Microsoft Windows 2000 Server와 Cisco 디바이스 간 IPSec 구성

목차

소개

이 문서에서는 미리 공유된 키를 사용하여 IPSec 터널을 형성하여 2개의 프라이빗 네트워크에 연결하는 방법을 설명합니다. Cisco 디바이스 내부의 프라이빗 네트워크(192.168.I.X) 및 Microsoft 2000 Server 내의 프라이빗 네트워크(10.32.50.X) 이 구성을 시작하기 전에 Cisco 디바이스 내부 및 2000 Server 내부에서 인터넷(172.18.124.X 네트워크로 표시)으로 이동하는 트래픽이 이동하는 것으로 가정합니다.

Microsoft 웹 사이트에서 Microsoft Windows 2000 서버를 구성하는 방법에 대한 자세한 내용을 확인할 수 있습니다. http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

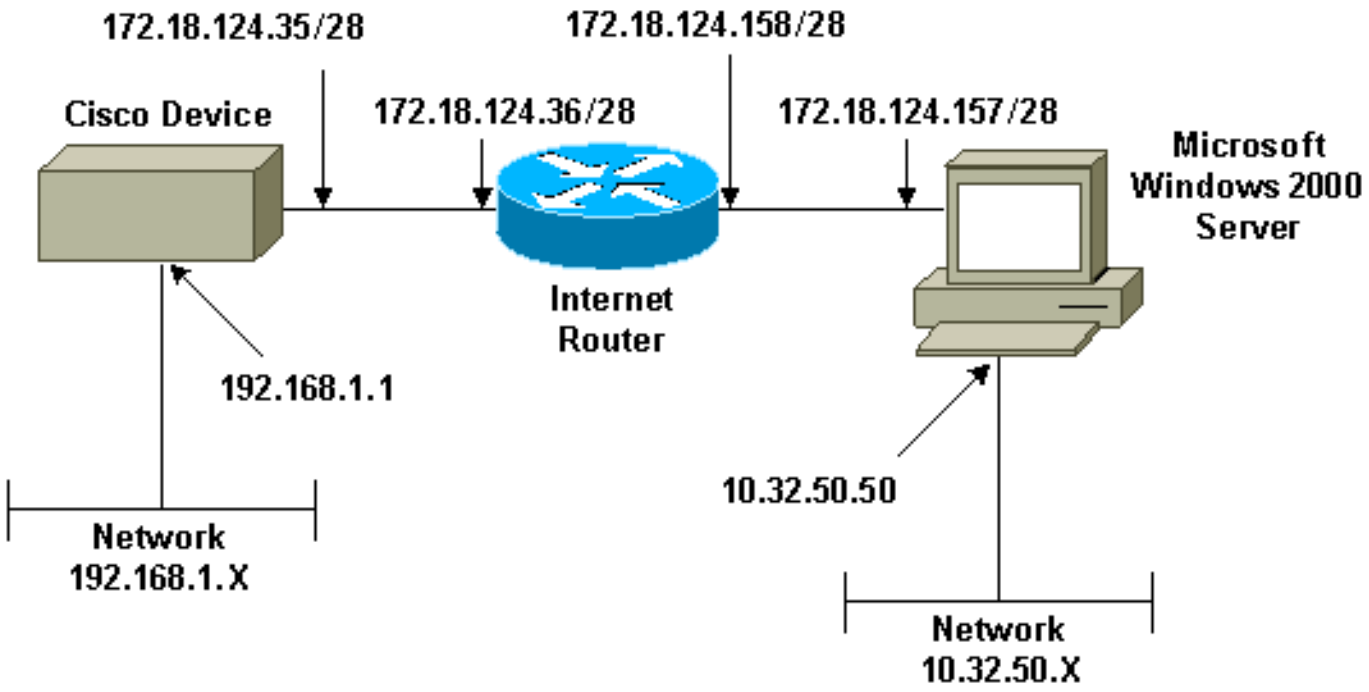
이러한 구성은 아래의 소프트웨어 및 하드웨어 버전을 사용하여 개발 및 테스트되었습니다.

- Microsoft Windows 2000 Server 5.00.2195
- Cisco IOS® 소프트웨어 릴리스 c3640-ik2o3s-mz.121-5.T.bin이 포함된 Cisco 3640 라우터
- Cisco Secure PIX Firewall with PIX Software 릴리스 5.2.1
- Cisco VPN 3000 Concentrator with VPN 3000 Concentrator Software 버전 2.5.2.F
- Cisco VPN 5000 Concentrator with VPN 5000 Concentrator 소프트웨어 버전 5.2.19

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

네트워크 다이어그램

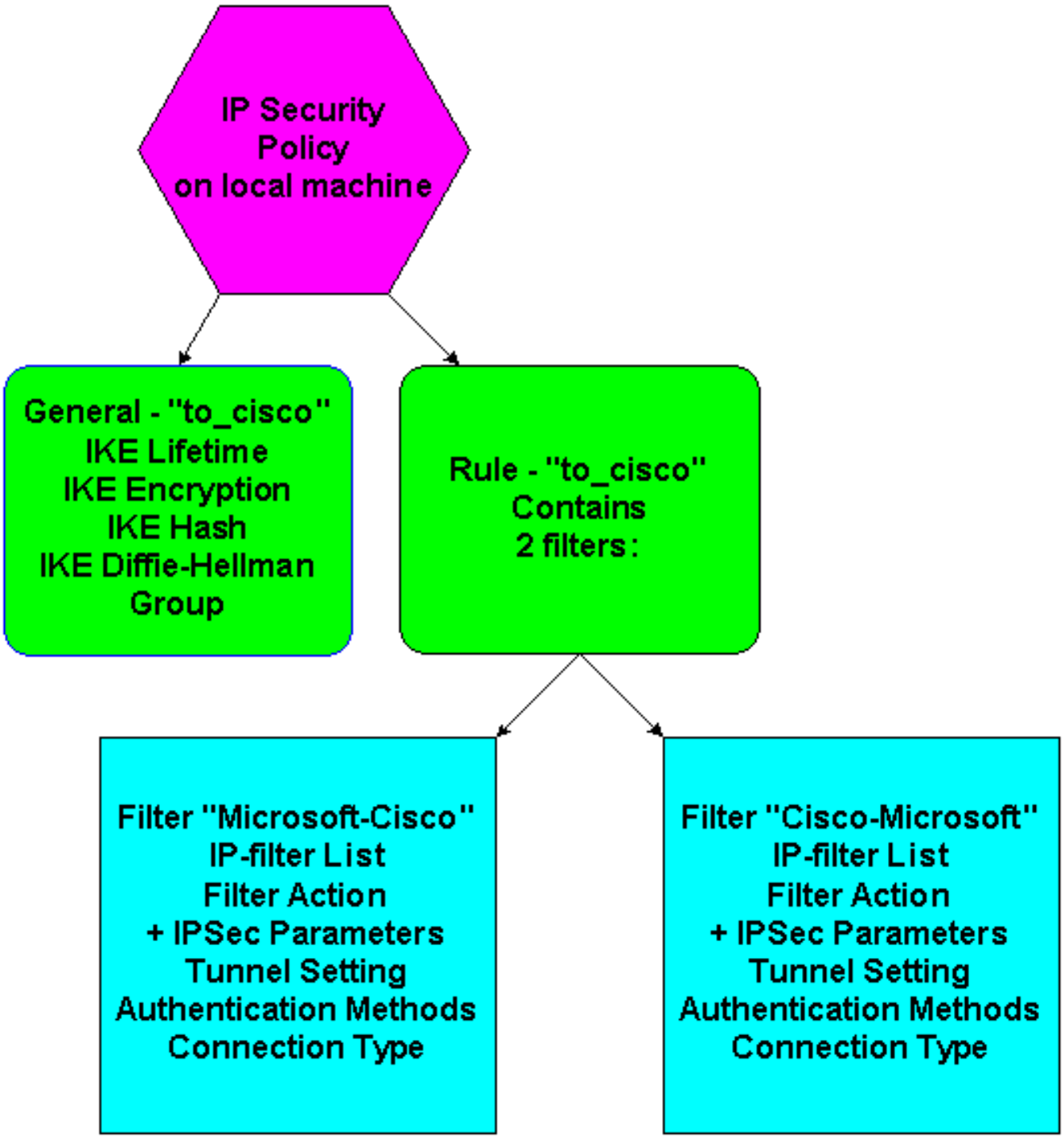
이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



Cisco 장치에서 작동하도록 Microsoft Windows 2000 Server 구성

수행된 작업

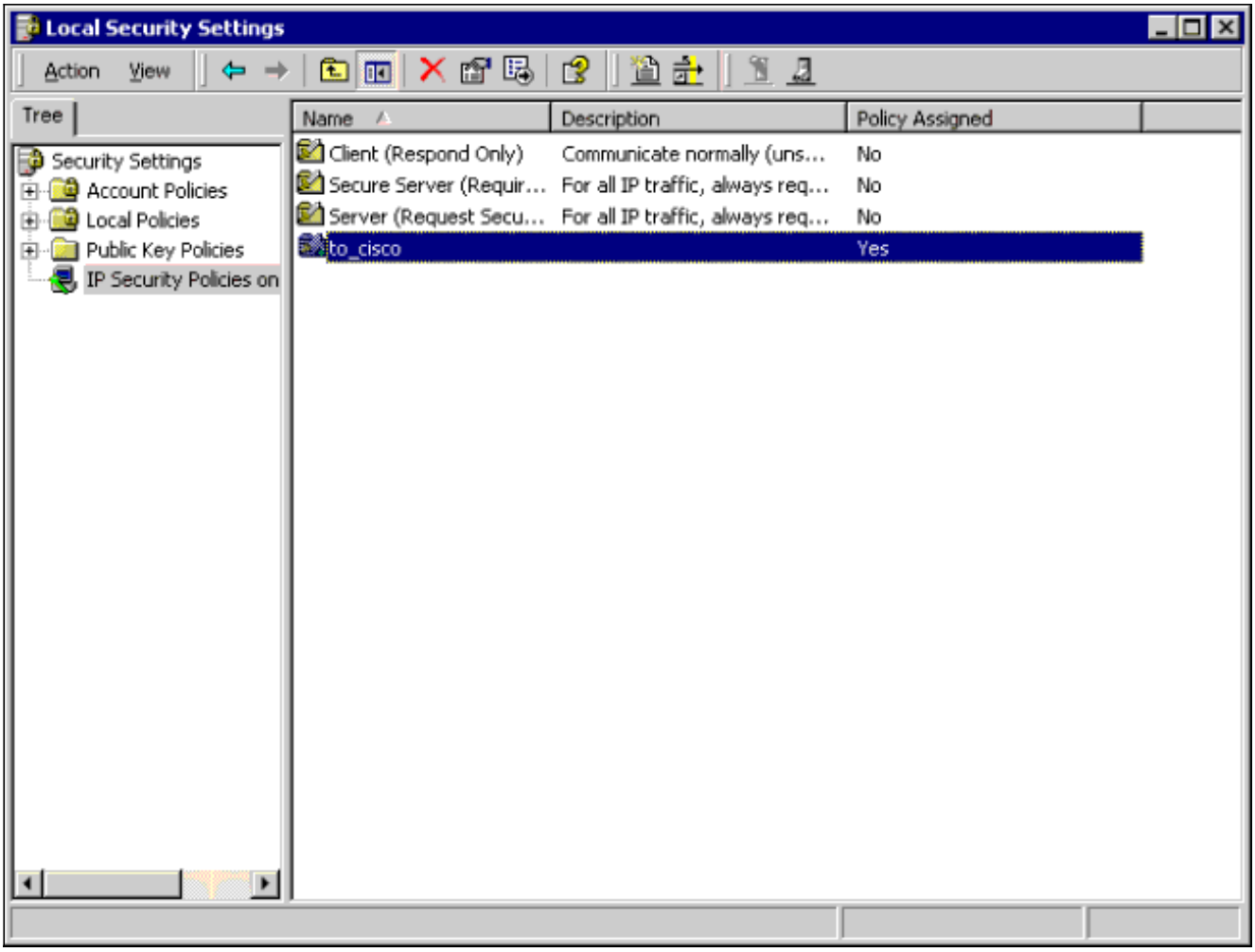
다음 다이어그램은 Microsoft Windows 2000 서버 구성에서 수행되는 작업을 보여 줍니다.



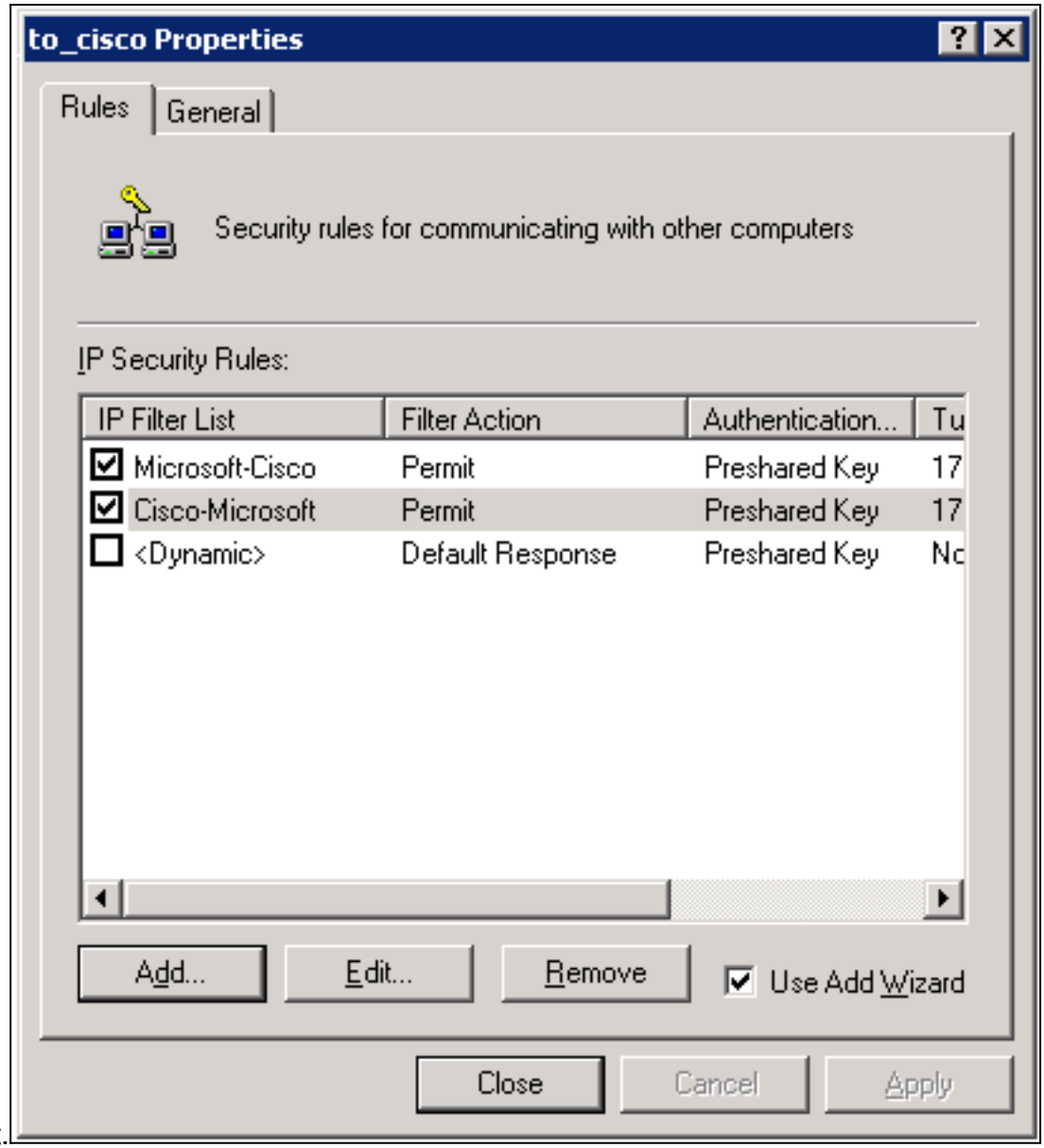
단계별 지침

Microsoft 웹 사이트의 컨피그레이션 지침 을 따랐으면 다음 단계를 사용하여 컨피그레이션이 Cisco 디바이스에서 작동할 수 있는지 확인합니다. 화면 캡처를 통해 코멘트와 변경 사항이 표시됩니다.

1. Microsoft Windows 2000 Server에서 **시작 > 실행 > secpol.msc를** 클릭하고 다음 화면의 정보를 확인합니다.Microsoft 웹 사이트의 지침을 사용하여 2000 서버를 구성하면 다음 터널 정보가 표시됩니다.**참고:** 예제 규칙을 "to_cisco"라고 합니다
   .

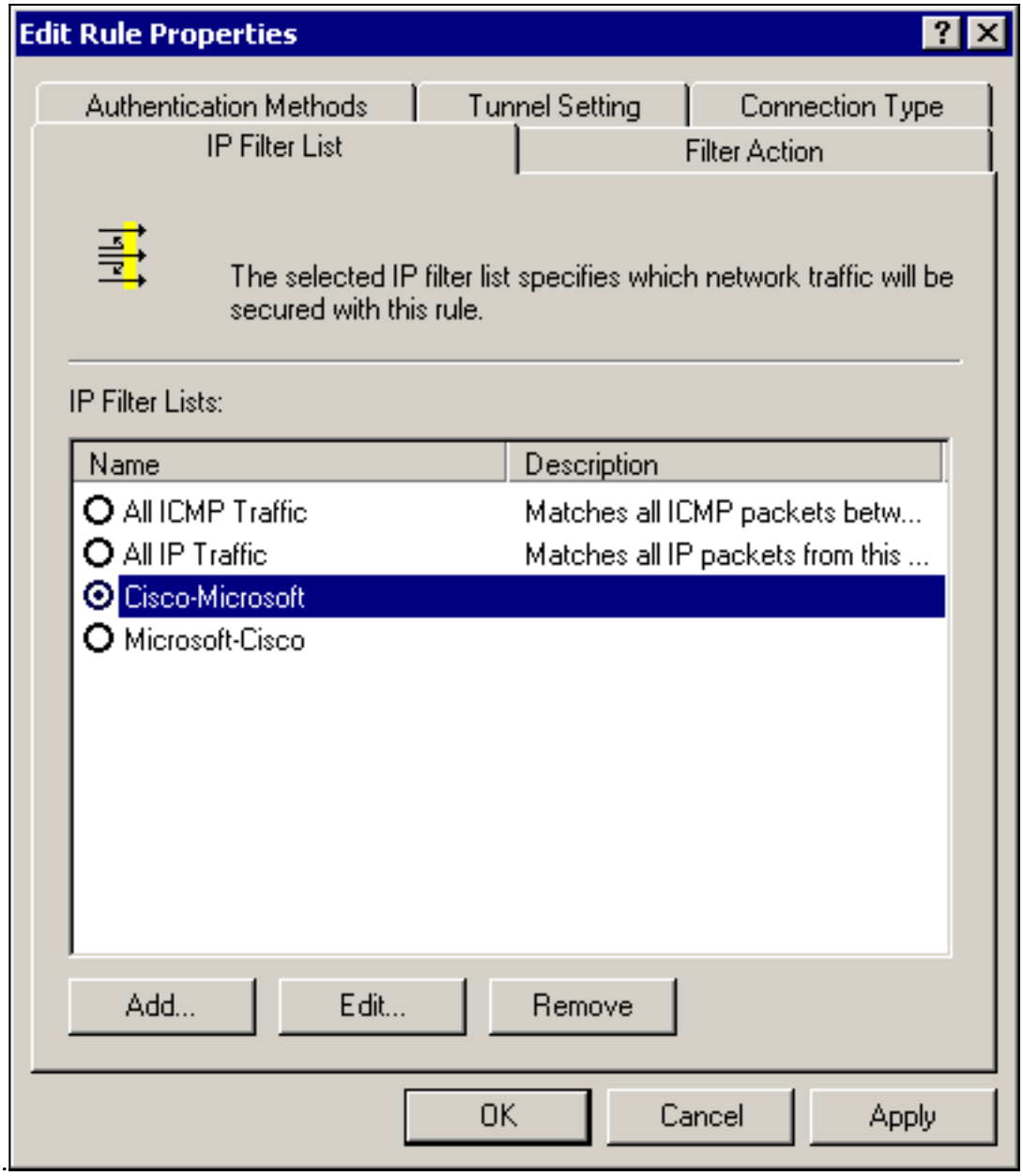


2. 이 예제 규칙에는 두 개의 필터가 있습니다. Microsoft-Cisco 및 Cisco-

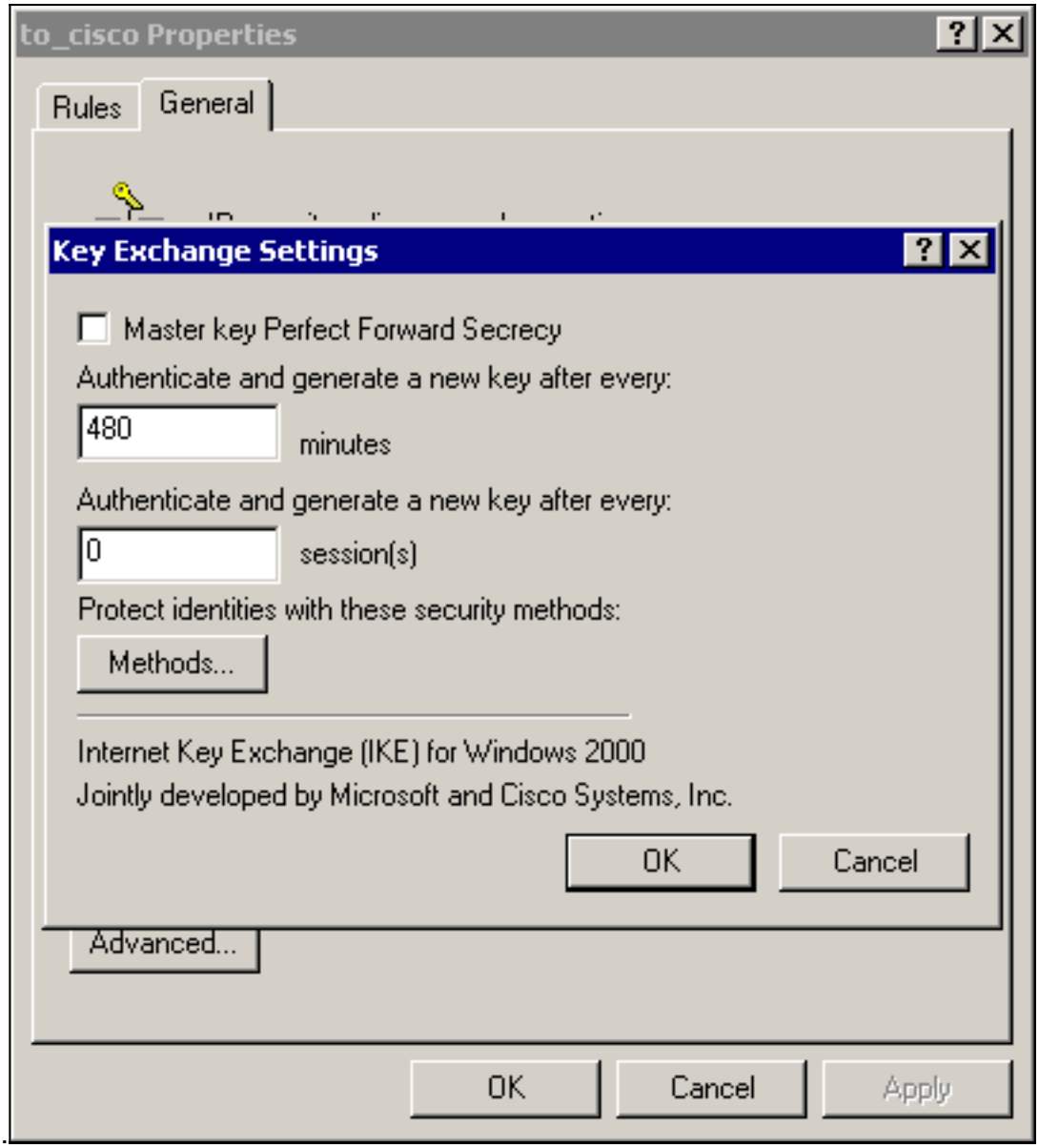


Microsoft.

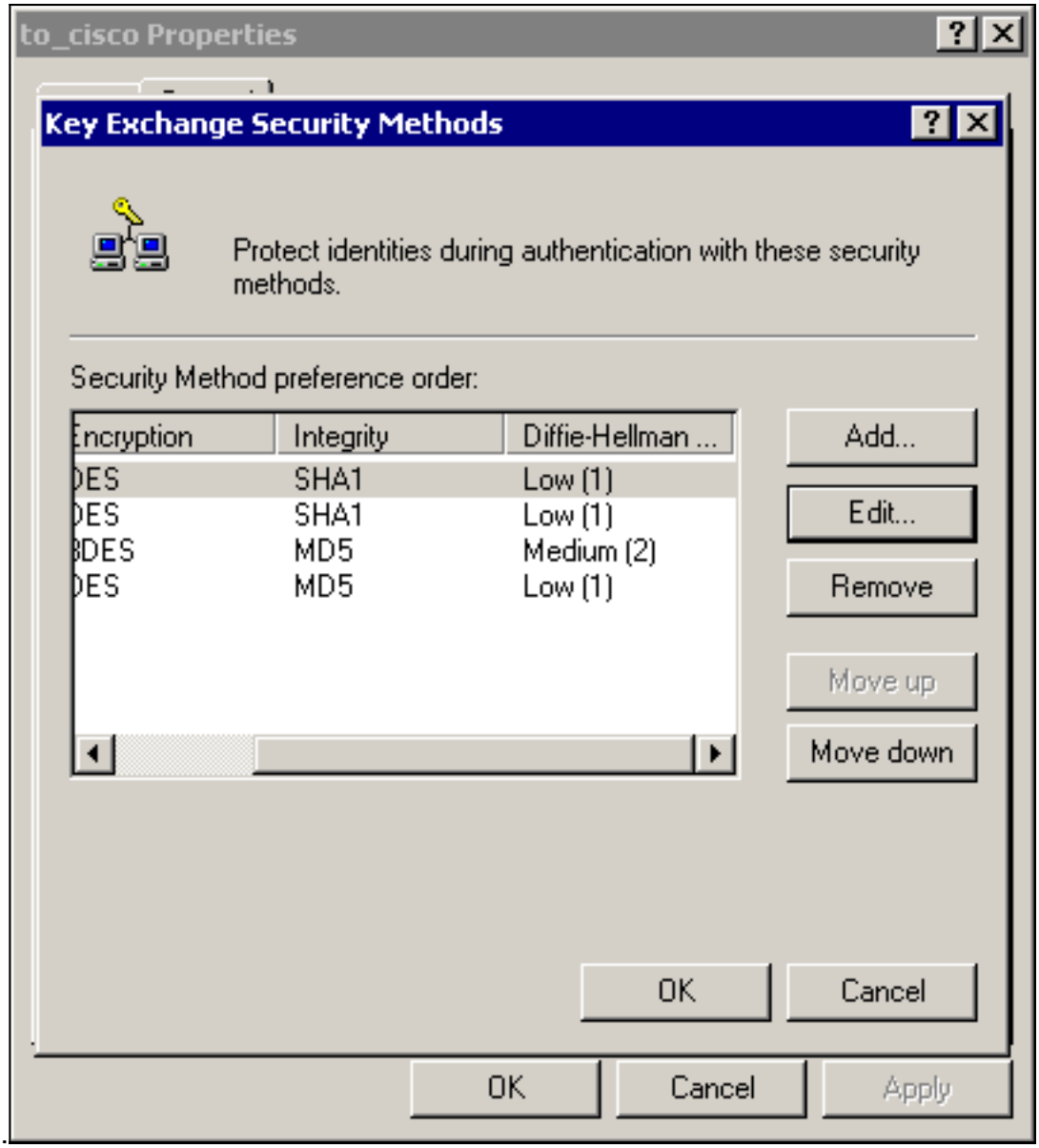
3. Cisco-Microsoft IP Security Rule(Cisco-Microsoft IP 보안 규칙)을 선택한 다음 **Edit(편집)**를 클릭하여 IP Filter Lists(IP 필터 목록)를 보거나 추가/편집합니다



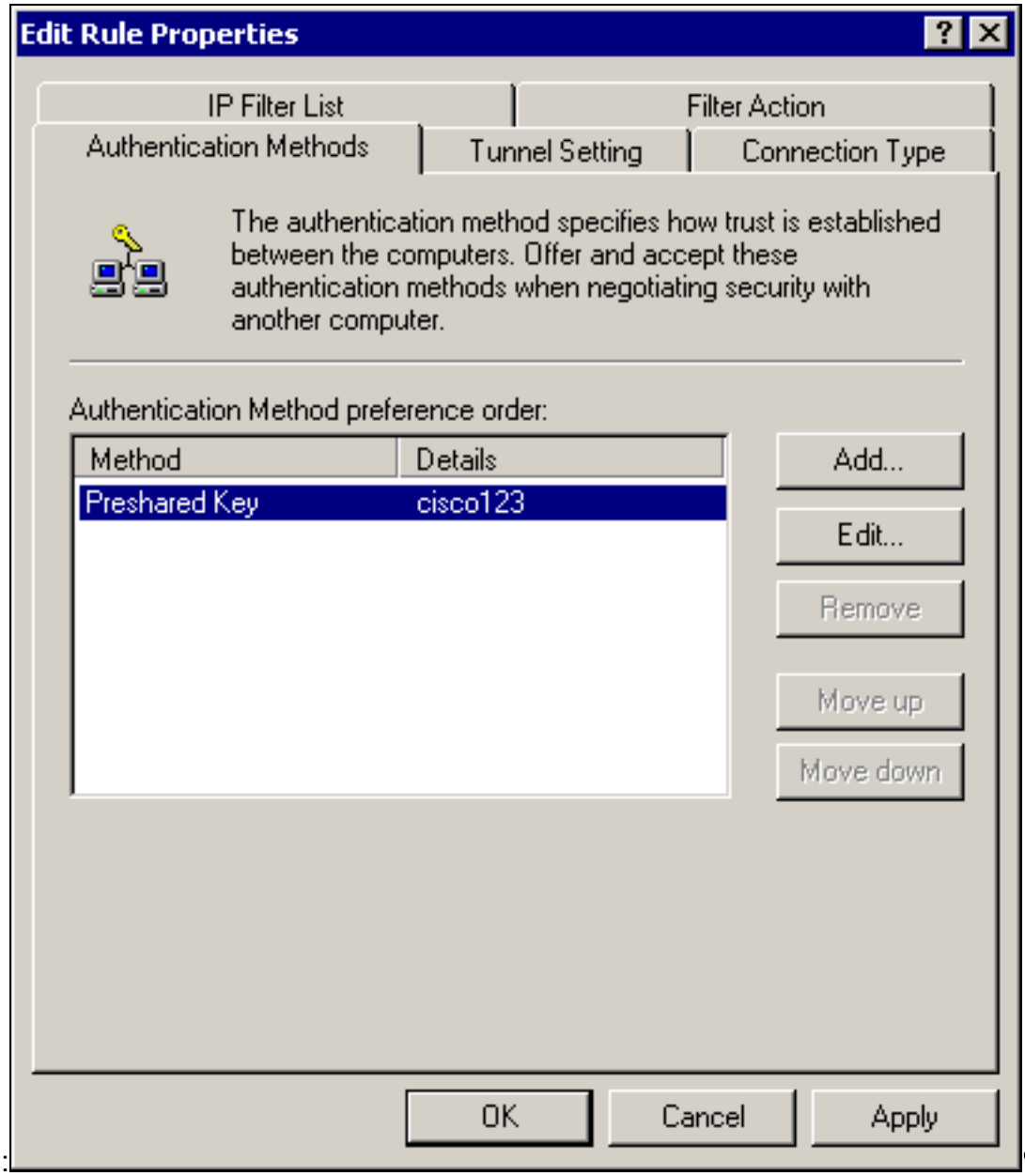
4. 규칙의 **General(일반) > Advanced(고급)** 탭에는 **IKE 수명**(480분 = 28800초)이 있습니다

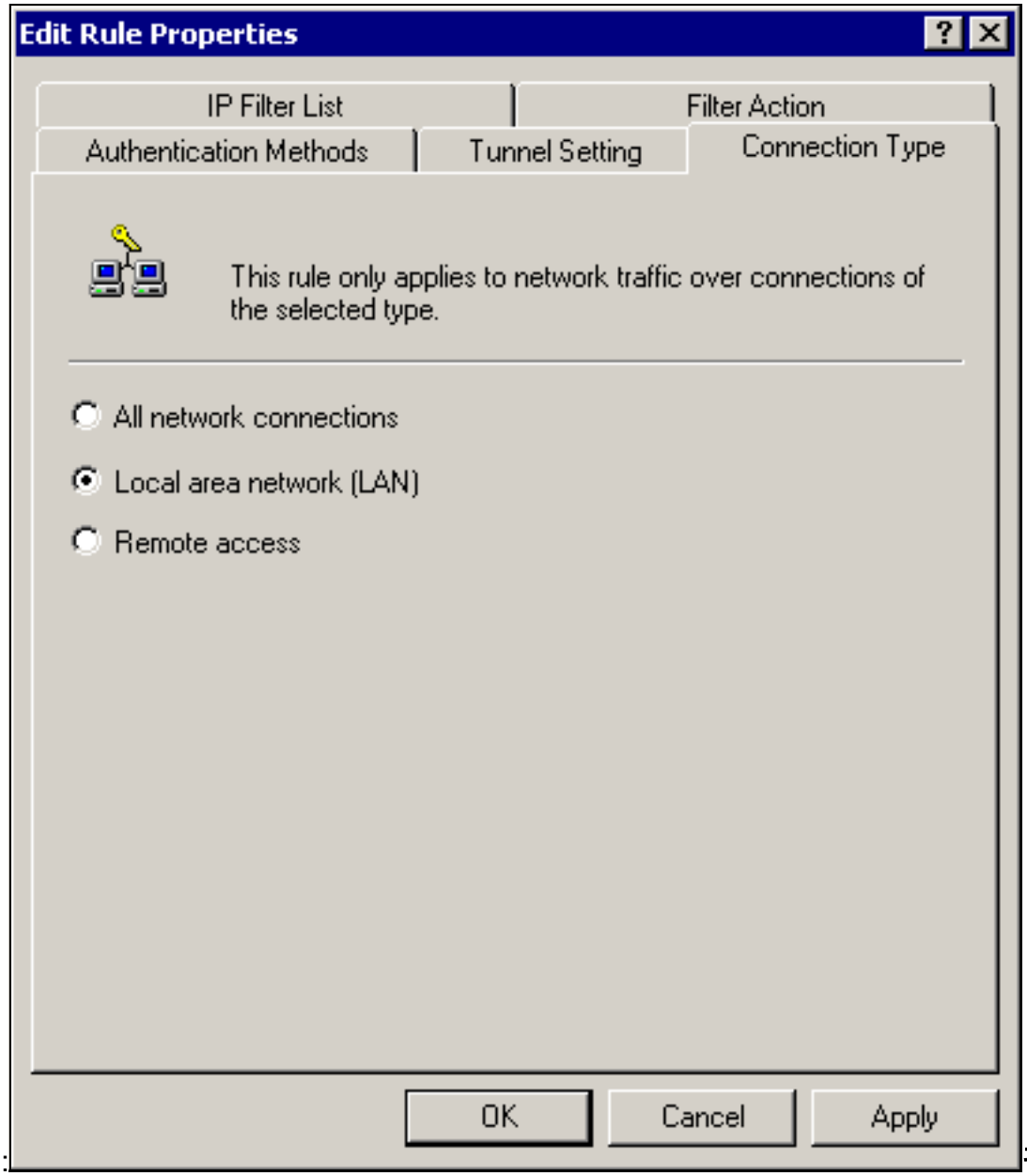


5. 규칙의 **General > Advanced > Methods** 탭에는 **IKE 암호화 방법**(DES), **IKE 해싱**(SHA1) 및 **Diffie-Helman 그룹**(Low(1))이 있습니다

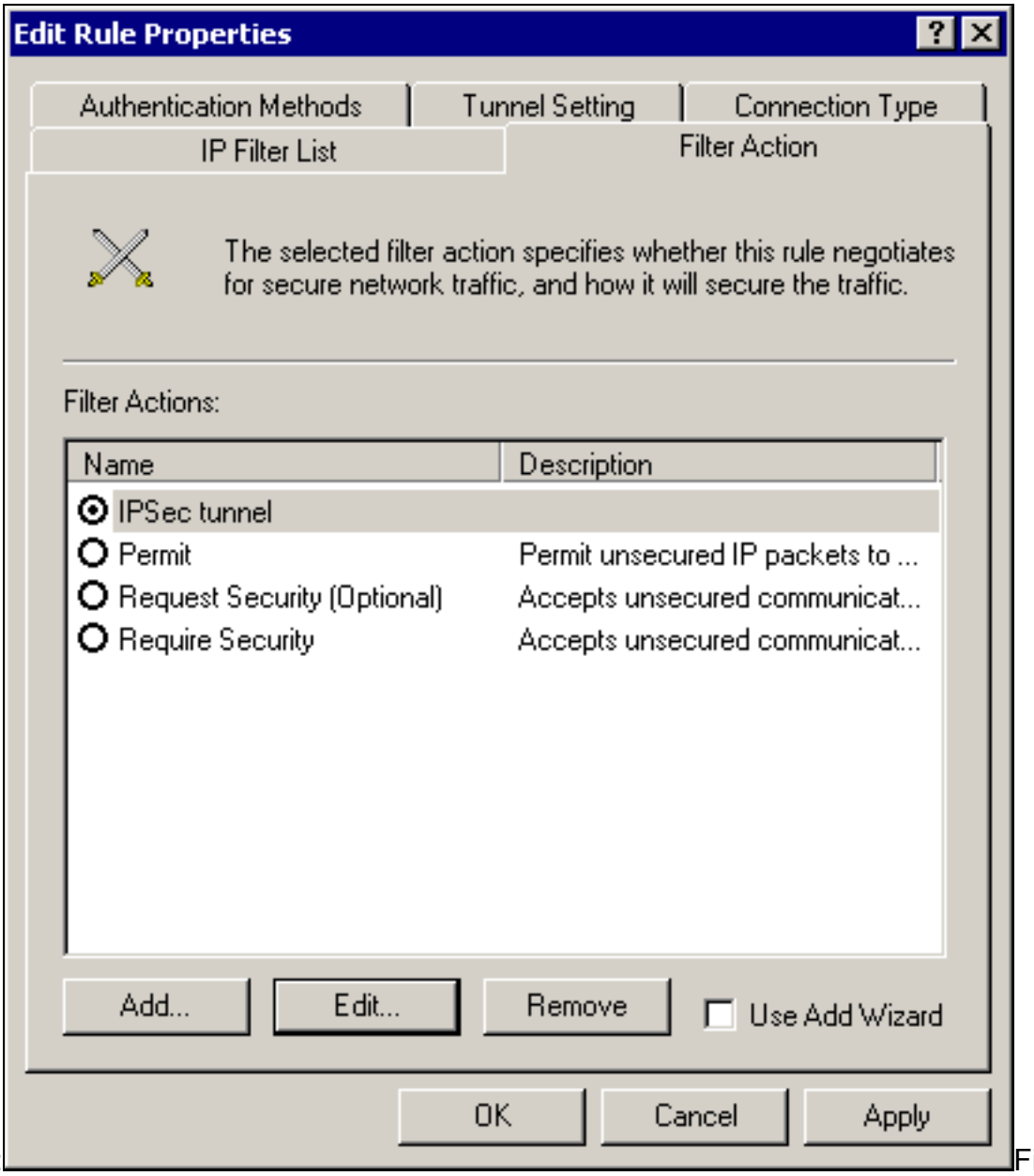


6. 각 필터에는 5개의 탭이 있습니다.**인증 방법**(IKE[Internet Key Exchange]용 사전 공유 키

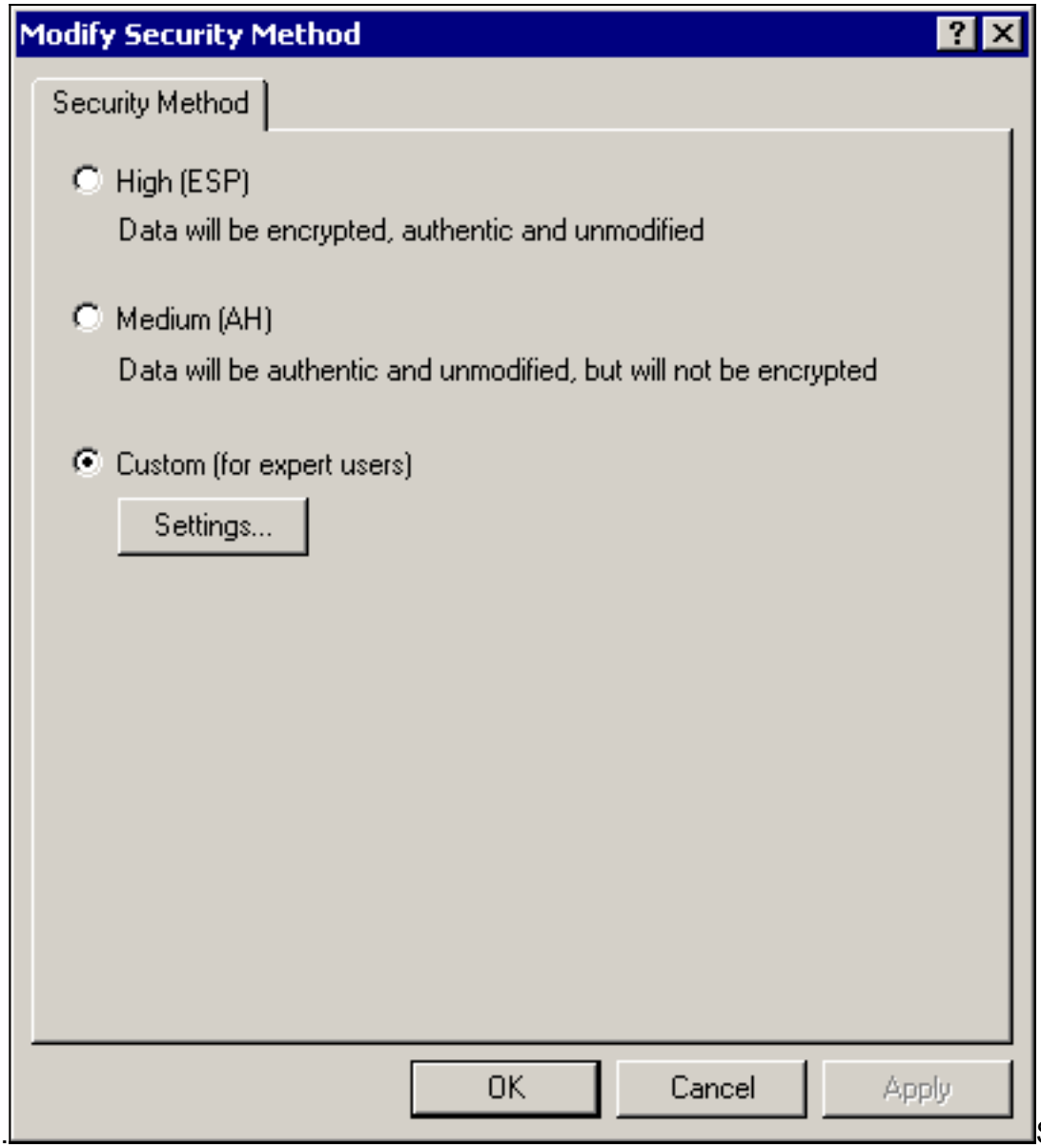

Edit Rule Properties
IP Filter List
Filter Action
Authentication Methods
Tunnel Setting
Connection Type
The authentication method specifies how trust is established between the computers. Offer and accept these authentication methods when negotiating security with another computer.
Authentication Method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


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

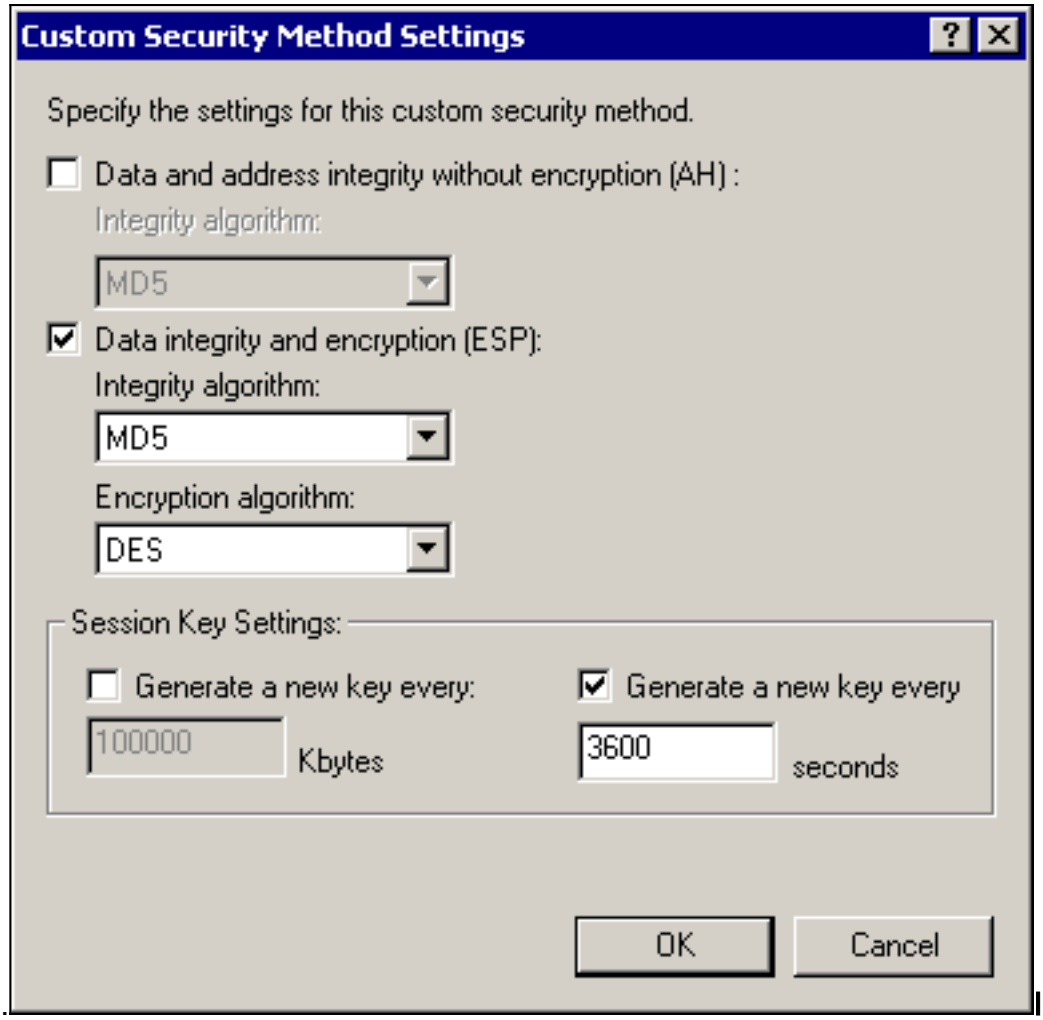
(LAN): **필터 동작**



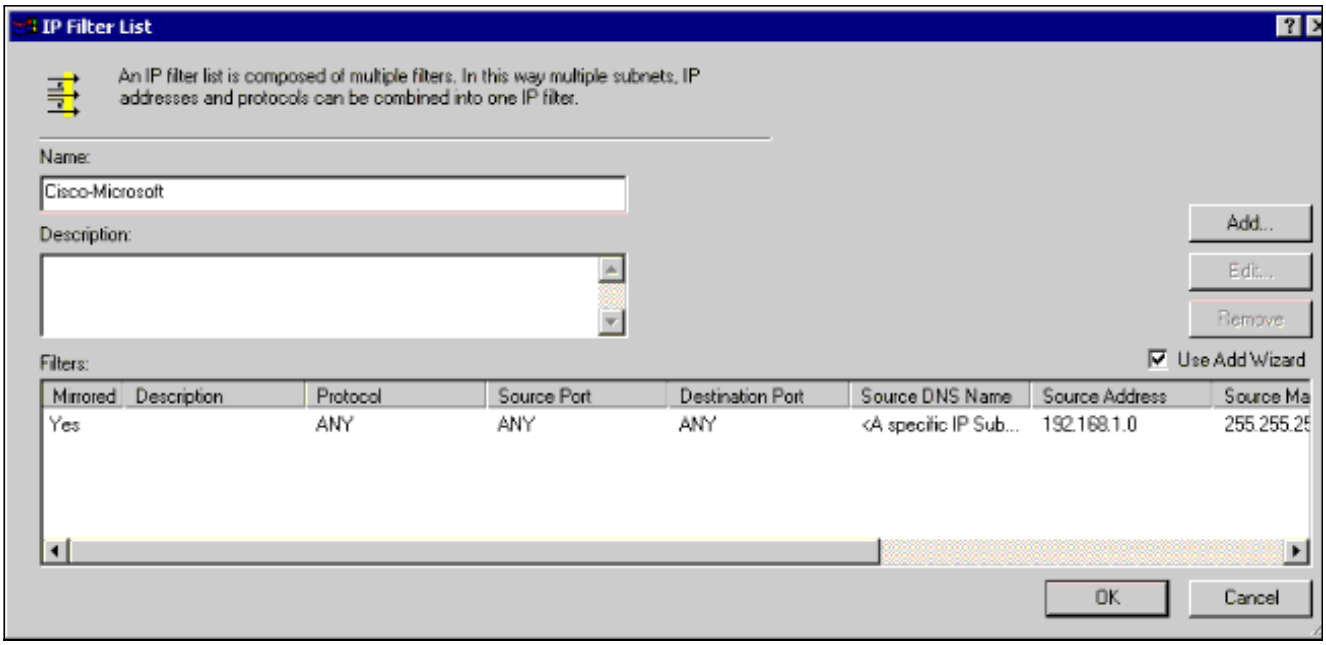
(IPSec): Filter **Action(필터 작업) > IPSec 터널 > Edit(편집) > Edit(편집)를** 선택하고 Custom(사용자 지정)을 **클릭합니다**



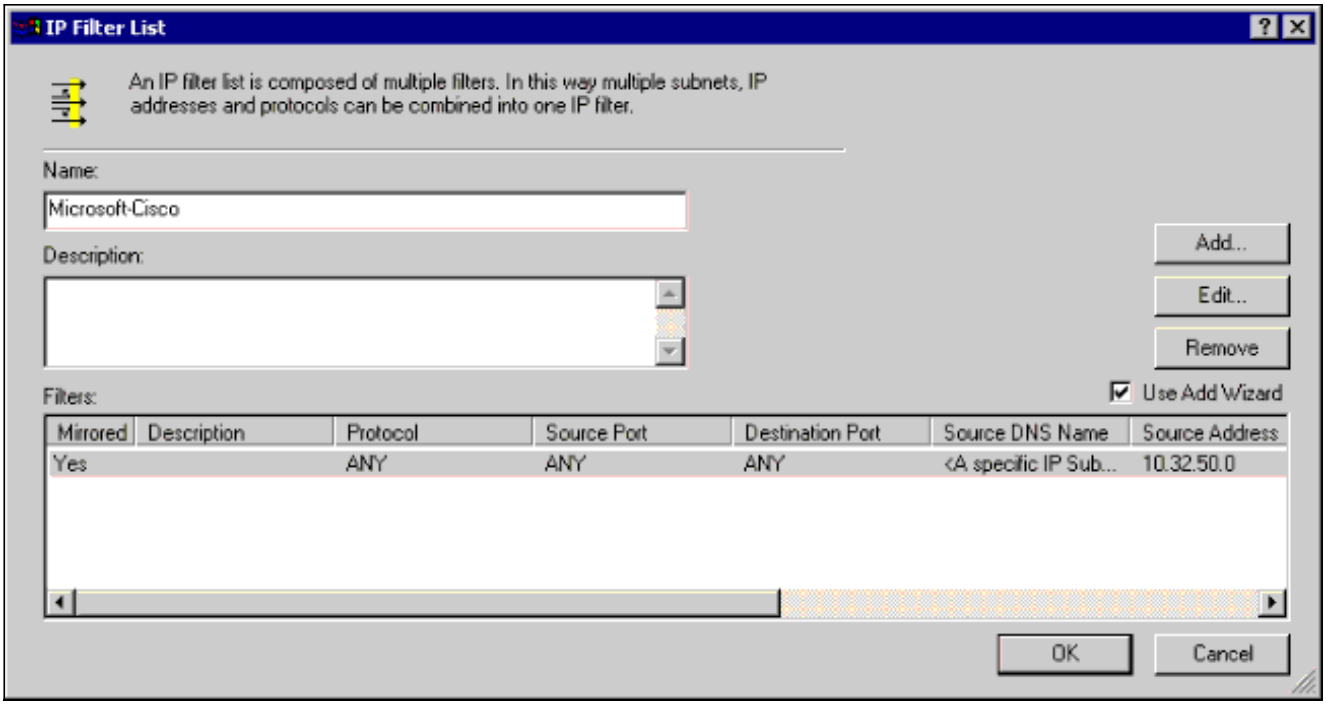
. Settings(**설정) - IPSec 변환** 및 IPSec **수명을 클릭합니다**



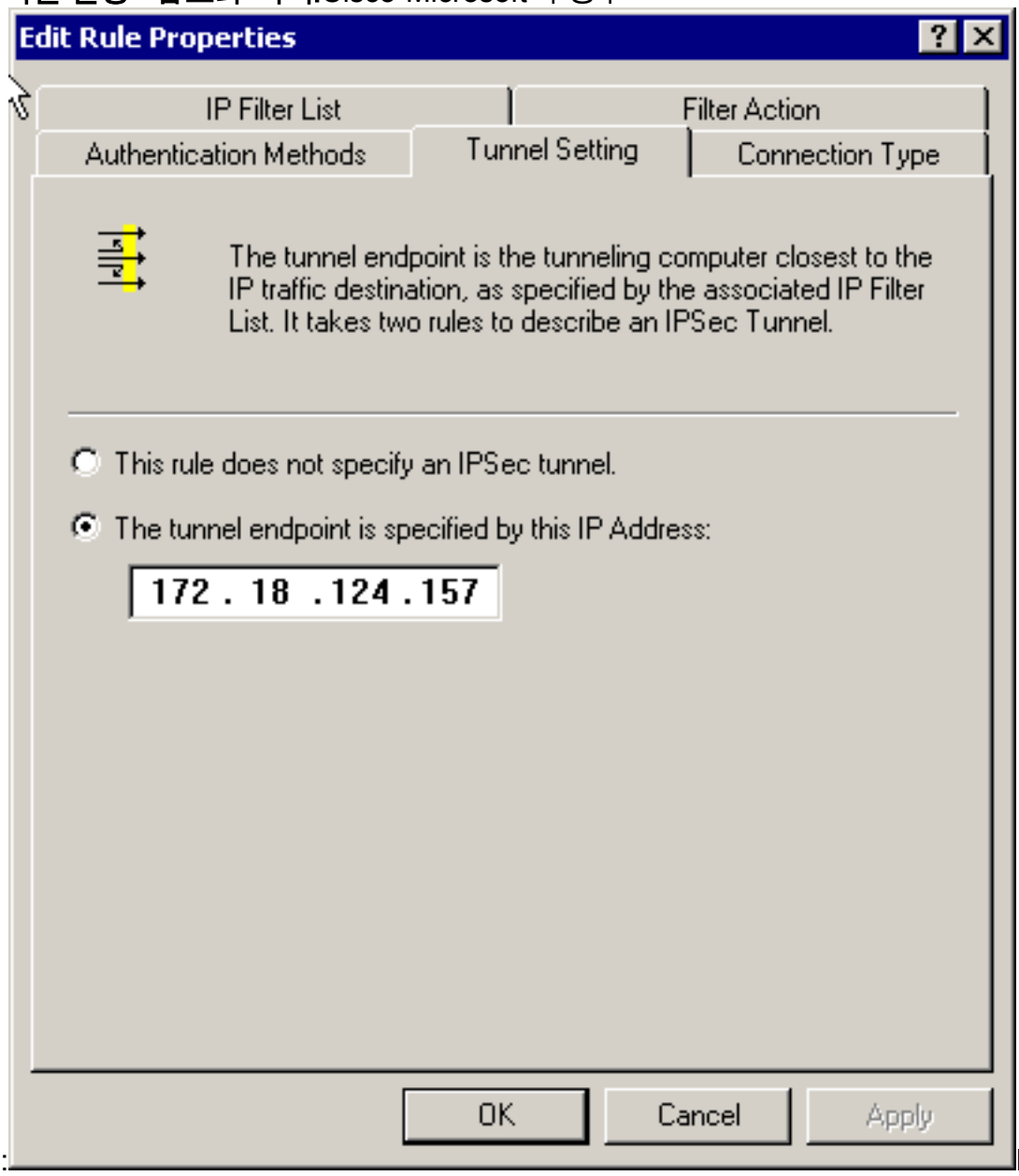
IP 필터 목록 - 암호화할 소스 및 **대상** 네트워크:Cisco-Microsoft의 경우
:



Microsoft-Cisco의 경우
:

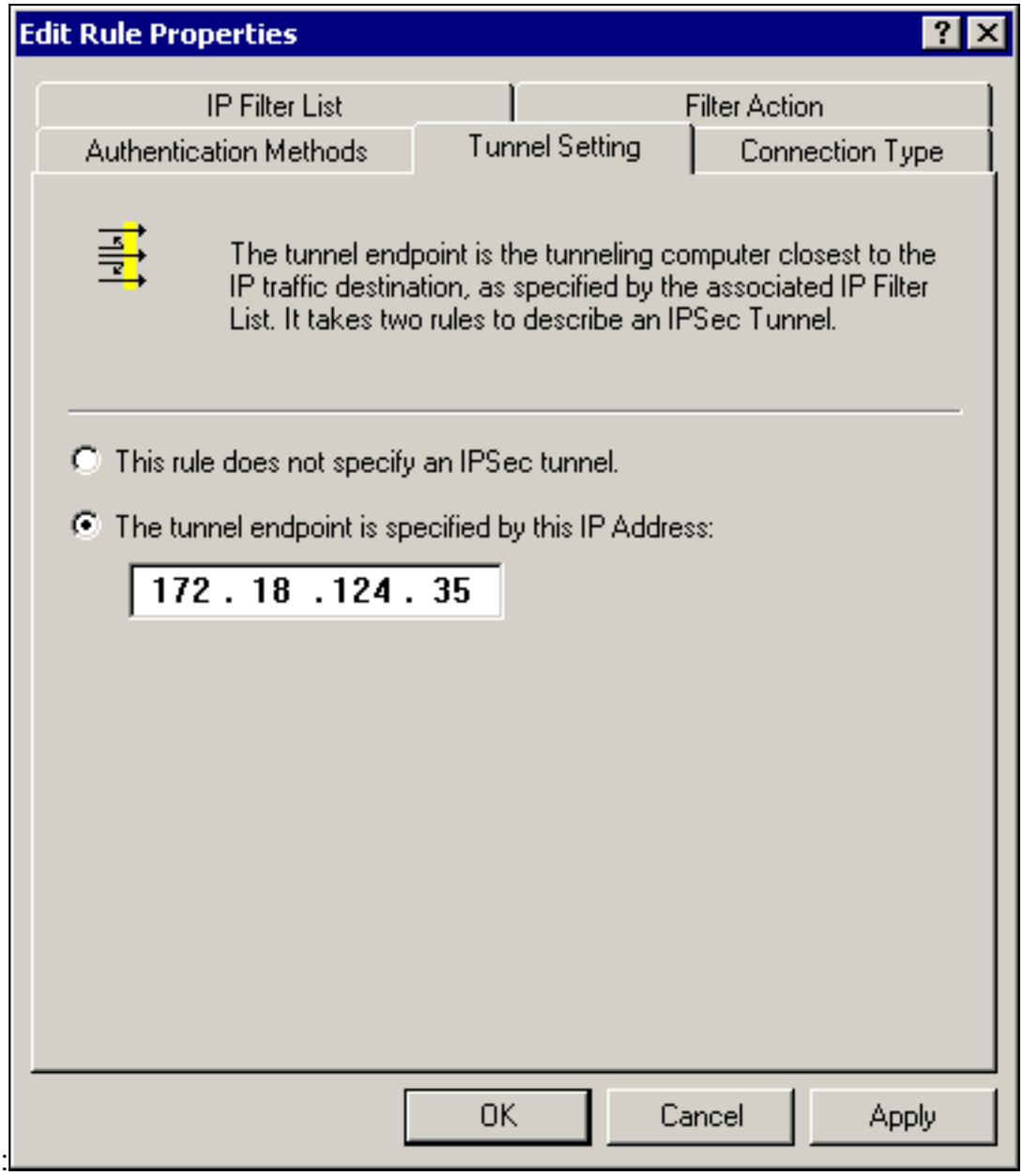


터널 설정 - 암호화 피어: Cisco-Microsoft의 경우



:Microsoft-

Cisco의 경우:



Cisco 디바이스 구성

아래 예와 같이 Cisco 라우터, PIX 및 VPN Concentrator를 구성합니다.

- Cisco 3640 Router
- PIX
- VPN 3000 Concentrator
- VPN 5000 Concentrator

Cisco 3640 라우터 구성

Cisco 3640 Router
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
```

PIX 구성

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 Concentrator 구성

필요에 따라 VPN Concentrator를 구성하려면 아래에 표시된 메뉴 옵션 및 매개변수를 사용합니다.

- IKE 제안을 추가하려면 Configuration(구성) **> System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec > IKE Proposals(IKE 제안) > Add a proposal(제안 추가)을** 선택합니다.

  ```
  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 터널을 정의하려면 Configuration(구성) **> System(시스템) > Tunneling Protocols(터널링 프로토콜) > IPSec LAN-to-LAN을 선택합니다.**

  ```
  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
  ```

- 보안 연결을 수정하려면 Configuration(구성) > **Policy Management(정책 관리) > Traffic Management(트래픽 관리) > Security Associations(보안 연결) > Modify(수정)**를 선택합니다.

```
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 Concentrator 구성

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.
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

Cisco 3640 Router

- **debug crypto engine** - 암호화 및 해독을 수행하는 암호화 엔진에 대한 디버그 메시지를 표시합니다.
- **debug crypto isakmp** - IKE 이벤트에 대한 메시지를 표시합니다.
- **debug crypto ipsec** - IPSec 이벤트를 표시합니다.
- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Association)를 모두 표시합니다.
- **show crypto ipsec sa** - 현재 보안 연결에서 사용하는 설정을 표시합니다.
- **clear crypto isakmp** - (컨피그레이션 모드에서) 모든 활성 IKE 연결을 지웁니다.
- **clear crypto sa** - (컨피그레이션 모드에서) 모든 IPSec 보안 연결을 삭제합니다.

PIX

- **debug crypto ipsec** - 2단계의 IPSec 협상을 표시합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.
- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **show crypto ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.
- **clear crypto isakmp** - (컨피그레이션 모드에서) IKE(Internet Key Exchange) 보안 연결을 지웁니다.
- **clear crypto ipsec sa** - (컨피그레이션 모드에서) IPSec 보안 연결을 지웁니다.

VPN 3000 Concentrator

- - Configuration(컨피그레이션) > System(**시스템) > Events(이벤트) > Classes(클래스) > Modify(Severity to Log**=1-13, Severity to Console=1-3)을 선택하여 VPN 300 Concentrator 디버그를 시작합니다. IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - 이벤트 로그는 Monitoring(모니터링) **> Event Log(이벤트 로그)**를 선택하여 지우거나 검색할 수 있습니다.
- - LAN-to-LAN 터널 트래픽은 **Monitoring > Sessions**에서 모니터링할 수 있습니다.
- - 터널은 Administration(관리) **> Administer Sessions(관리 세션) > LAN-to-LAN sessions(LAN-to-LAN 세션) > Actions(작업) - Logout(로그아웃)에서 지울 수 있습니다.**

VPN 5000 Concentrator

- **vpn trace dump all** - 시간, VPN 번호, 피어의 실제 IP 주소, 스크립트가 실행된 상태, 오류가 발생한 소프트웨어 코드의 루틴 및 라인 번호를 포함하여 모든 일치하는 VPN 연결에 대한 정보를 표시합니다.
- **show vpn statistics** - Users, Partners(사용자, 파트너) 및 Total(합계)에 대한 다음 정보를 표시합니다. (모듈형 모델의 경우 각 모듈 슬롯에 대한 섹션이 표시됩니다.) 현재 활성 - 현재 활성 연결입니다. Negot - 현재 협상 연결. High Water - 마지막 재부팅 이후 최대 동시 활성 연결 수

입니다. Running Total - 마지막 재부팅 이후 성공한 총 연결 수입니다. Tunnel Starts(터널 시작) - 터널 시작 수입니다. Tunnel OK(터널 확인) - 오류가 없는 터널 수입니다. 터널 오류 - 오류가 있는 터널 수입니다.

- **show vpn statistics verbose** - ISAKMP 협상 통계 및 더 많은 활성 연결 통계를 표시합니다.

관련 정보

- Cisco VPN 5000 Series Concentrator 판매 중단 발표
- IPSec 네트워크 보안 구성
- 인터넷 키 교환 보안 프로토콜 구성
- Technical Support - Cisco Systems