Konfigurieren von IPSec zwischen einem Microsoft Windows 2000-Server und einem Cisco Gerät

Inhalt

Einführung

In diesem Dokument wird veranschaulicht, wie ein IPSec-Tunnel mit vorinstallierten Schlüsseln erstellt wird, um zwei privaten Netzwerken beizutreten: ein privates Netzwerk (192.168.I.X) innerhalb eines Cisco Geräts und ein privates Netzwerk (10.32.50.X) innerhalb des Microsoft 2000-Servers. Wir gehen davon aus, dass der Datenverkehr vom Cisco Gerät und innerhalb des 2000-Servers zum Internet (hier durch die Netzwerke 172.18.124.X dargestellt) vor Beginn dieser Konfiguration fließt.

Ausführliche Informationen zur Konfiguration des Microsoft Windows 2000-Servers finden Sie auf der Microsoft-Website: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

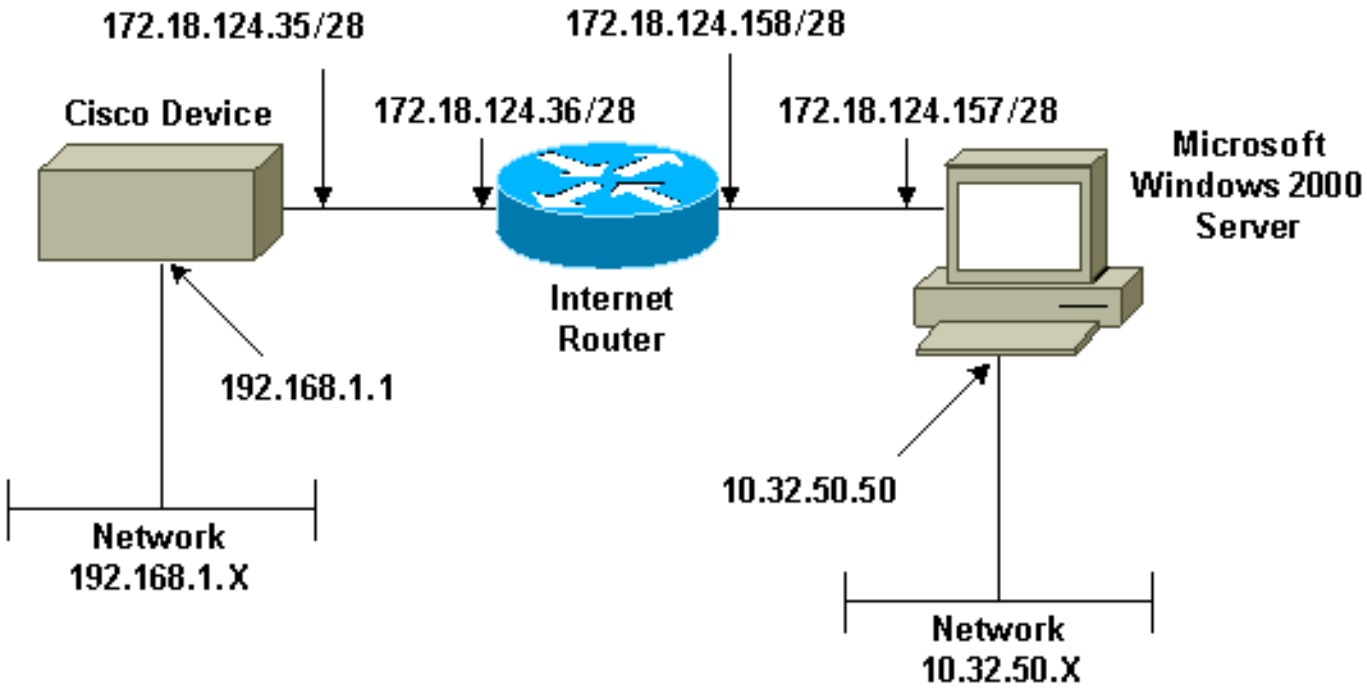
Diese Konfigurationen wurden mit den unten stehenden Software- und Hardwareversionen entwickelt und getestet.

- Microsoft Windows 2000 Server 5.00.2195
- Cisco 3640 Router mit Cisco IOS® Software-Version c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX Firewall mit PIX Software Version 5.2.1
- Cisco VPN 3000 Concentrator mit VPN 3000 Concentrator Software Version 2.5.2.F
- Cisco VPN 5000 Concentrator mit VPN 500 Concentrator Software Version 5.2.19

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Netzwerkdiagramm

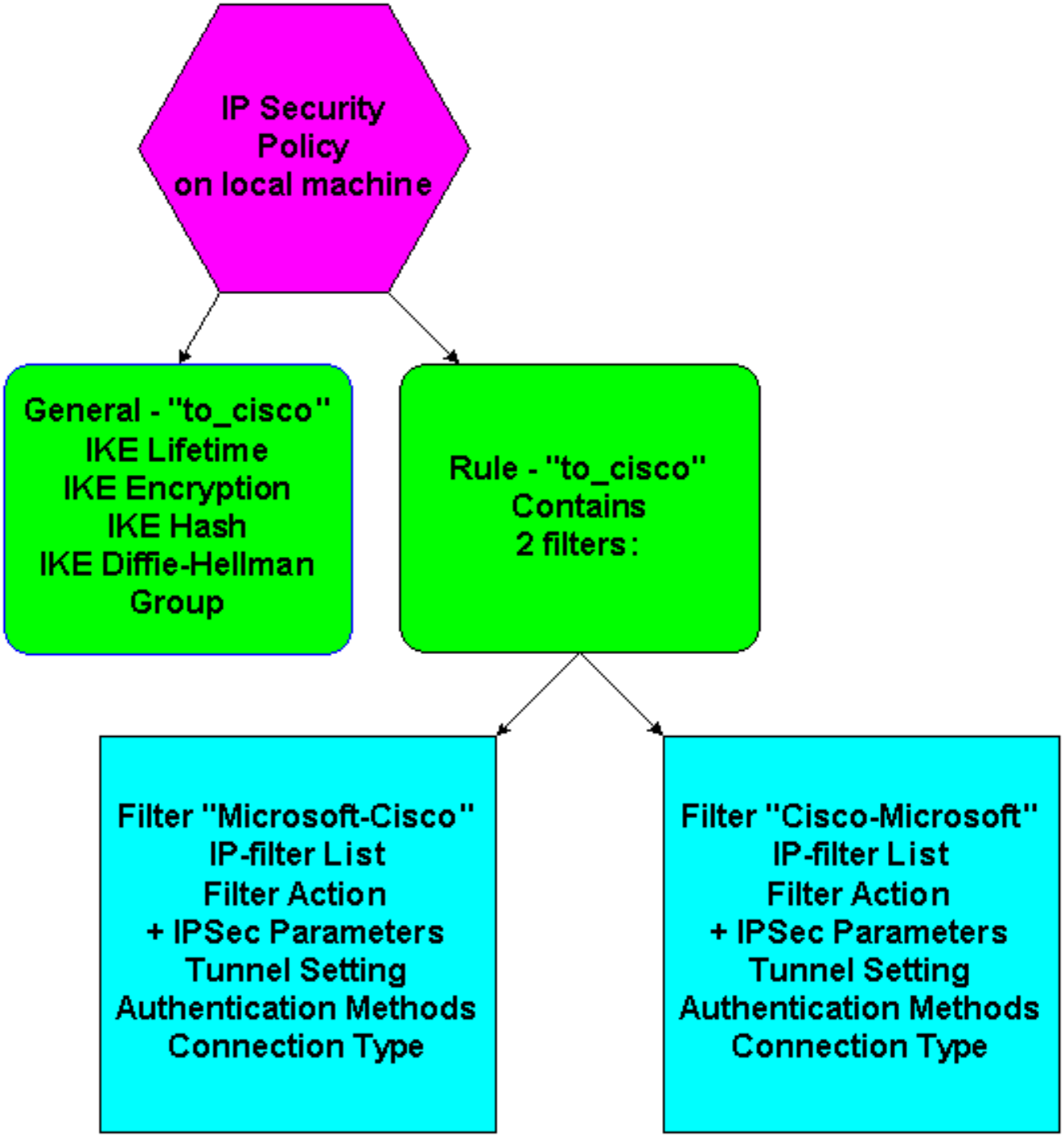
In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Konfigurieren des Microsoft Windows 2000-Servers für die Arbeit mit Cisco Geräten

Durchgeführte Aufgaben

Dieses Diagramm zeigt die in der Microsoft Windows 2000-Serverkonfiguration ausgeführten Aufgaben:

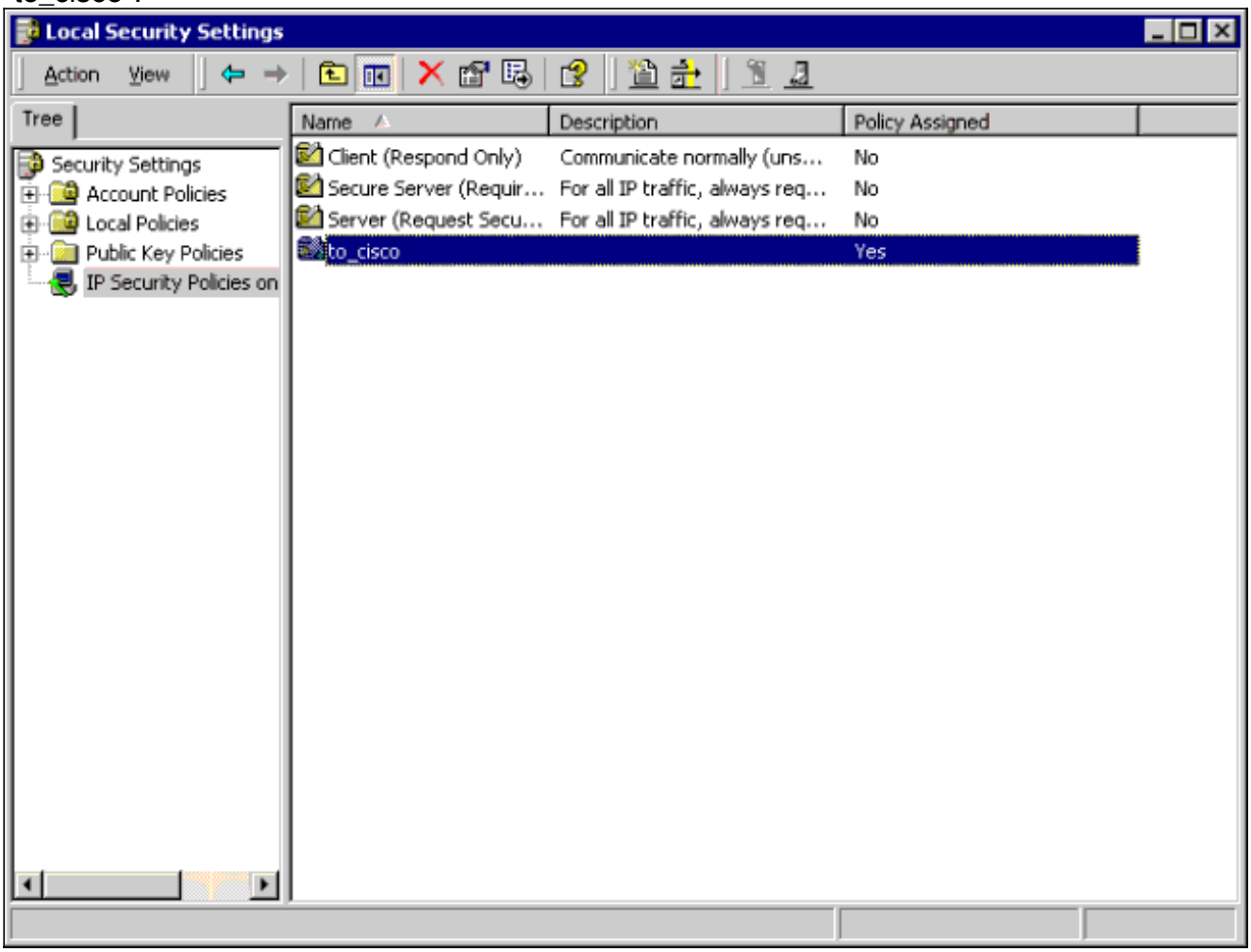


Schrittweise Anleitung

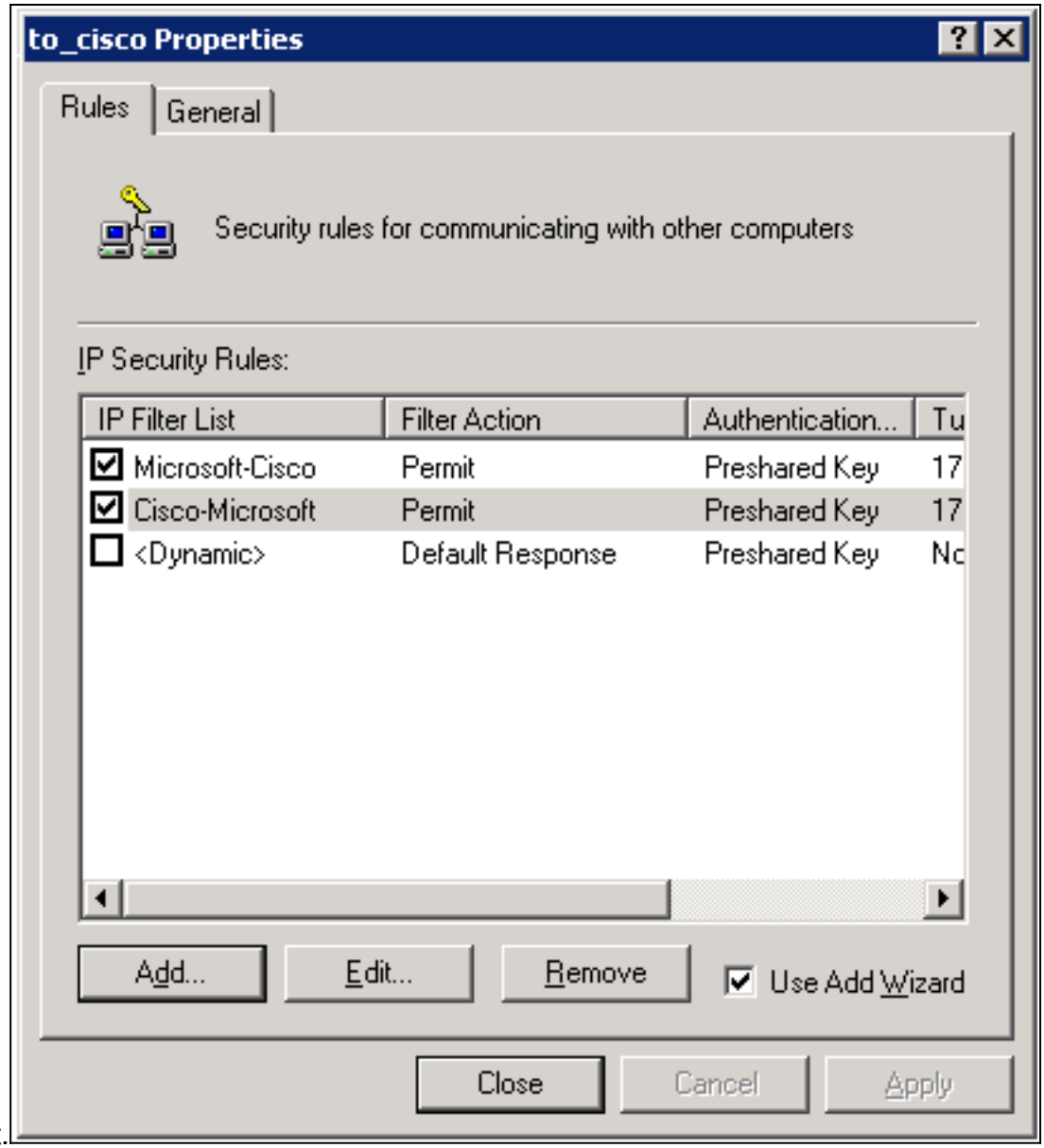
Wenn Sie die Konfigurationsanweisungen auf der Microsoft-Website befolgt haben, überprüfen Sie anhand der folgenden Schritte, ob Ihre Konfiguration mit Cisco Geräten kompatibel ist. Kommentare und Änderungen werden mit den Screenshots vermerkt.

1. Klicken Sie auf dem Microsoft Windows 2000-Server auf **Start > Ausführen > secpol.msc**, und überprüfen Sie die Informationen auf den folgenden Bildschirmen.Nachdem die Anweisungen auf der Microsoft-Website zur Konfiguration eines 2000-Servers verwendet wurden, wurden die folgenden Tunnelinformationen angezeigt.**Hinweis:** Die Beispielregel heißt

"to_cisco".

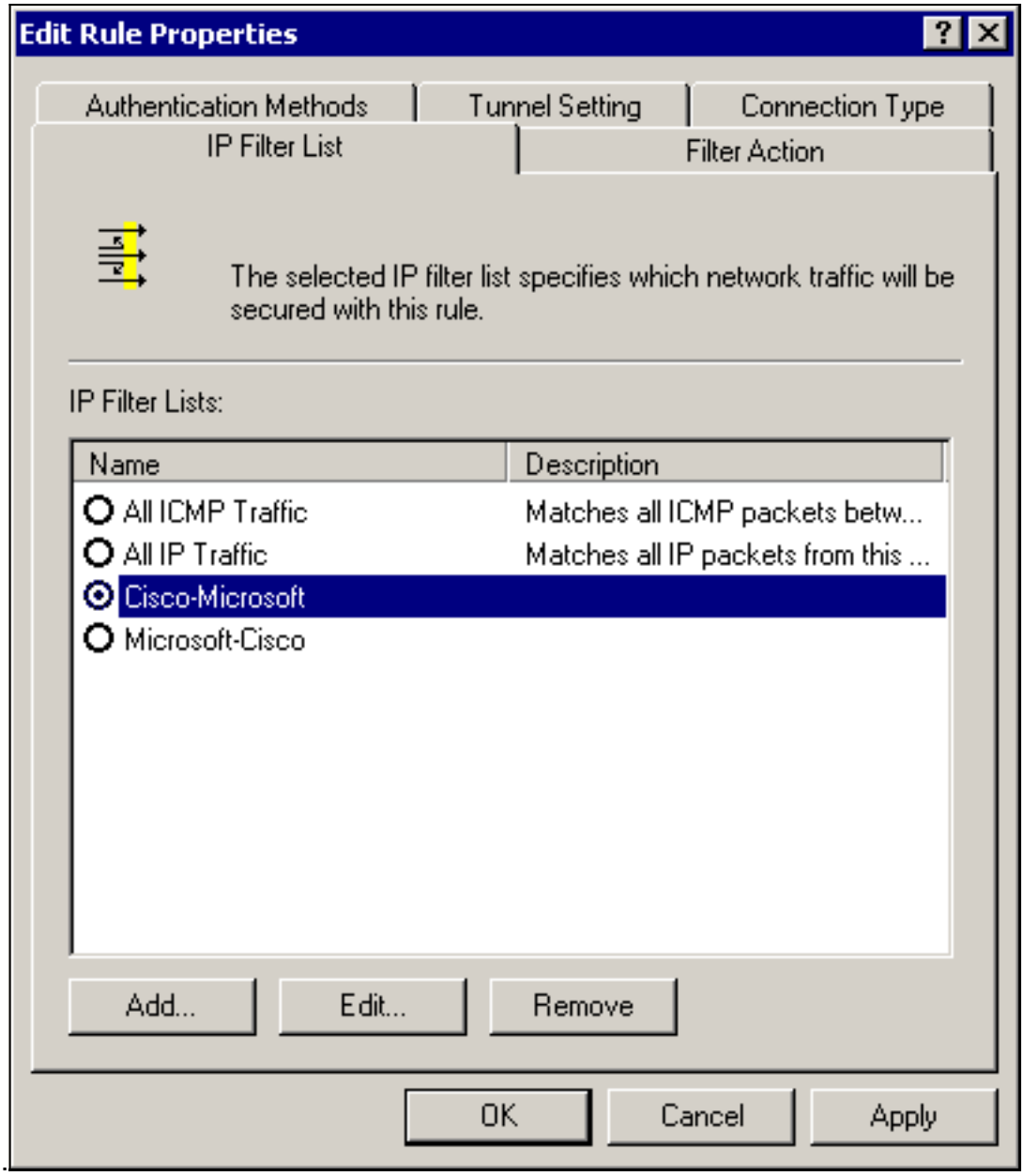


2. Diese Beispielregel enthält zwei Filter: Microsoft-Cisco und Cisco-



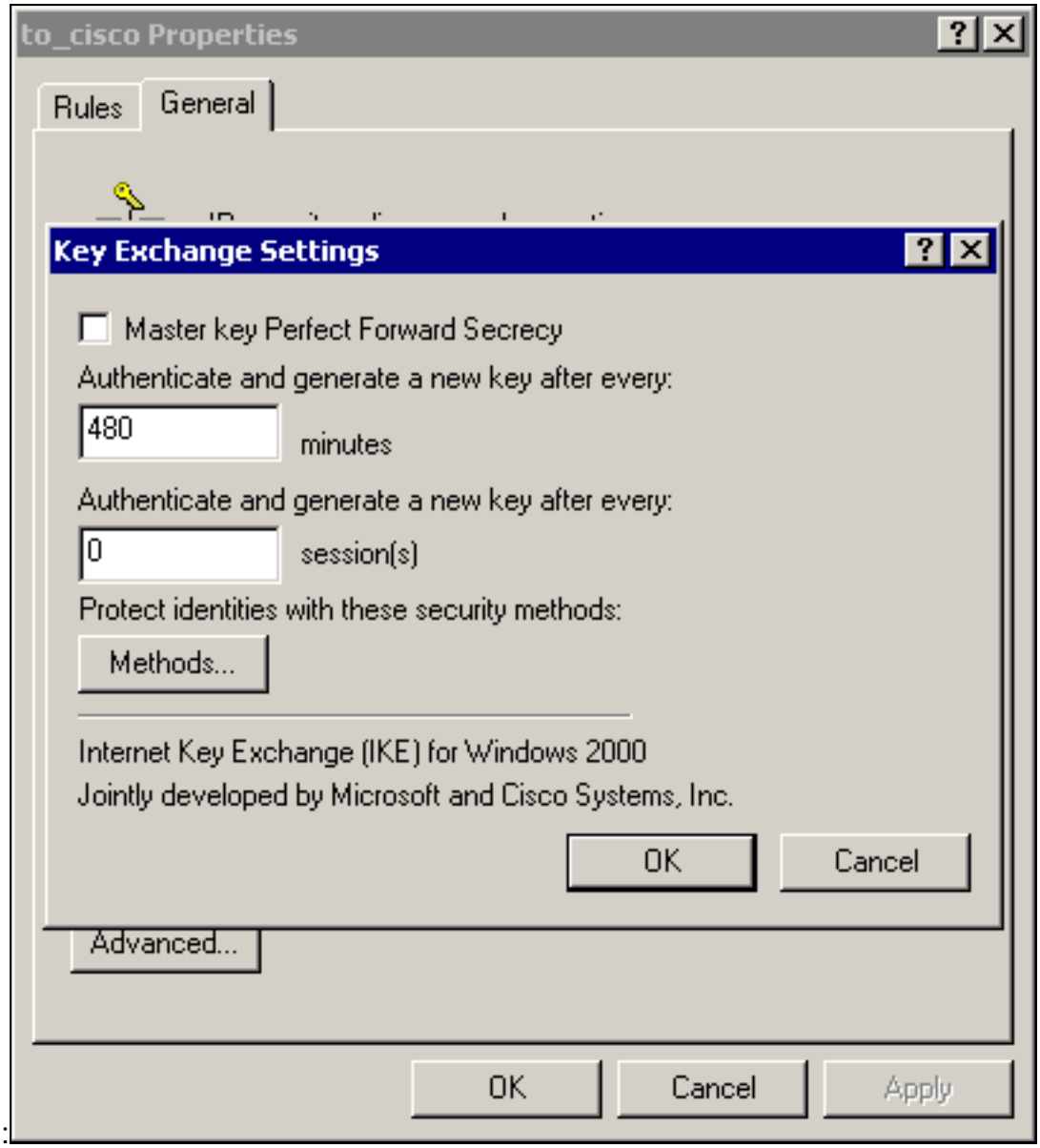
Microsoft.

3. Wählen Sie die Cisco-Microsoft IP-Sicherheitsregel aus, und klicken Sie dann auf **Bearbeiten**, um die IP-Filterlisten anzuzeigen/hinzuzufügen/zu



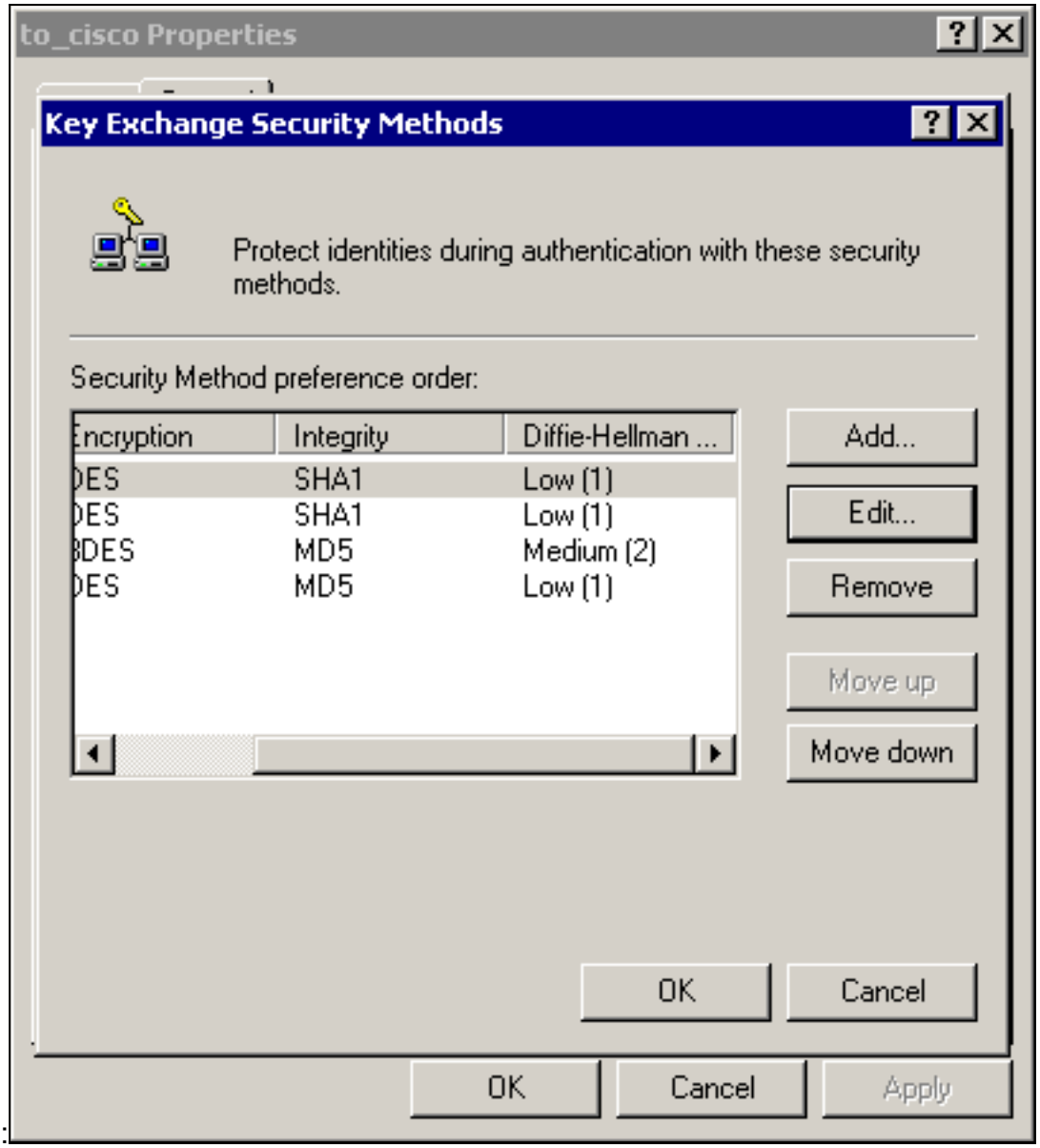
bearbeiten.

4. Die Registerkarte **Allgemein > Erweitert** der Regel hat die **IKE-Lebensdauer** (480 Minuten = 28.800



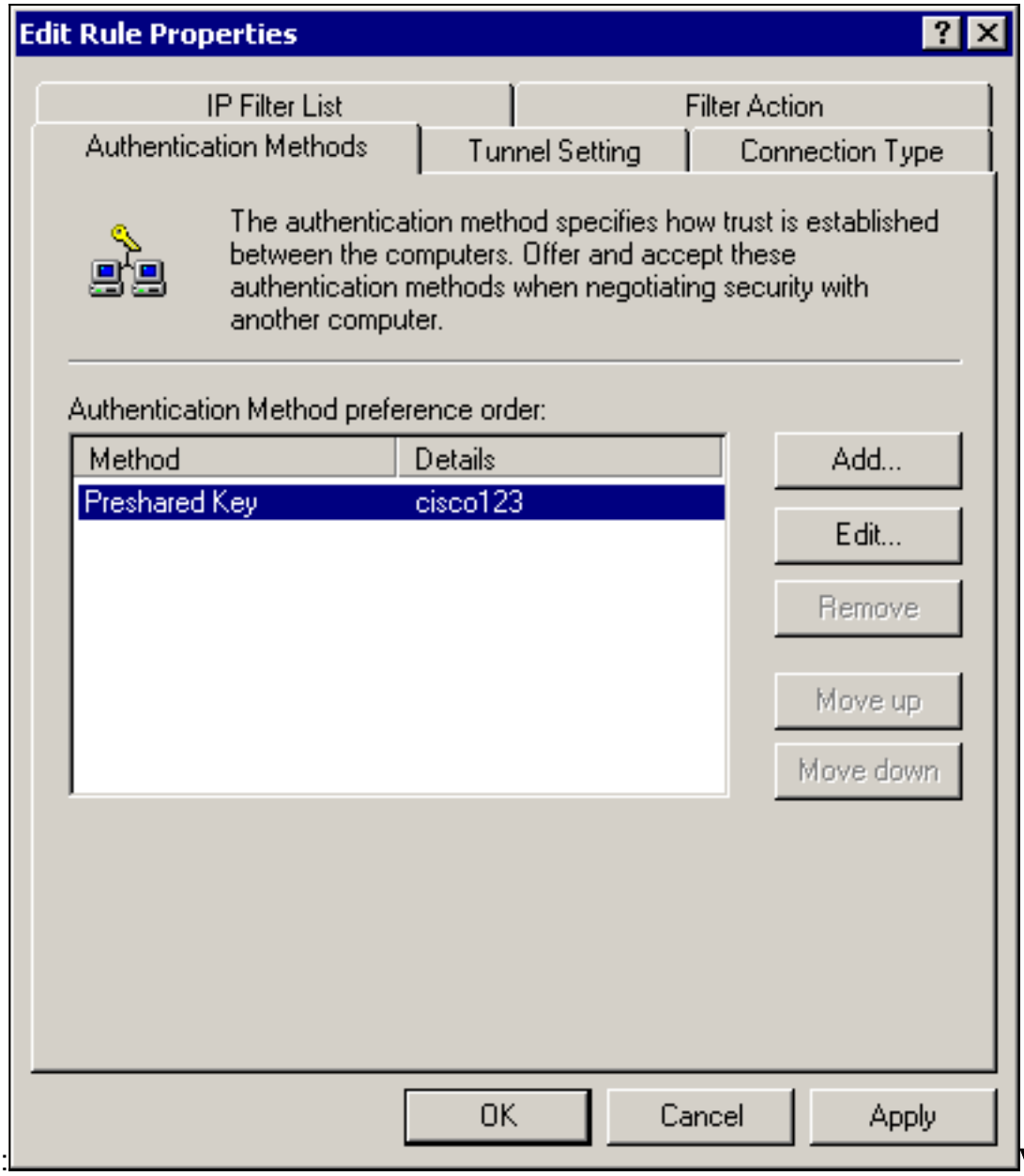
Sekunden):

5. Die Registerkarte **Allgemein > Erweitert > Methoden** enthält die **IKE-Verschlüsselungsmethode** (DES), **IKE-Hashing** (SHA1) und die **Diffie-Helman-Gruppe**

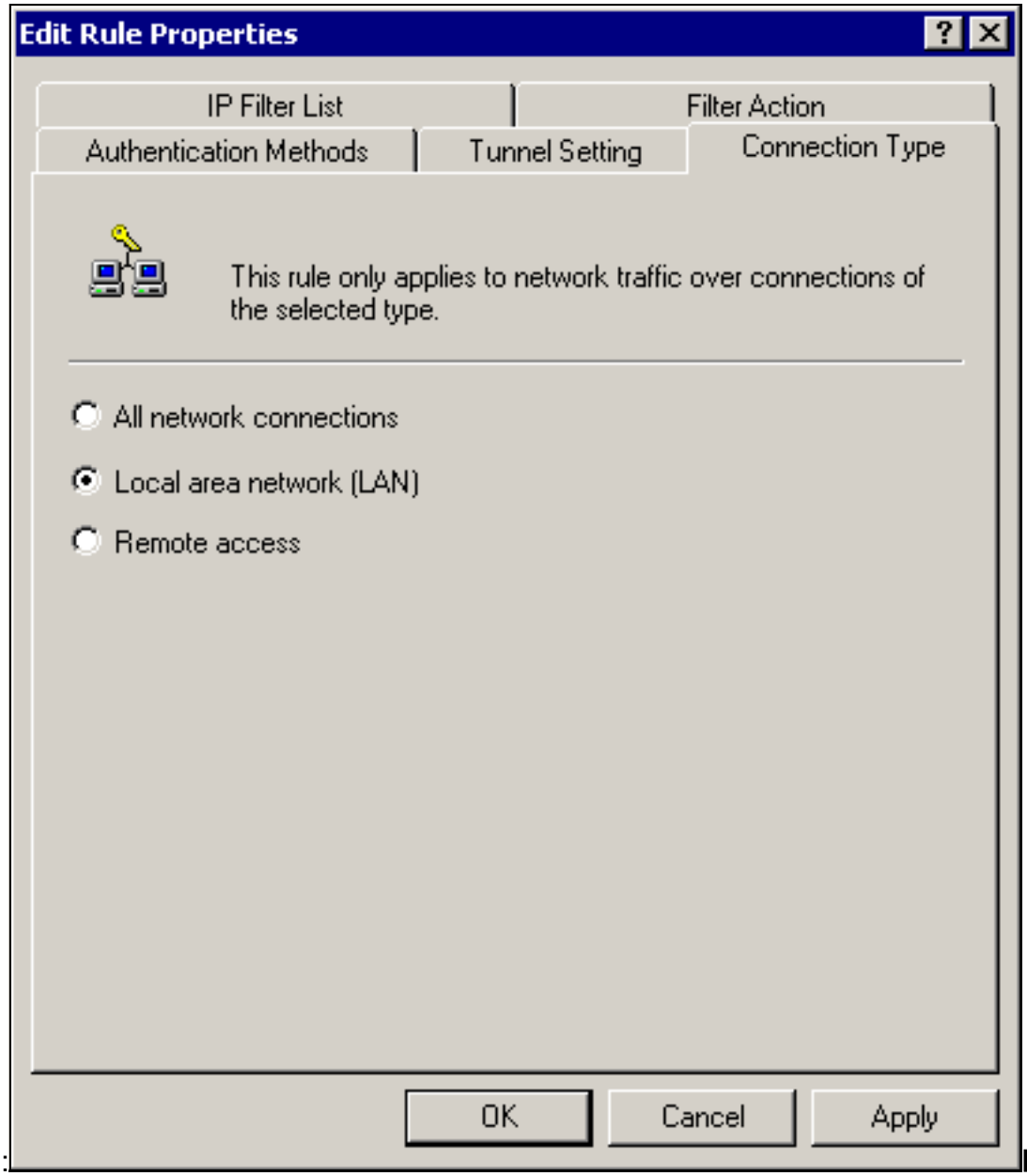


(Niedrig(1)):

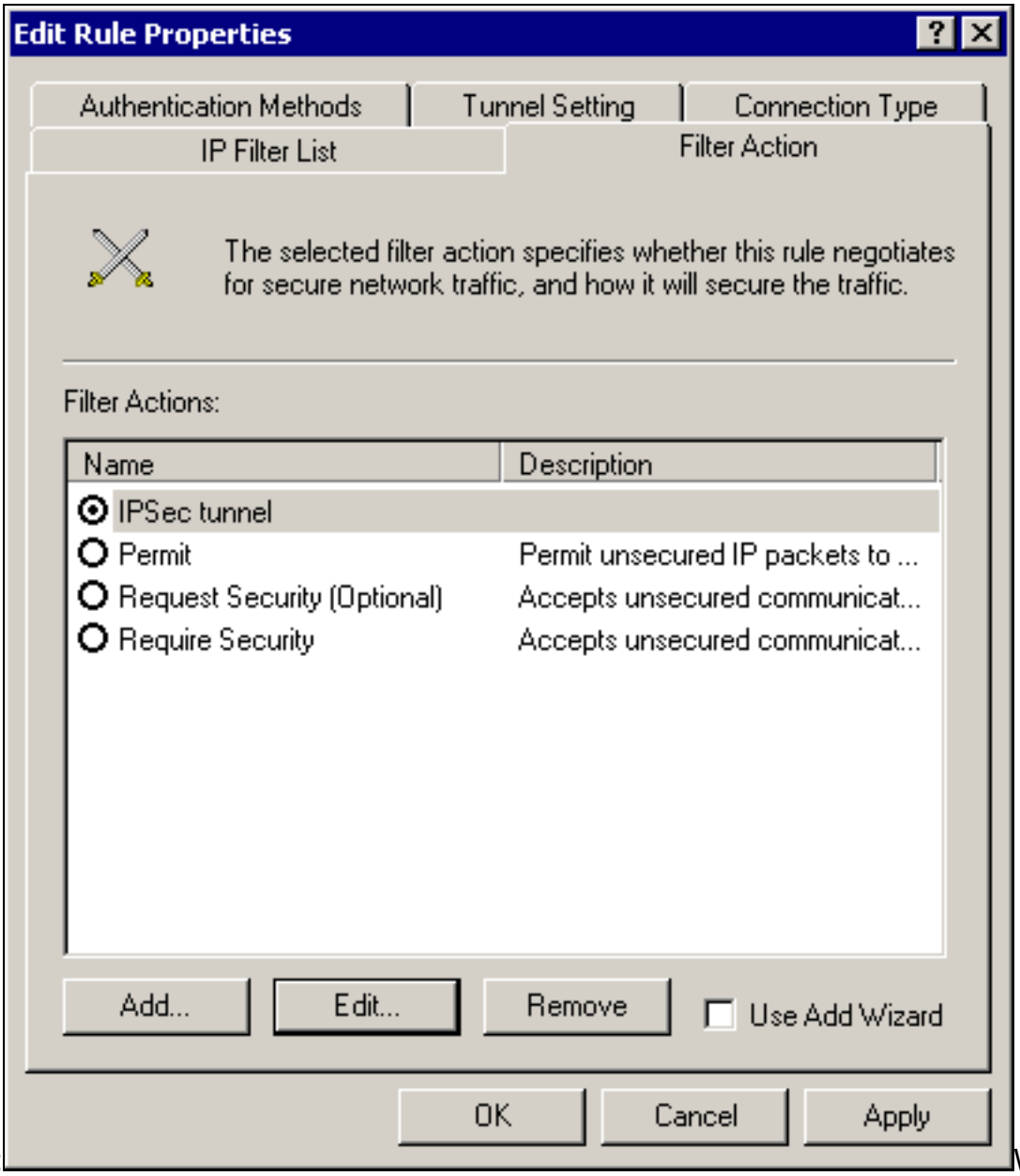
6. Jeder Filter hat fünf Registerkarten:**Authentifizierungsmethoden** (vorinstallierte Schlüssel für Internet Key Exchange



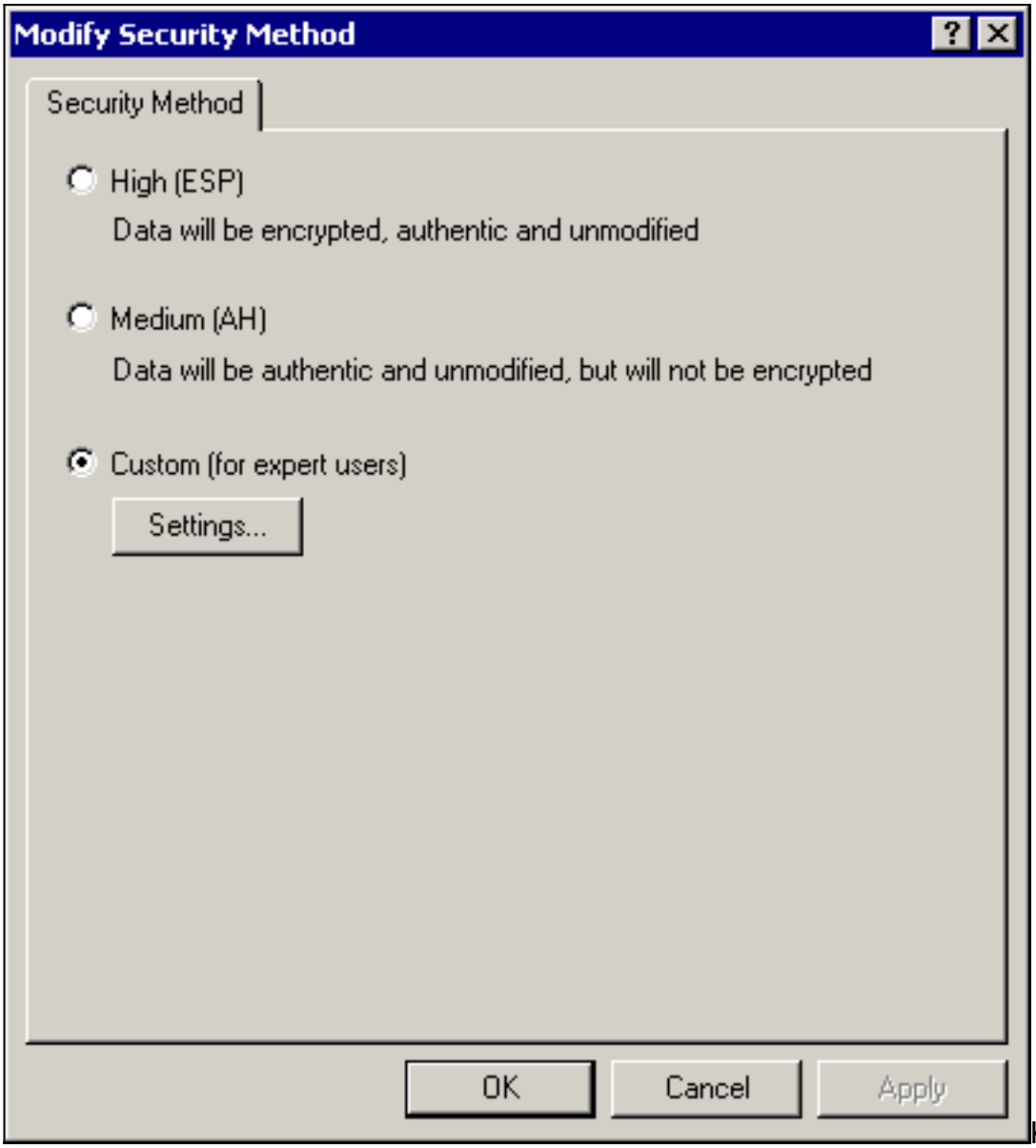
[IKE]): **Verbindungstyp**



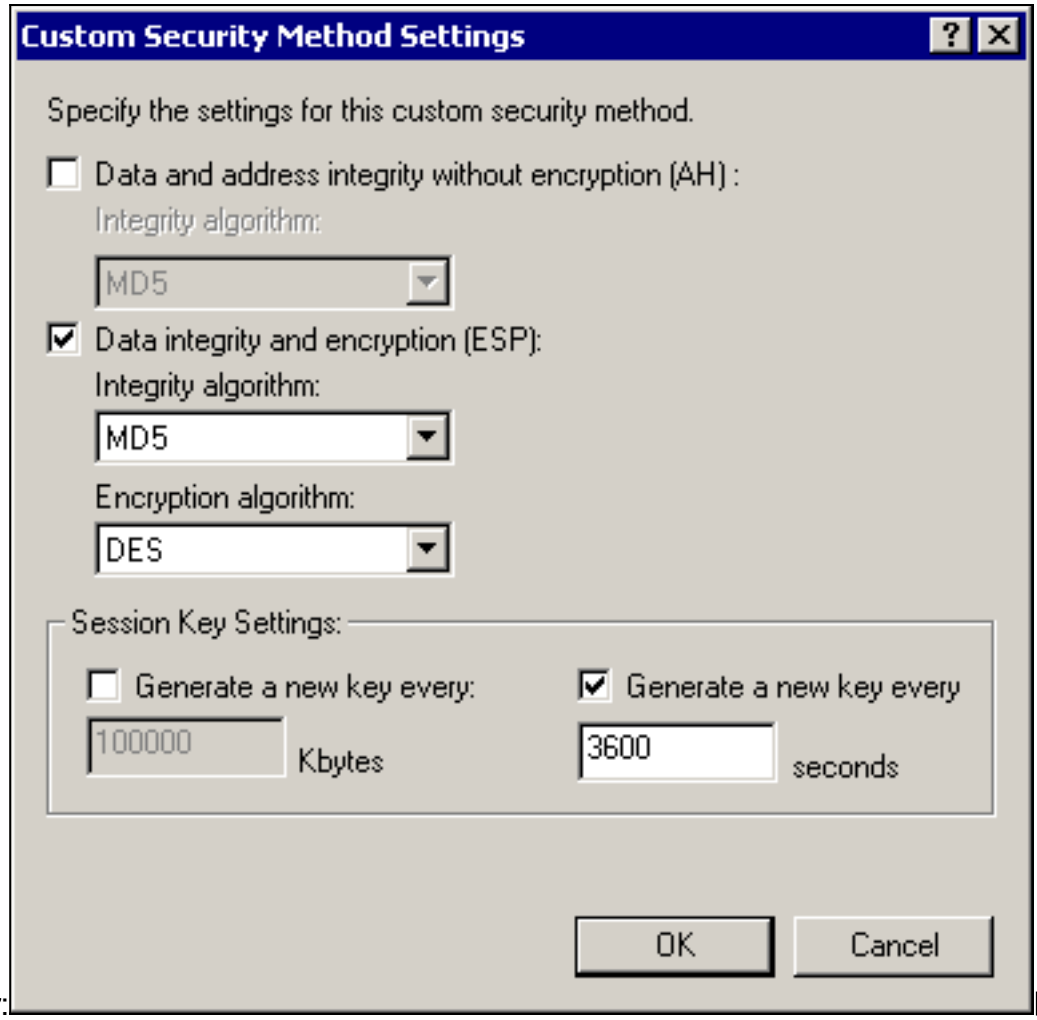
(LAN): **Filteraktion**



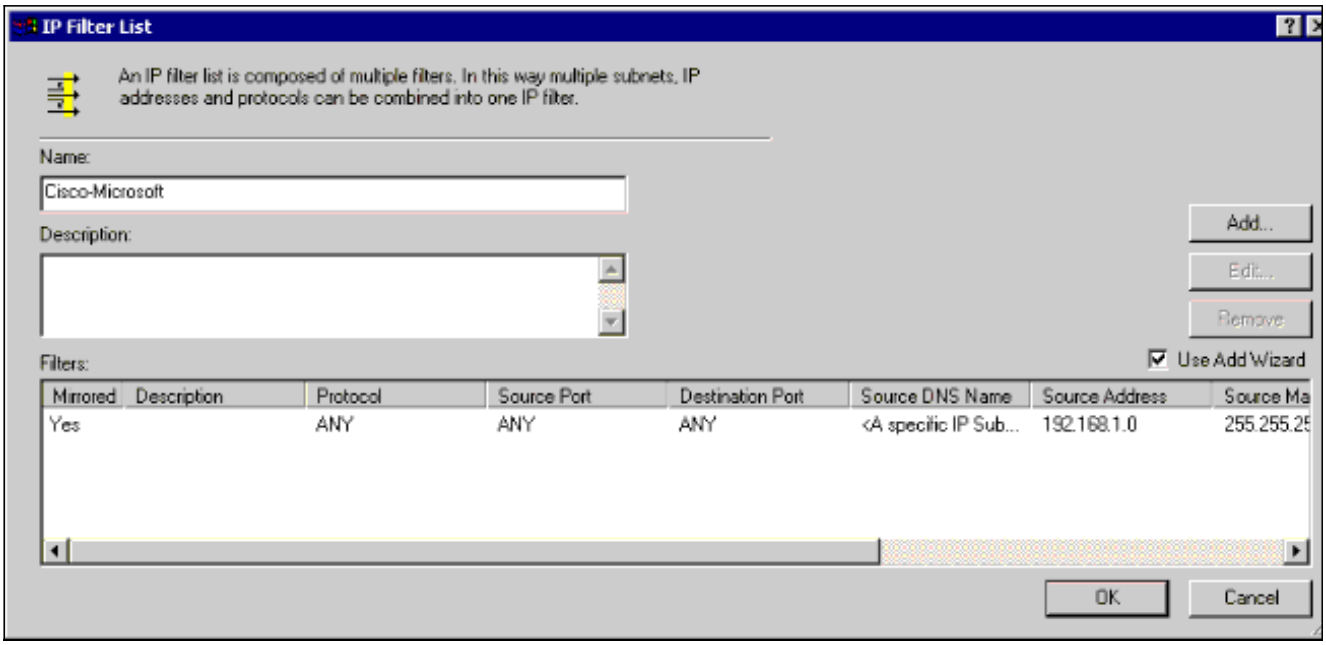
(IPSec): Wählen Sie **Filteraktion > IPSec-Tunnel > Bearbeiten > Bearbeiten**, und klicken Sie auf **Benutzerdefiniert**:



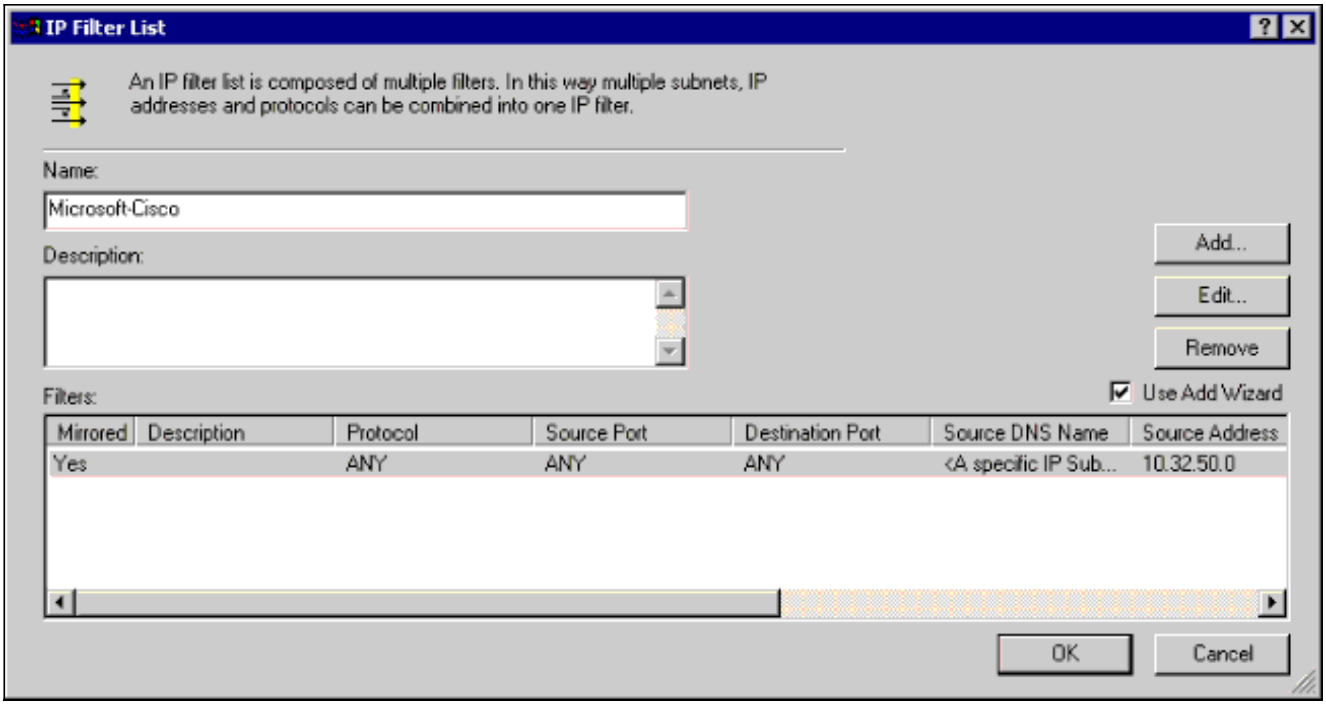
Klicken Sie auf **Einstellungen - IPSec transformiert** und **IPSec-**



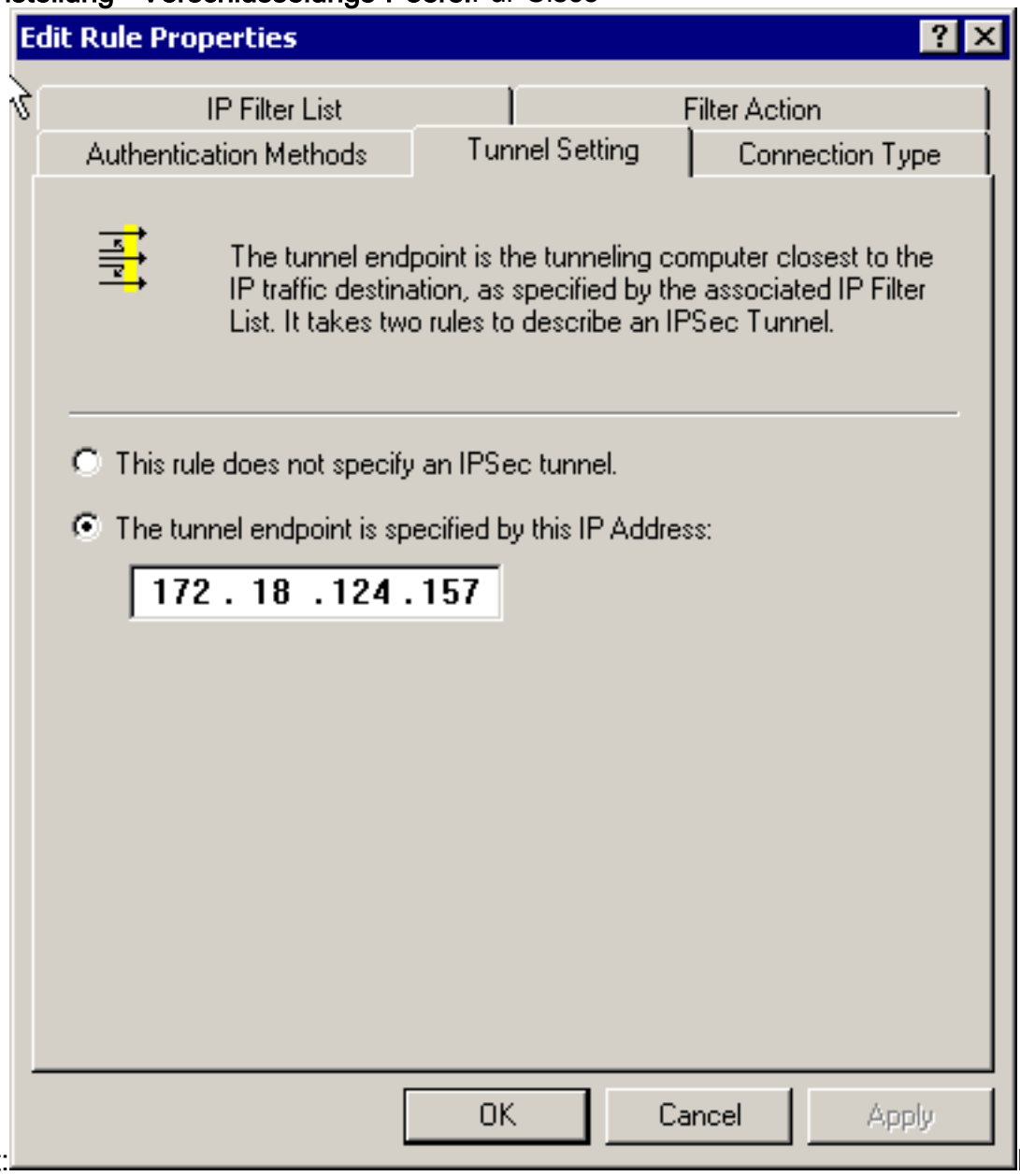
Lebensdauer:**IP-Filterliste - Zu** verschlüsselnde **Quell**- und **Zielnetzwerke**:Für Cisco-Microsoft:



Für Microsoft-Cisco:

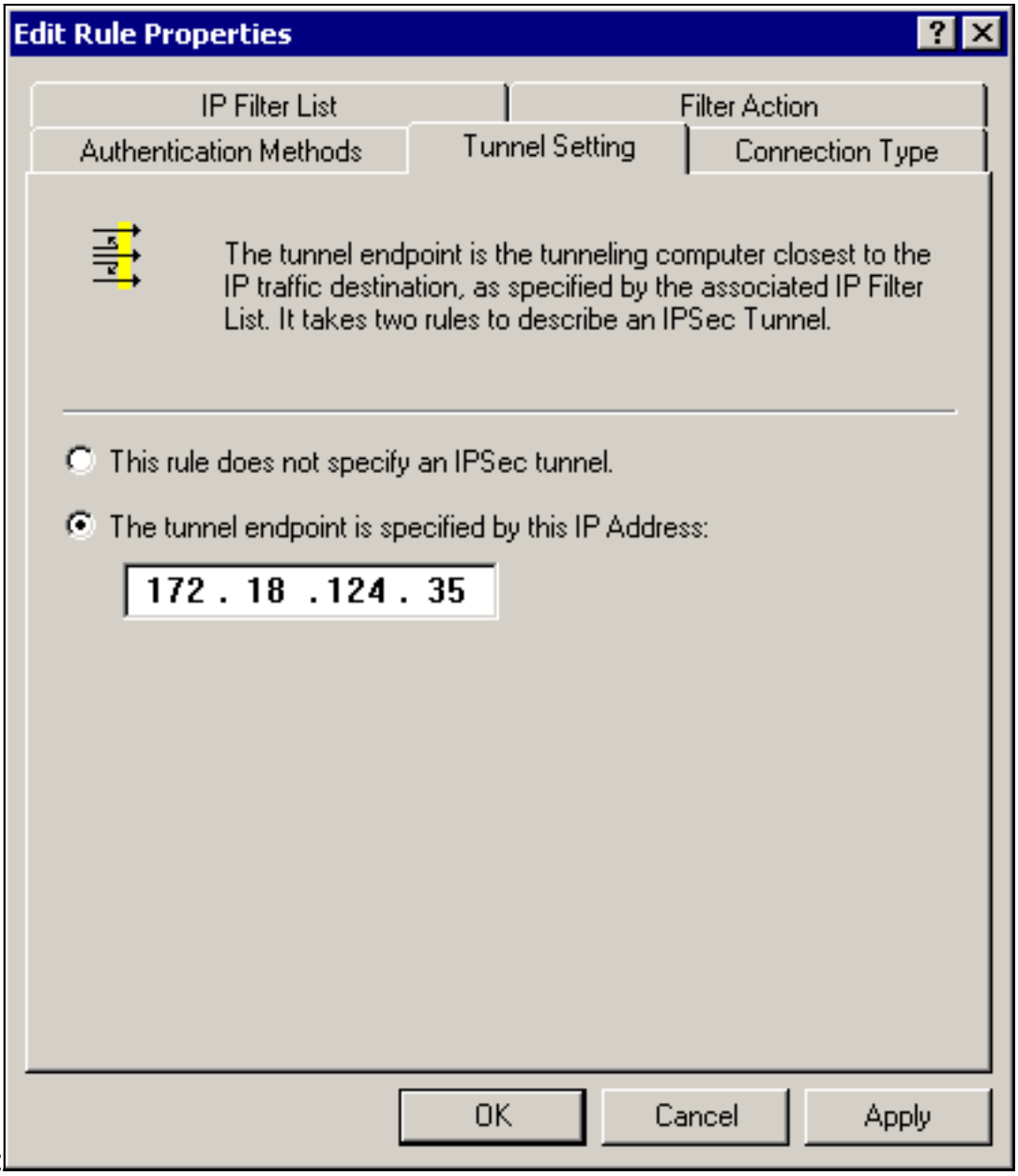


Tunneleinstellung - Verschlüsselungs-Peers:Für Cisco-



Microsoft:Für

Microsoft-Cisco:



Konfigurieren der Cisco Geräte

Konfigurieren Sie die Cisco Router-, PIX- und VPN-Konzentratoren wie in den folgenden Beispielen gezeigt.

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

Konfigurieren des Cisco 3640 Routers

Cisco Router 3640

`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
```

Konfigurieren von 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
```

Konfigurieren des VPN 3000-Konzentrators

Verwenden Sie die Menüoptionen und Parameter unten, um den VPN Concentrator nach Bedarf zu konfigurieren.

- Um ein IKE-Angebot hinzuzufügen, wählen Sie **Configuration > System > Tunneling Protocols > IPSec > IKE Proposals > Add a Proposal (Konfiguration > System > Tunneling-Protokolle > IPSec > IKE-Vorschläge) aus.**

  ```
  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
  ```

- Um den LAN-to-LAN-Tunnel zu definieren, wählen Sie **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN aus.**

  ```
  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
```

- Um die Sicherheitszuordnung zu ändern, wählen Sie **Configuration > Policy Management > Traffic Management > Security Associations > Modify aus.**

```
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
```

Konfigurieren des VPN 500-Konzentrators

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.
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihren Konfigurationen.

Befehle zur Fehlerbehebung

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

Cisco Router 3640

- **debug crypto engine** - Zeigt Debugmeldungen über Krypto Engines, die Verschlüsselung und Entschlüsselung durchführen.
- **debug crypto isakmp** - Zeigt Meldungen über IKE-Ereignisse an.
- **debug crypto ipsec** - Zeigt IPSec-Ereignisse an.
- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an.
- **show crypto ipsec sa** - Zeigt die Einstellungen an, die von aktuellen Sicherheitszuordnungen verwendet werden.
- **clear crypto isakmp** - (aus Konfigurationsmodus) Löscht alle aktiven IKE-Verbindungen.
- **clear crypto sa** - (aus dem Konfigurationsmodus) Löscht alle IPSec-Sicherheitszuordnungen.

PIX

- **debug crypto ipsec** - Zeigt die IPSec-Verhandlungen von Phase 2 an.
- **debug crypto isakmp** - Zeigt die Verhandlungen der Internet Security Association und des Key Management Protocol (ISAKMP) über Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **show crypto ipsec sa** - Zeigt die Sicherheitszuordnungen für Phase 2 an.
- **show crypto isakmp sa** - Zeigt die Sicherheitszuordnungen für Phase 1 an.
- **clear crypto isakmp** - (aus dem Konfigurationsmodus) Löscht die Sicherheitszuordnungen für Internet Key Exchange (IKE).
- **clear crypto ipsec sa** - (aus dem Konfigurationsmodus) Löscht IPSec-Sicherheitszuordnungen.

VPN 3000-Konzentrator

- - Starten Sie den VPN 300 Concentrator-Debugging, indem Sie **Configuration > System > Events > Classes > Modify** auswählen (Severity to Log=1-13, Severity to Console=1-3): IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - Das Ereignisprotokoll kann gelöscht oder abgerufen werden, indem Sie **Monitoring > Event Log (Überwachung > Ereignisprotokoll)** auswählen.
- - Der LAN-zu-LAN-Tunnelverkehr kann unter **Überwachung > Sitzungen** überwacht werden.
- - Der Tunnel kann unter **Administration > Administration Sessions > LAN-to-LAN Sessions > Actions - Logout** gelöscht werden.

VPN 5000 Concentrator

- **vpn trace dump all** - Zeigt Informationen über alle übereinstimmenden VPN-Verbindungen an, einschließlich Informationen über die Zeit, die VPN-Nummer, die tatsächliche IP-Adresse des Peers, die ausgeführten Skripts und im Falle eines Fehlers die Routine und die Leitungsnummer des Software-Codes, in dem der Fehler aufgetreten ist.
- **show vpn statistics** - Zeigt die folgenden Informationen für Benutzer, Partner und die Gesamtsumme für beide an. (Bei modularen Modellen umfasst die Anzeige einen Abschnitt für jeden Modulsteckplatz.) Current Active - Die aktuell aktiven Verbindungen. In Negot - Die derzeit verhandelnden Verbindungen. High Water - Die höchste Anzahl gleichzeitiger aktiver Verbindungen seit dem letzten Neustart. Running Total (Gesamt ausführen) - Die Gesamtzahl erfolgreicher Verbindungen seit dem letzten Neustart. Tunnel Starts (Tunnel wird gestartet) - Die Anzahl der Tunnelstarts. Tunnel OK - Die Anzahl der Tunnel, für die keine Fehler aufgetreten sind. Tunnel Error (Tunnelfehler): Die Anzahl der Tunnel mit Fehlern.
- **show vpn statistics ausführliche** - Zeigt Statistiken zur ISAKMP-Aushandlung und viele weitere aktive Verbindungsstatistiken an.

Zugehörige Informationen

- Cisco VPN Concentrators der Serie 5000 - Ankündigung des Vertriebsendes
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Technischer Support - Cisco Systems