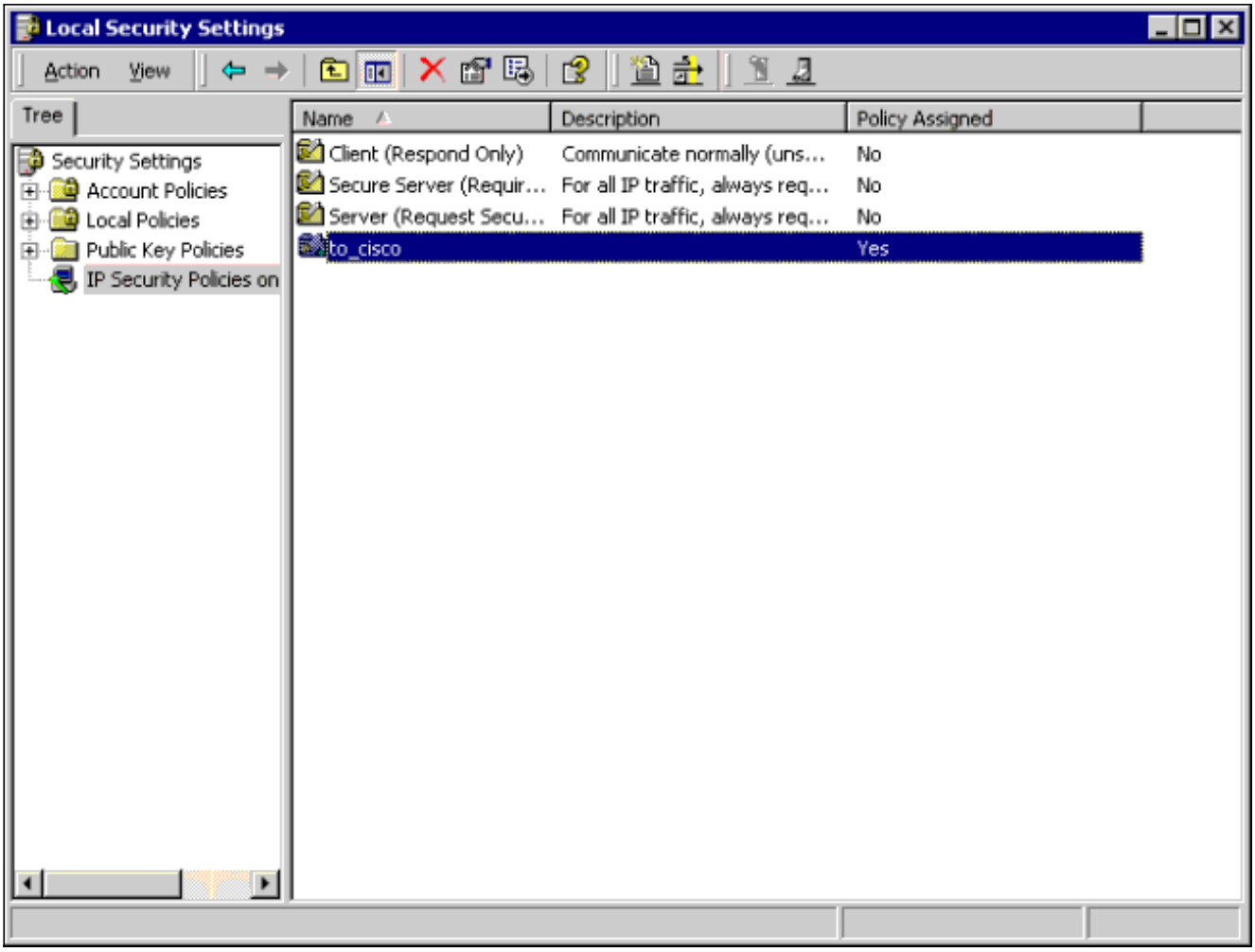
次の図は、Microsoft Windows 2000 サーバの設定で実行するタスクを示しています。



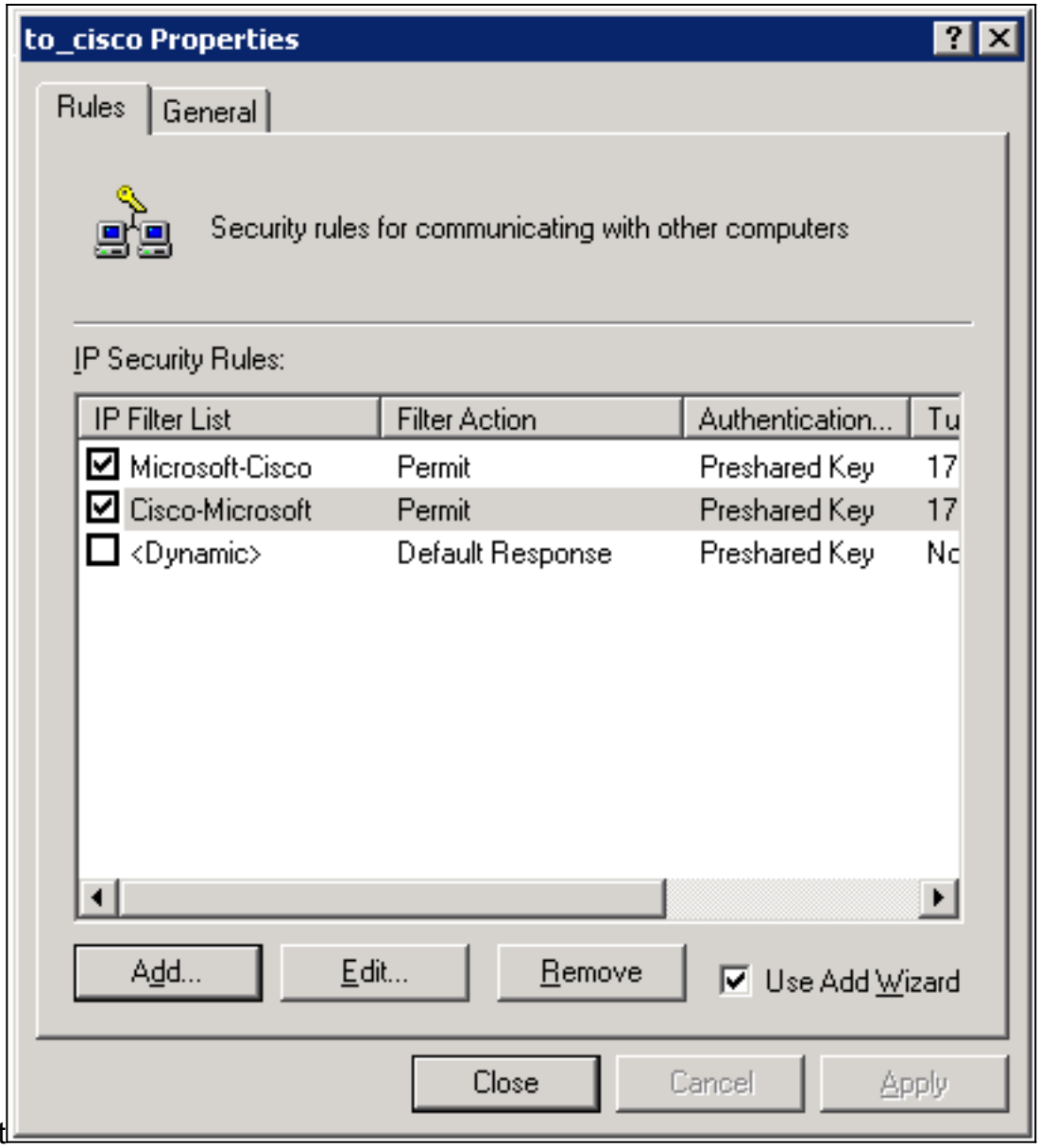

## 手順ごとの説明

MicrosoftのWebサイトで設定の手順に従った 、次の手順を使用して、設定がシスコデバイスで動作することを確認します。コメントと変更が、スクリーン キャプチャとともに示されています。

1. Microsoft Windows 2000 Server の [スタート] > [実行] > [secpol.msc] をクリックして、次の画面で情報を検証します。Microsoft ウェブ サイトの手順を使用して 2000 サーバを設定した後で、次のトンネル情報が表示されています。**注：例**のルールは「to_cisco」と呼ばれます。

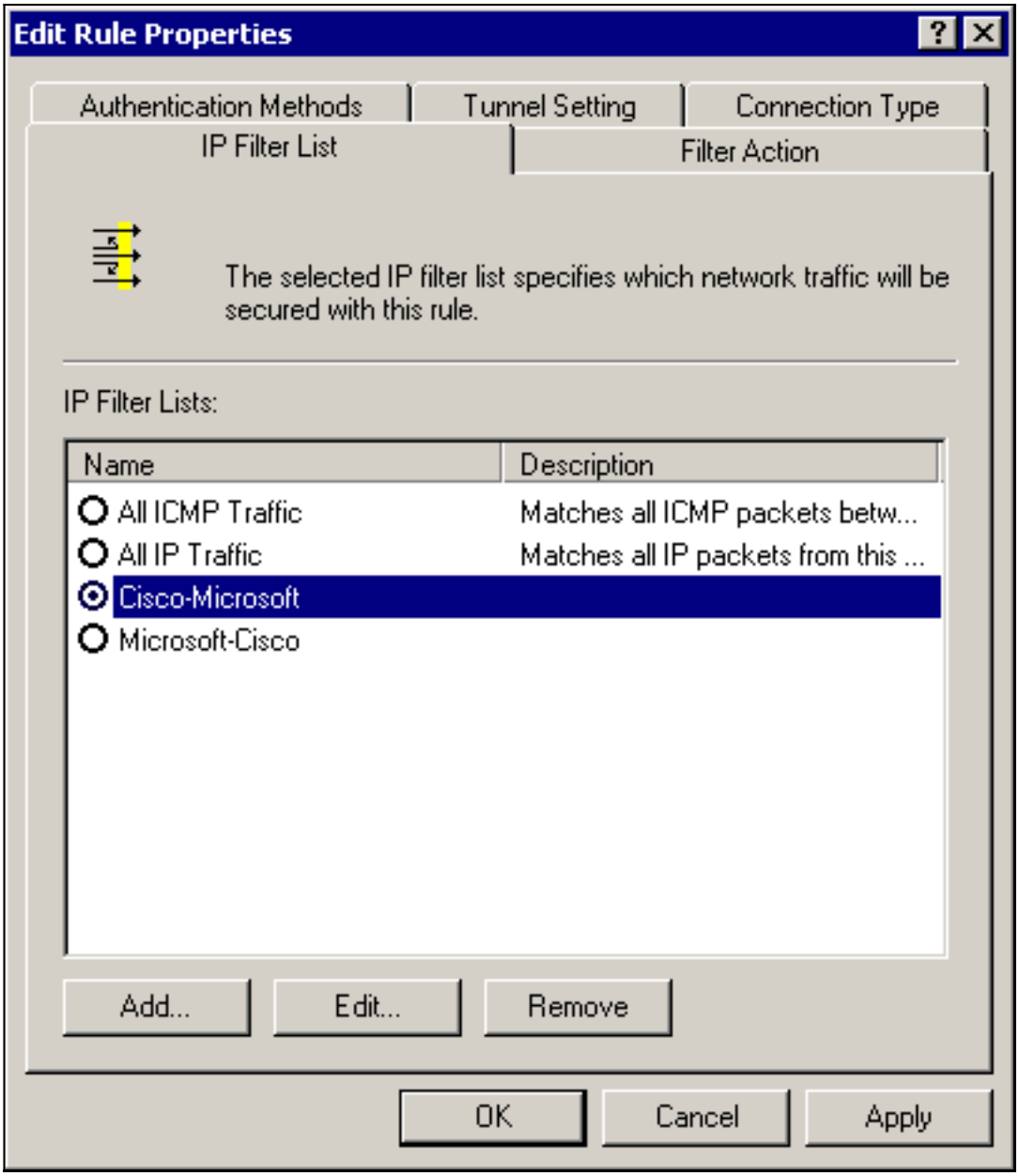



2. このルールの例には、2つのフィルタが含まれています。Microsoft-CiscoおよびCisco-

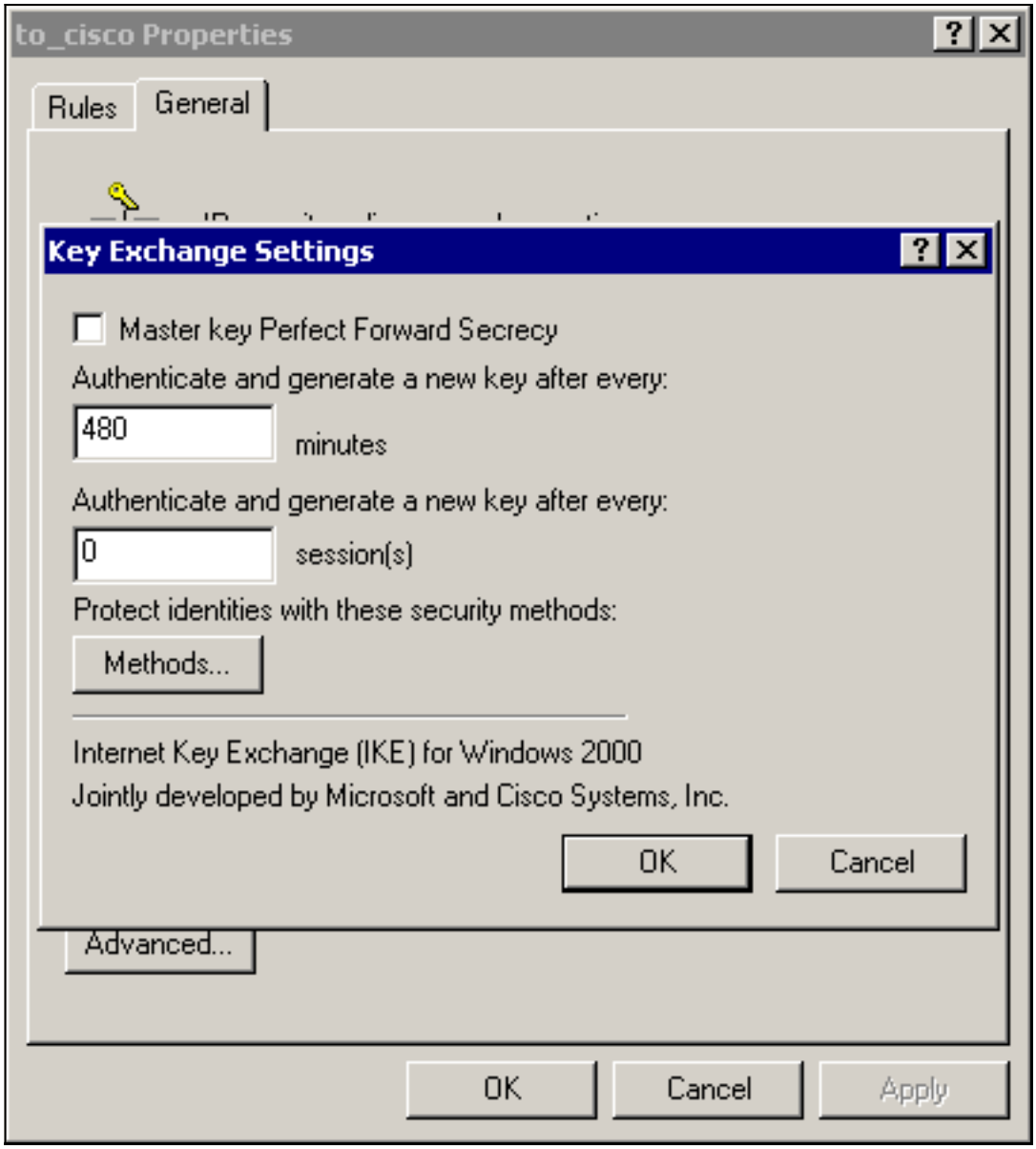



Microsoft

3. Cisco-Microsoft IP Security Ruleを選択し、**Edit**をクリックして、IPフィルタリストを表示/追加/編集します。

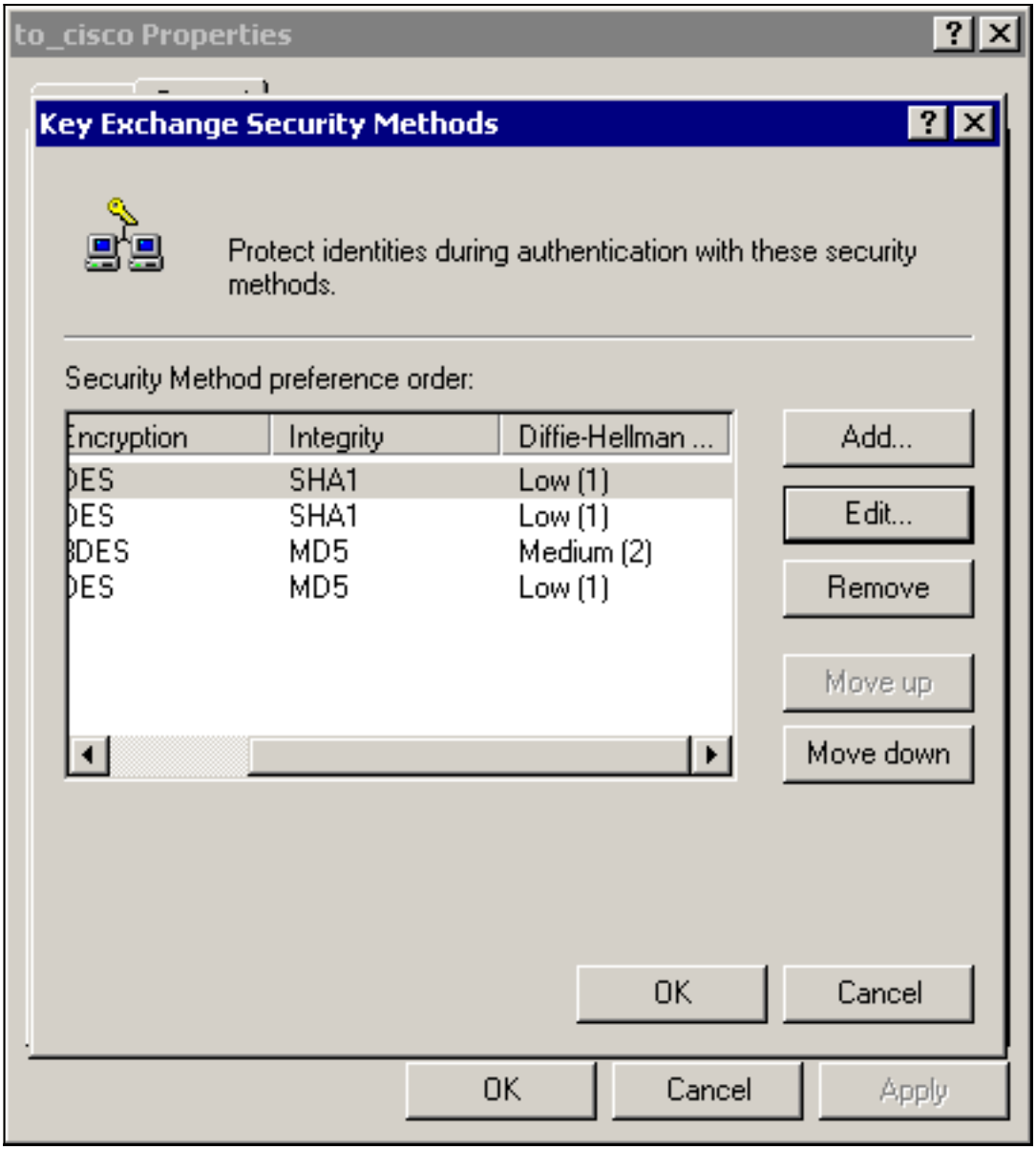



4. ルールの[一般] > [詳細] タブには IKE ライフタイム（480 分 = 28800 秒）が表示されていま

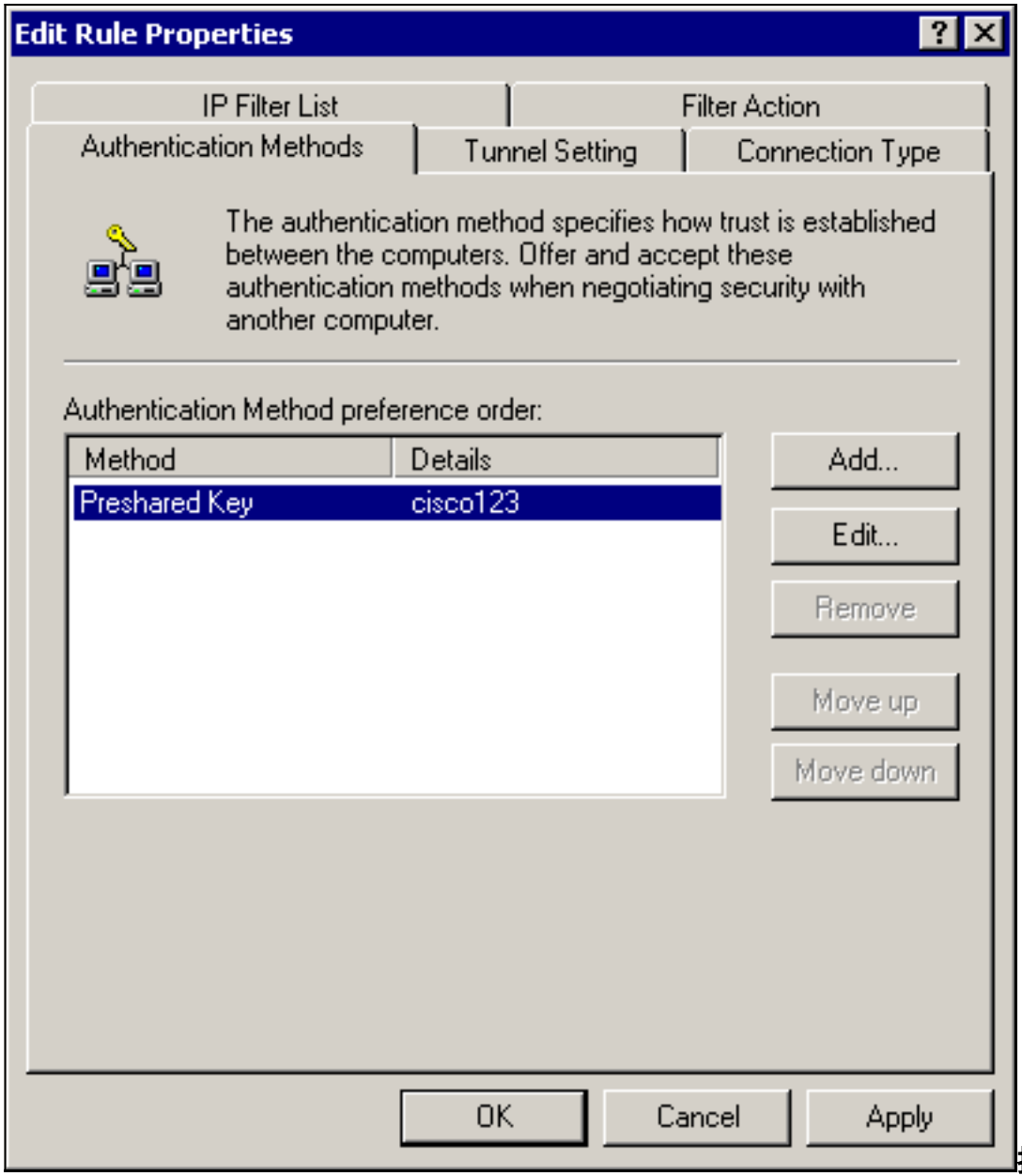



す。

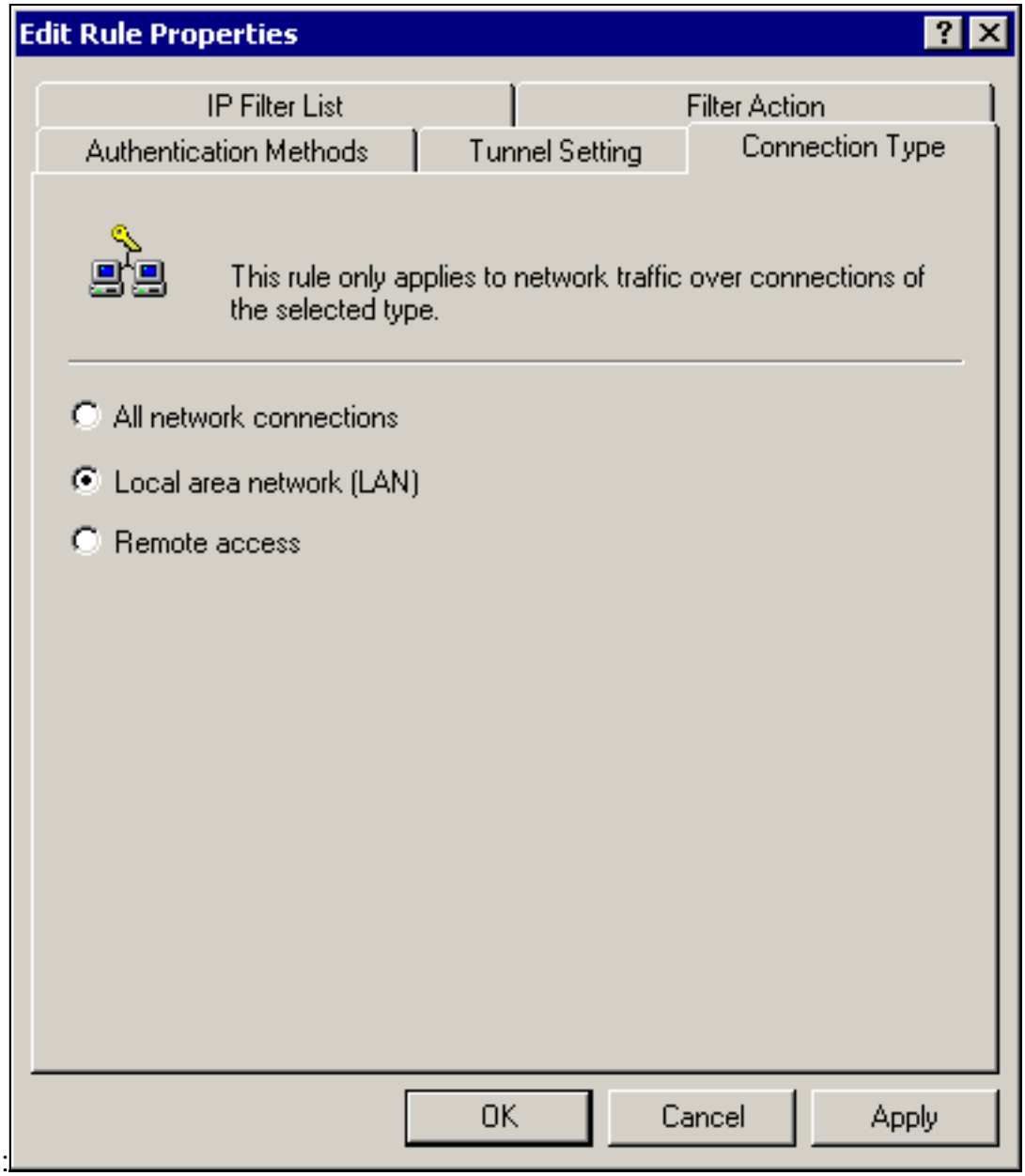
5. ルールの [一般] > [詳細] > [方式] タブには IKE 暗号化方式（DES）、IKE ハッシング（SHA1）、および Diffie-Helman グループ（Low(1)）が表示されています。



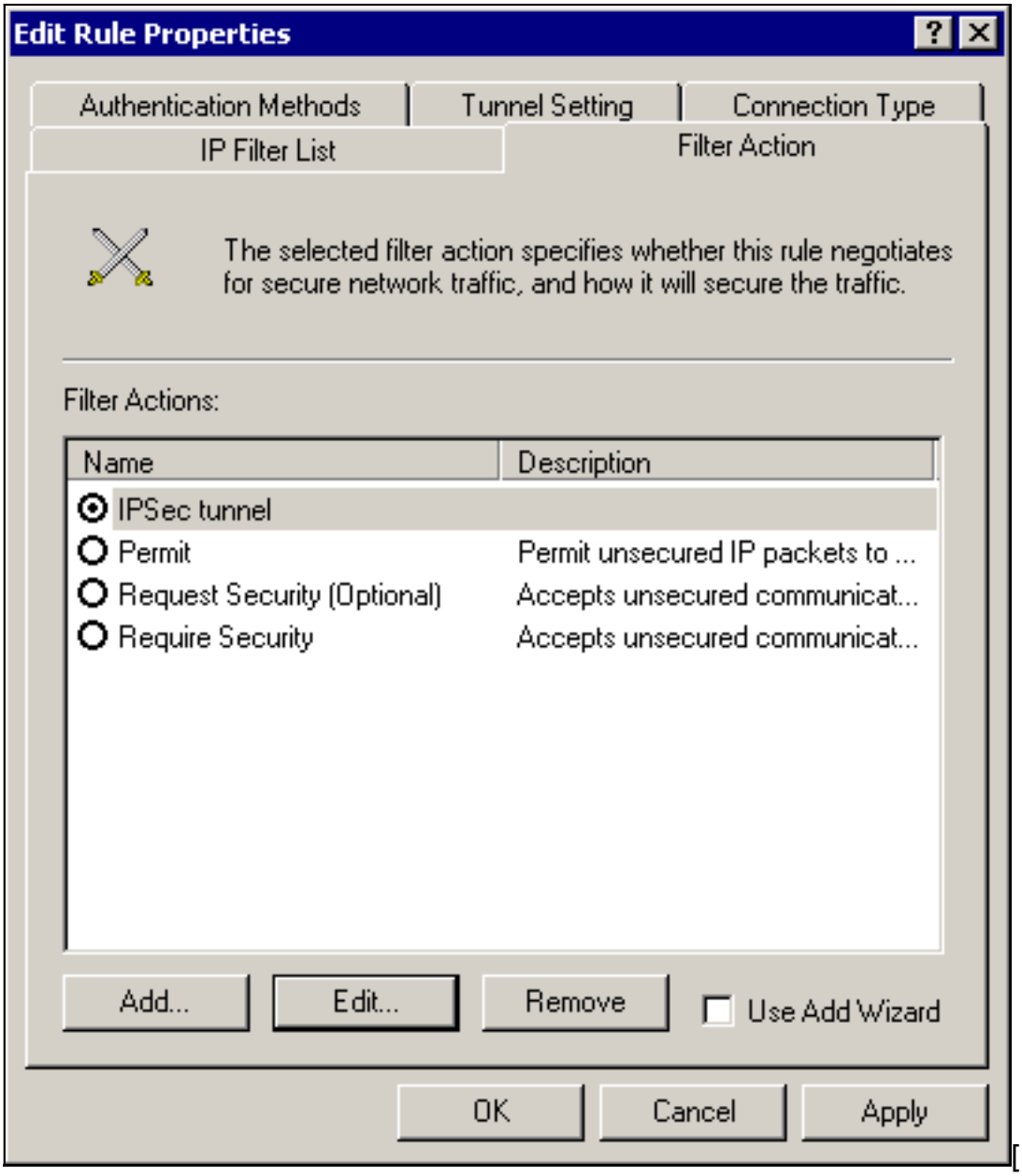

6. 各フィルタには、5 つのタブがあります。**認証方式 ( IKE の事前共有キー**


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

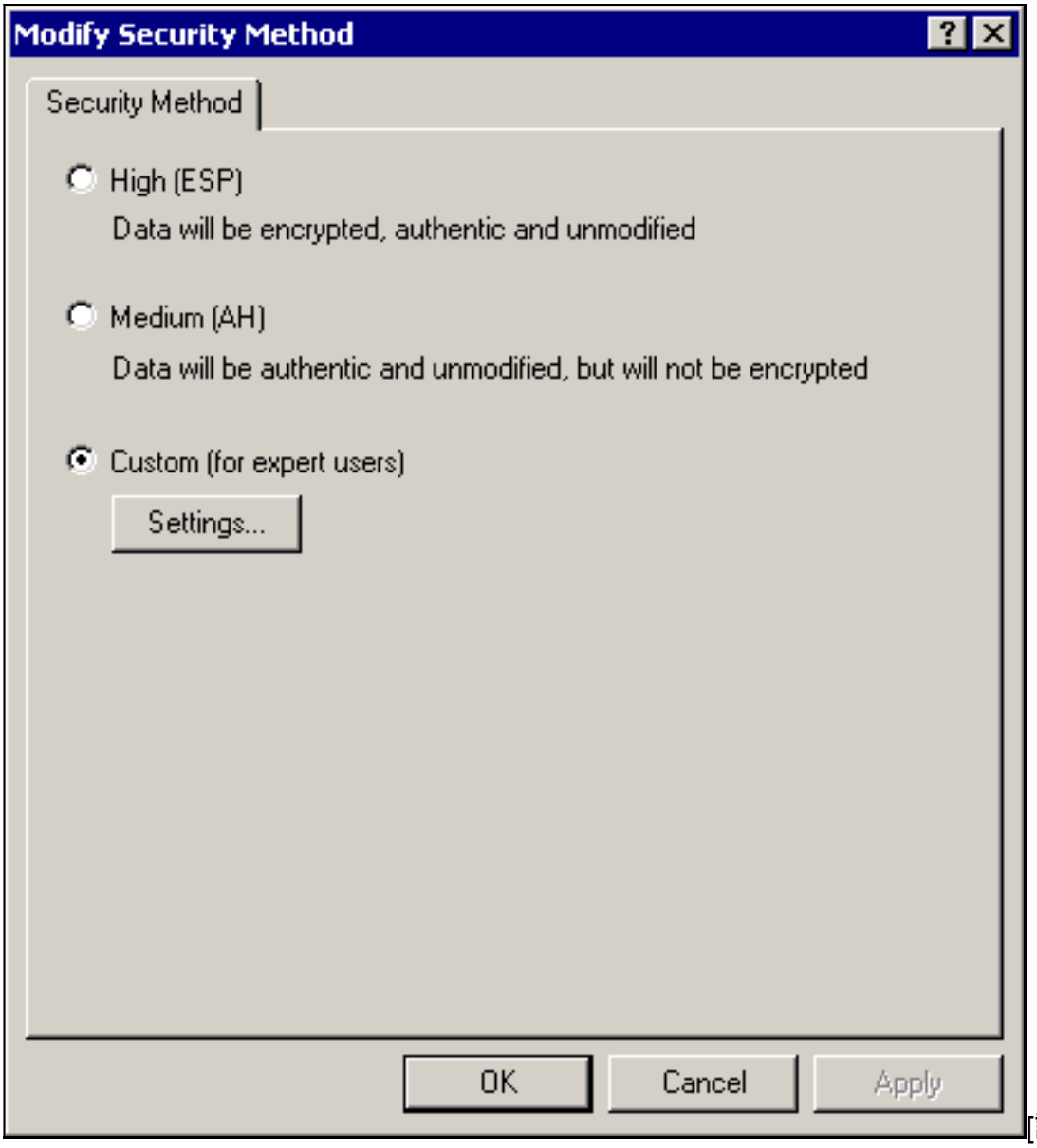
**接続タイプ**


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

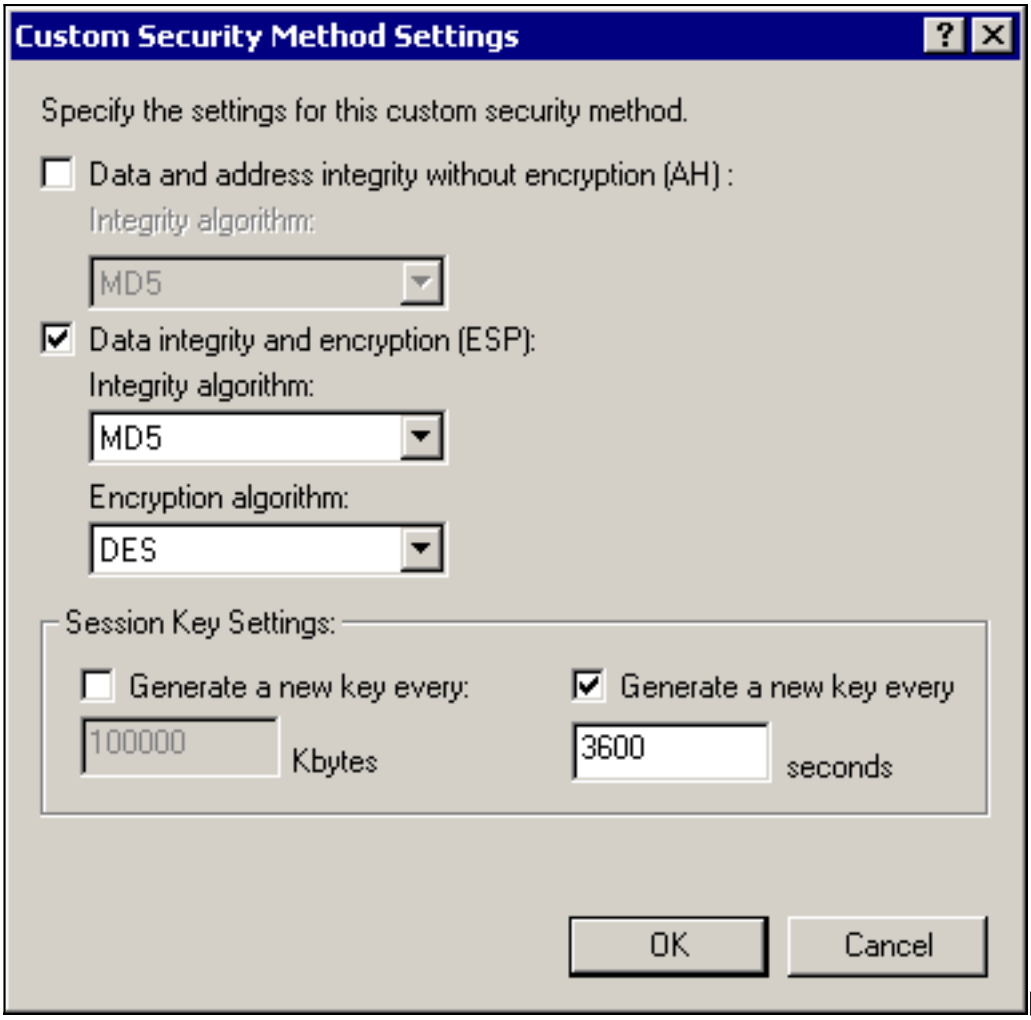
(LAN):**フィルタの動作**



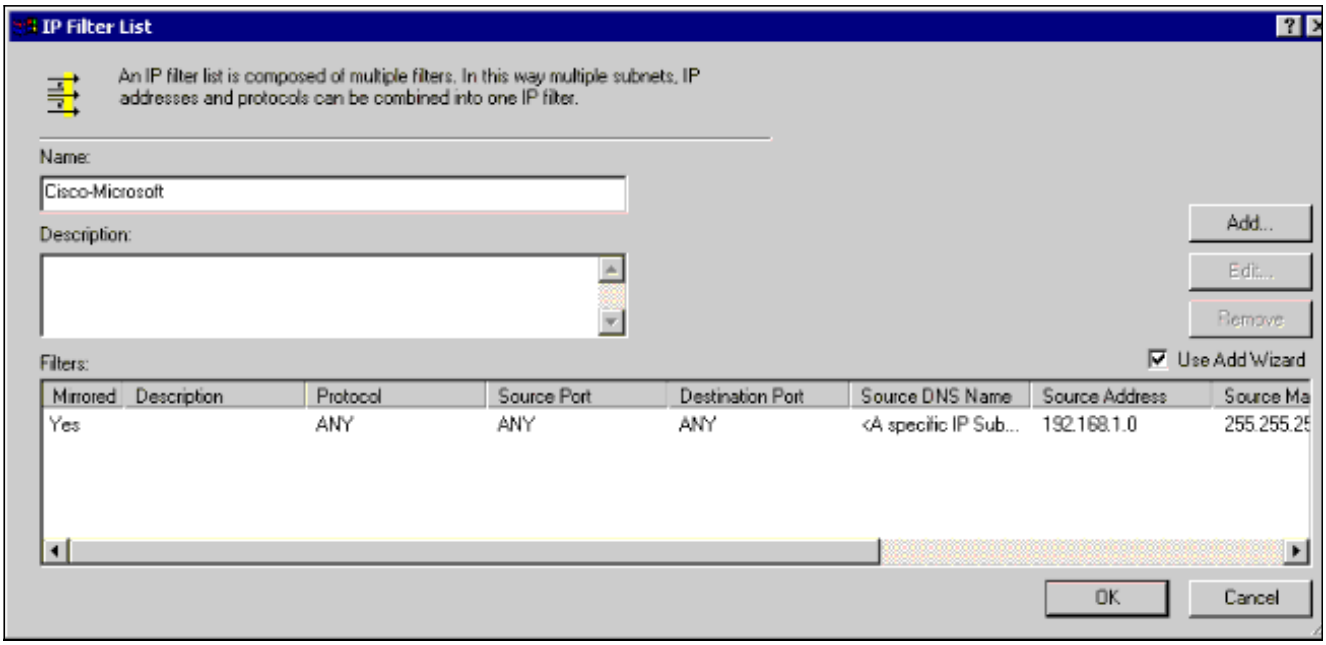

( IPSec ) [フィルタの動作] > [IPSec トンネル] > [編集] > [編集]を選択して、[カスタム]をクリックします。



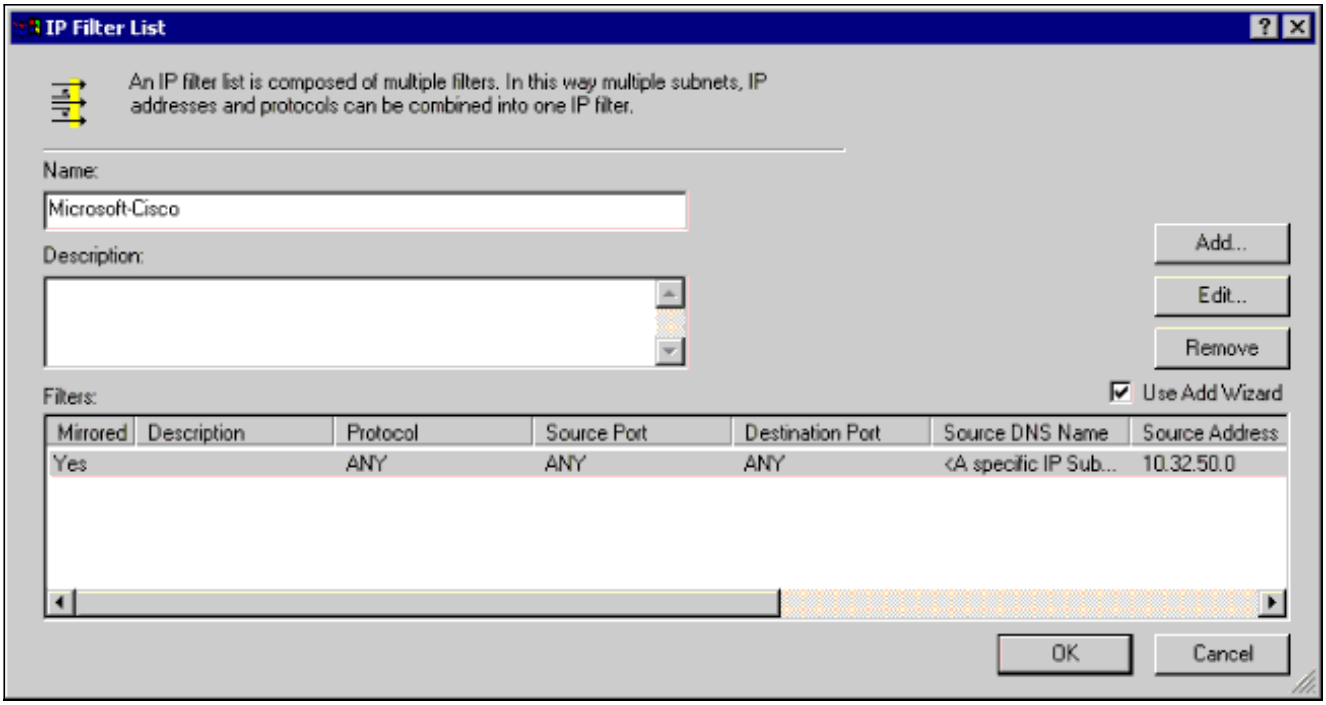

[設定値] - [IPSec トランスフォーム] と [IPSec ライフタイム] をクリックします。



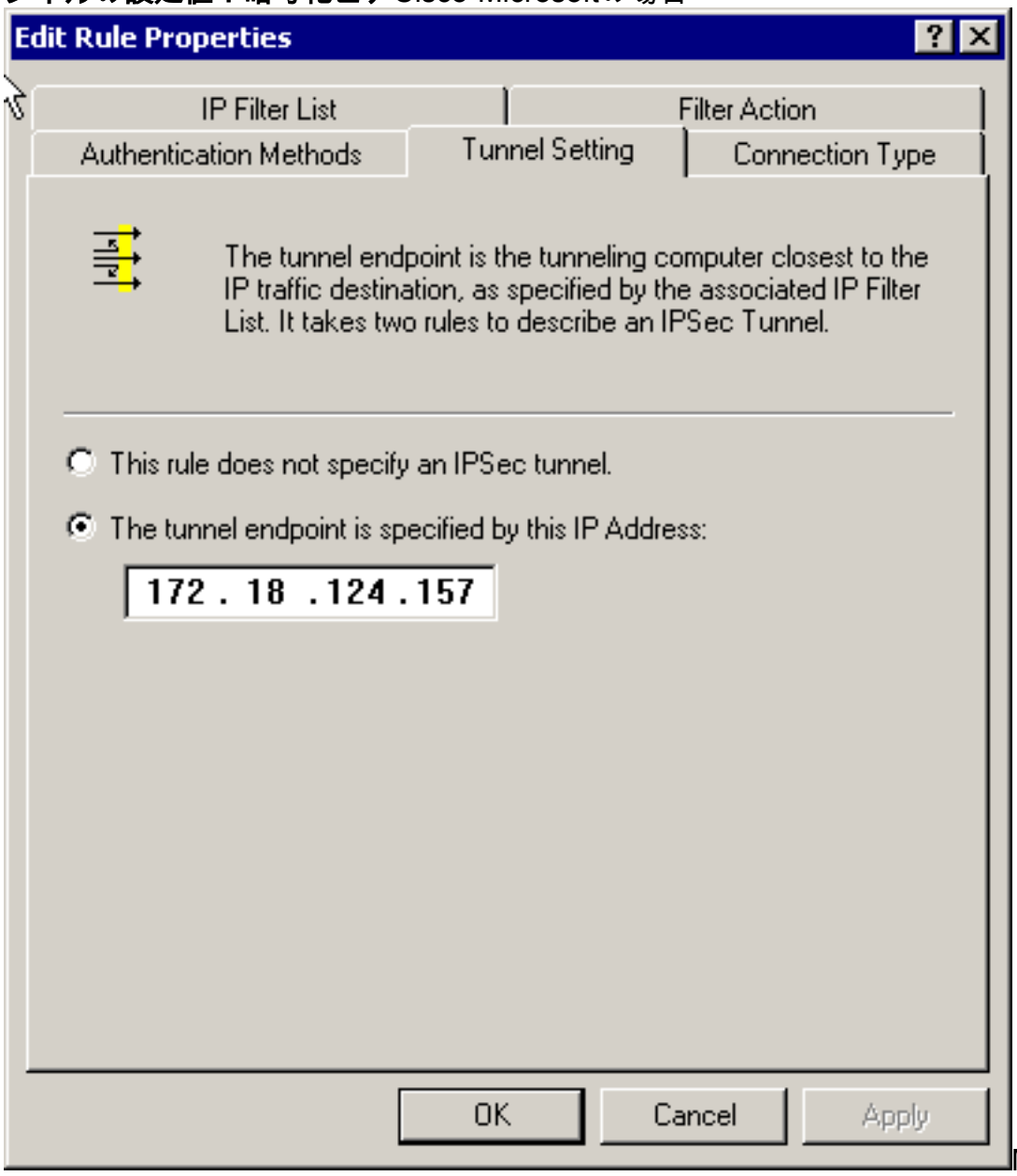

**IPフィルタリスト – 暗号化する**送信元**および**宛先ネットワーク：Cisco-Microsoftの場合
：




Microsoft-
Cisco:

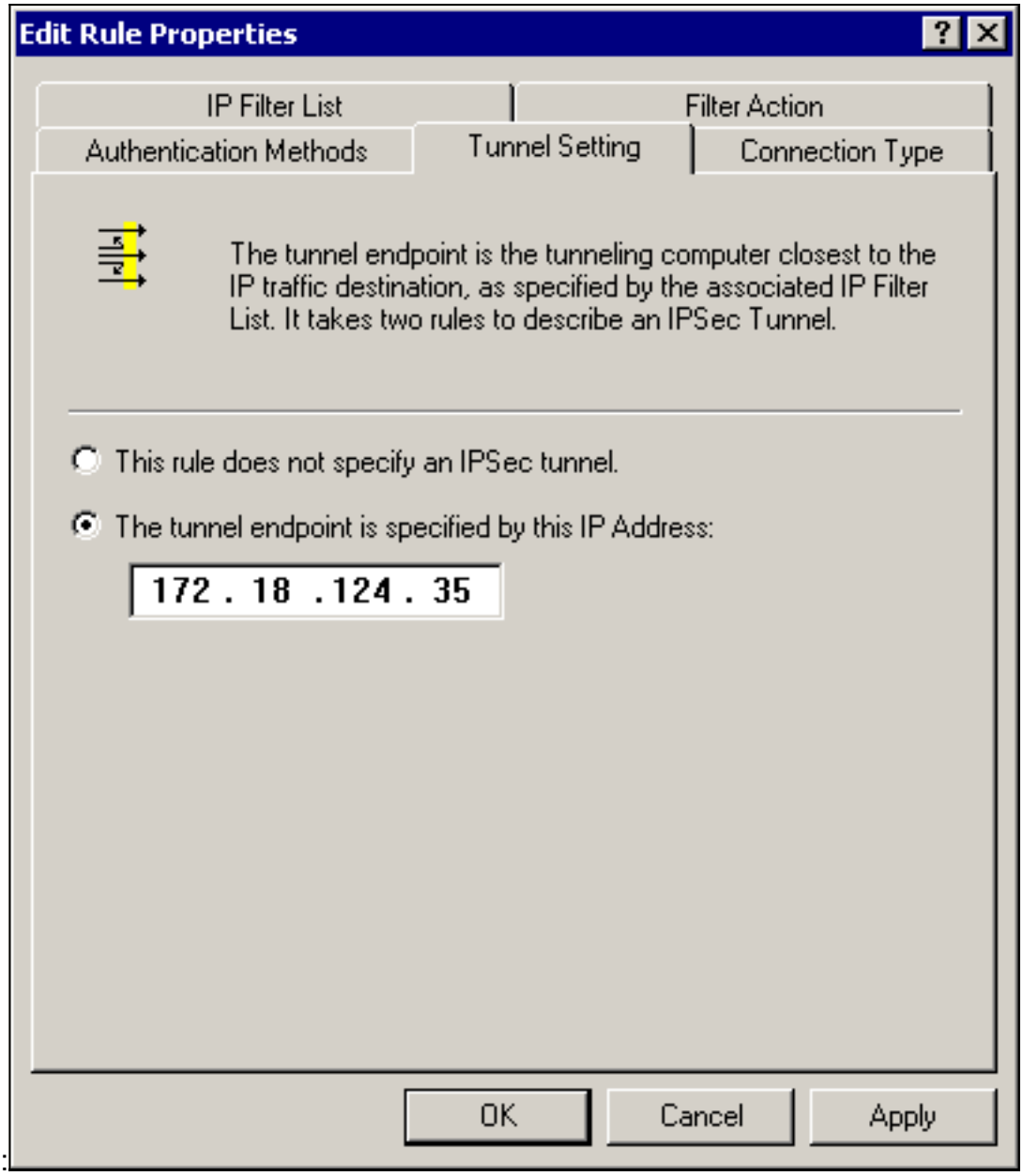



**トンネルの設定値：暗号化ピア**Cisco-Microsoftの場合




: Microsoft-

Cisco:




## Ciscoデバイスの設定

次の例に示すように、Ciscoルータ、PIX、およびVPNコンセントレータを設定します。

- Cisco 3640 ルータ
- PIX
- VPN 3000 コンセントレータ
- VPN 5000 コンセントレータ

### Cisco 3640 ルータの設定

| Cisco 3640 ルータ |
| --- |
| Current configuration : 1840 bytes<br>!<br>version 12.1<br>no service single-slot-reload-enable<br>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
```

## PIX の設定

**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
```

## VPN 3000 コンセントレータの設定

必要に応じてVPNコンセントレータを設定するには、次に示すメニューオプションとパラメータを使用します。

- [設定] > [システム] > [トンネリング プロトコル] > [IPSec] > [IKE 提案] > [提案の追加]：
  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
- LAN-to-LANトンネルを定義するには、**Configuration > System > Tunneling Protocols > IPSec LAN-to-LANの順に選択します。**
  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

- セキュリティアソシエーションを変更するには、[Configuration] > [Policy Management] > [Traffic Management] > [Security Associations] > [Modify]を選択します。

```
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
```

## VPN 5000 コンセントレータの設定

**VPN 5000 コンセントレータ**

```
[ 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.
```

# 確認

現在、この設定に使用できる確認手順はありません。

# トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

## トラブルシューティングのためのコマンド

一部の show コマンドはアウトプット インタープリタ ツールによってサポートされています（登録ユーザ専用）。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

**注：debug コマンドを使用する前に、「debug コマンドに関する重要な情報」を参照してください。**

## Cisco 3640 ルータ

- **debug crypto engine ：暗号化と暗号解除を実行する crypto エンジンに関するデバッグ メッセージを表示します。**
- **debug crypto isakmp ：IKE イベントに関するメッセージを表示します。**
- **debug crypto ipsec ：IPSec イベントを表示します。**
- **show crypto isakmp sa**：ピアの現在の IKE セキュリティ アソシエーション（SA）すべてを表示します。
- **show crypto ipsec sa ：現在の SA が使用する設定を表示します。**
- **clear crypto isakmp ：（設定モードから）すべてのアクティブな IKE 接続をクリアーします。**
- **clear crypto sa ：（設定モードから）すべての IPSec SAを削除します。**

## PIX

- **debug crypto ipsec：IPSec ネゴシエーションのフェーズ 2 を表示します。**
- **debug crypto isakmp - フェーズ 1 の Internet Security Association and Key Management Protocol（ISAKMP）ネゴシエーションを表示します。**
- **debug crypto engine：暗号化されたトラフィックを表示します。**
- **show crypto ipsec sa - フェーズ 2 のセキュリティ アソシエーションを表示します。**
- **show crypto isakmp sa - フェーズ 1 のセキュリティ結合を表示します。**
- **clear crypto isakmp ：（設定モードから）Internet Key Exchange（IKE） SA をクリアーします。**
- **clear crypto ipsec sa ：（設定モードから）IPSec SA を削除します。**

## VPN 3000 コンセントレータ

- VPN 3000 コンセントレータのデバッグを開始するために、[設定] > [システム] > [イベント] > [クラス] > [修正] を選択します（ログ重大度 =1-13、コンソール重大度 =1-3）:IKE、IKEDBG、IKEDECODE、IPSEC、IPSECDBG、IPSECDECODE
- イベント ログをクリアーまたは取得するには、[モニタリング] > [イベント ログ]を選択します。
- LAN-to-LAN トンネル トラフィックは[モニタリング] > [セッション]でモニタできます。
- トンネルをクリアーするには、[管理] > [セッションの管理] > [LAN-to-LAN セッション] > [アクション・ ログアウト]を選択します。

## VPN 5000 コンセントレータ

- **vpn trace dump all ：すべての一致する VPN 接続の情報を表示します。時間、VPN 番号、ピアの実際の IP アドレス、どのスクリプトが実行されているかの情報、そしてエラーの場合は**

**エラーが発生したソフトウェア コードのルーチンと回線番号が表示されます。**

- **show vpn statistics ：ユーザやパートナーの次の情報を表示します。**（モジュラ モデルでは、ディスプレイには各モジュール スロットのセクションが含まれます）。 Current Active ：現在アクティブな接続です。In Negot ：現在ネゴシエート中の接続です。High Water ：最後のリブート以降のアクティブな同時接続の最高数です。Running Total ：最後のリブート以降の成功した接続の合計数です。Tunnel Starts ：トンネル開始の数です。Tunnel OK ：エラーのないトンネルの数です。Tunnel Error ：エラーが発生したトンネルの数です。
- **show vpn statistics verbose ：ISAKMP ネゴシエーション統計情報と、さらに多数のアクティブ接続の統計情報を表示します。**

## 関連情報

- Cisco VPN 5000 シリーズ コンセントレータの販売終了のお知らせ
- IPSec ネットワーク セキュリティの設定
- Internet Key Exchange セキュリティ プロトコルの設定
- テクニカルサポート - Cisco Systems