IPSec configureren tussen een Microsoft Windows 2000-server en een Cisco-apparaat

Inhoud

Inleiding

Dit document toont aan hoe u een IPSec-tunnel met pre-gedeelde sleutels kunt vormen om zich aan 2 privé netwerken aan te sluiten: een privaat netwerk (192.168.l.X) binnen een Cisco-apparaat en een privaat netwerk (10.32.50.X) binnen de Microsoft 2000-server. We gaan ervan uit dat het verkeer van binnen het Cisco-apparaat en binnen de Cisco-server van 2000 naar het internet (hier weergegeven door de 172.18.124.X-netwerken) toeneemt voordat u deze configuratie start.

U vindt uitgebreide informatie over het configureren van de Microsoft Windows 2000-server op de Microsoft website: http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP

Voordat u begint

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Voorwaarden

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

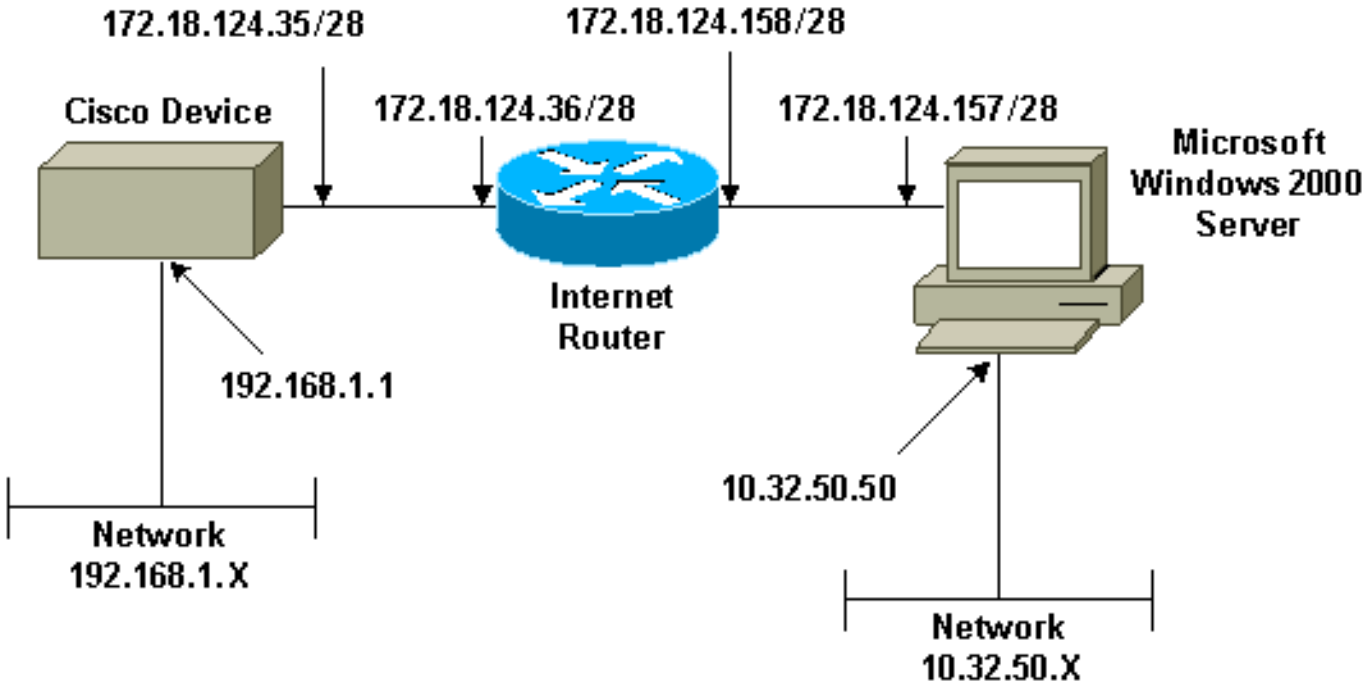
Deze configuraties zijn ontwikkeld en getest met behulp van de onderstaande software- en hardwareversies.

- Microsoft Windows 2000 Server 5.0.2195
- Cisco 3640 router met Cisco IOS® softwarerelease c3640-ik2o3s-mz.121-5.T.bin
- Cisco Secure PIX-firewall met PIX-softwarerelease 5.2.1
- Cisco VPN 3000 Concentrator met VPN 3000 Concentrator-software versie 2.5.2.F
- Cisco VPN 5000 Concentrator met VPN 5000 Concentrator-software versie 5.2.19

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Netwerkdiagram

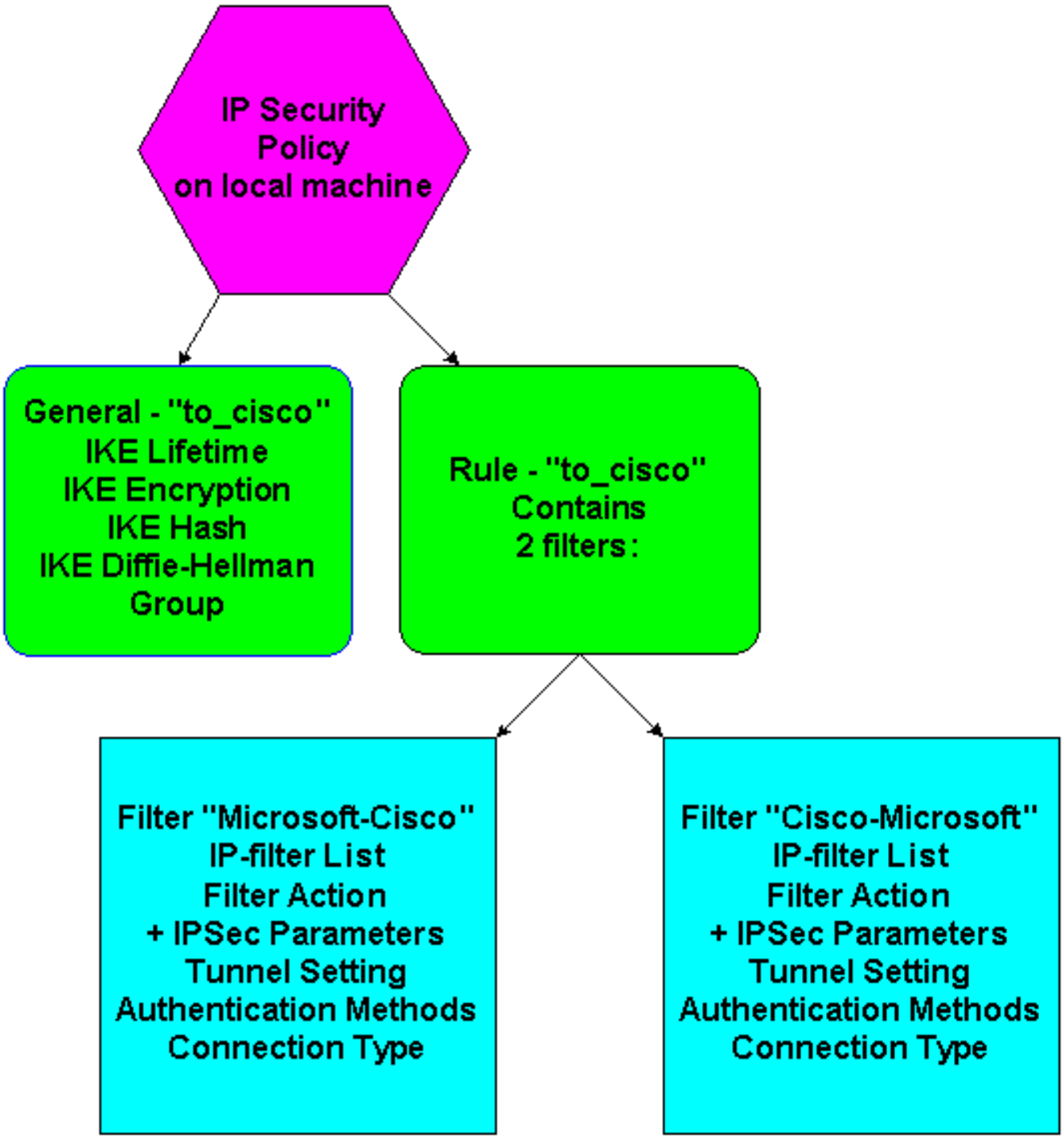
Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



De Microsoft Windows 2000-server configureren om met Cisco-apparaten te werken

Taken die worden uitgevoerd

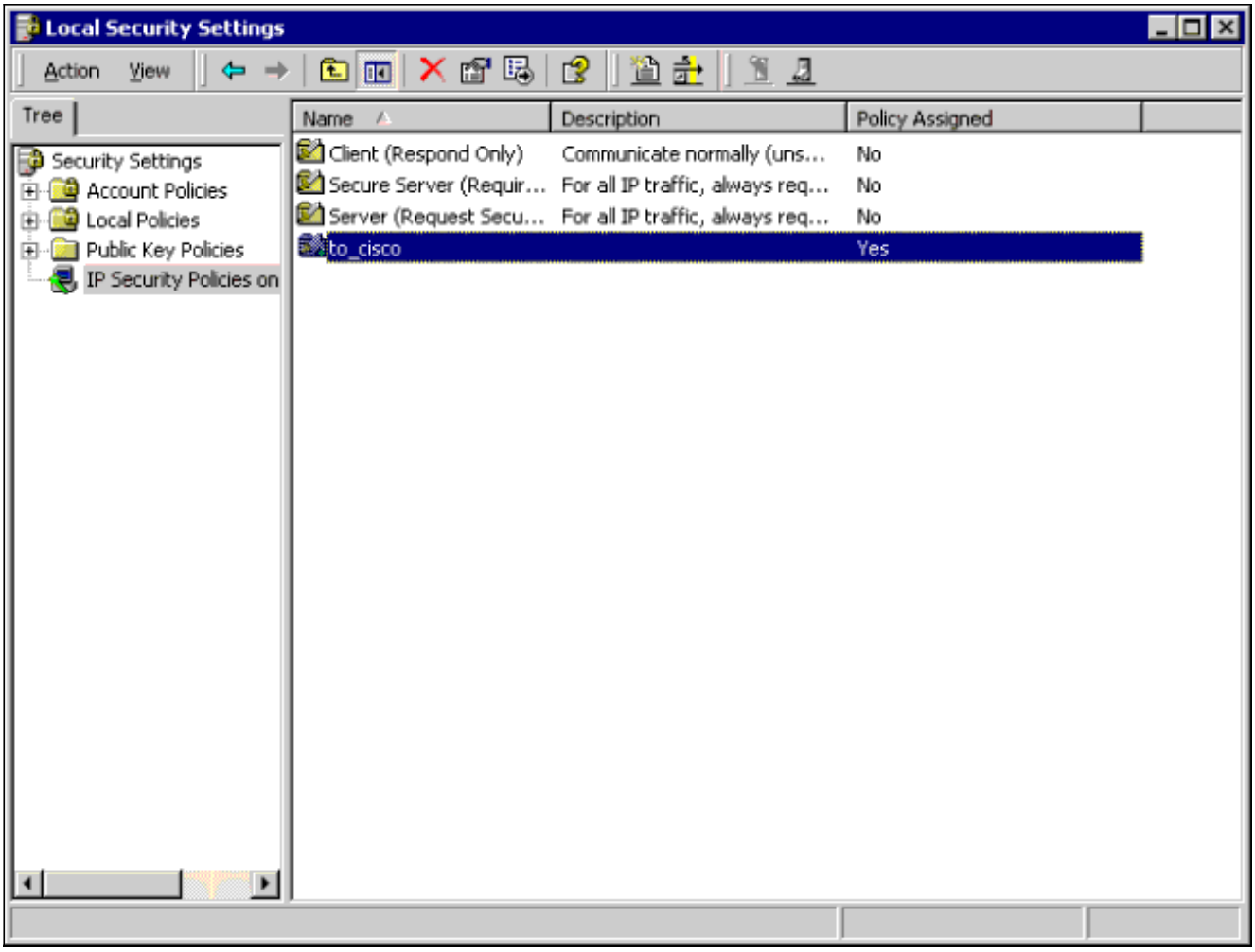
In dit diagram worden de taken weergegeven die in de serverconfiguratie van Microsoft Windows 2000 zijn uitgevoerd:



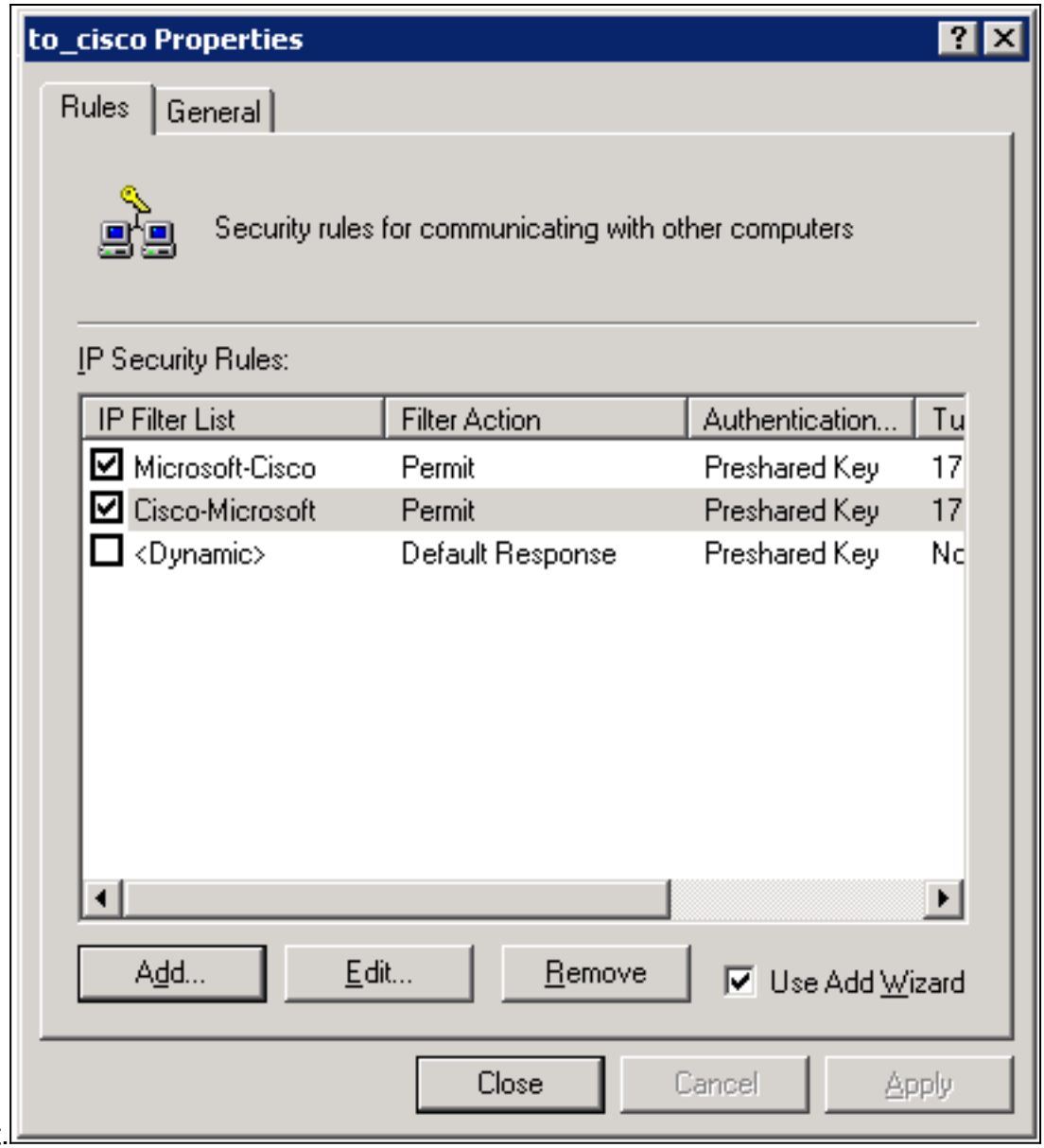
Stapsgewijze instructies

Nadat u de configuratie-instructies op de Microsoft website hebt gevolgd, gebruikt u de volgende stappen om te controleren of uw configuratie met Cisco-apparaten kan werken. Opmerkingen en wijzigingen worden genoteerd met de schermopnamen.

1. Klik op **Start > Run > secpol.msc** op de Microsoft Windows 2000 Server en controleer de informatie op de volgende schermen.Nadat de instructies op de Microsoft website werden gebruikt om een server van 2000 te configureren werd de volgende tunnelinformatie weergegeven.**Opmerking:** De voorbeeldregel wordt "to_cisco" genoemd.

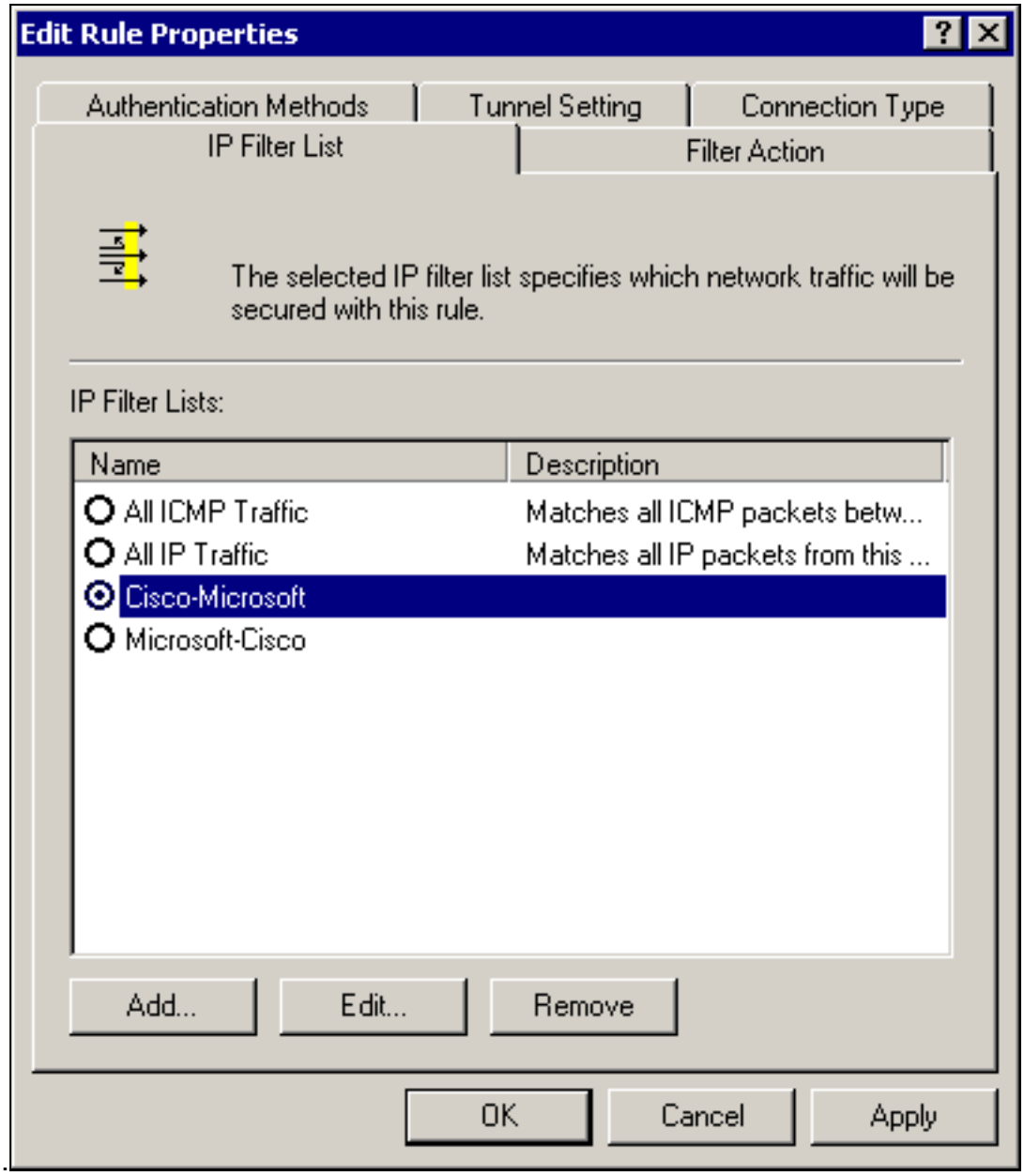


2. Deze voorbeeldregel bevat twee filters: Microsoft-Cisco en Cisco-



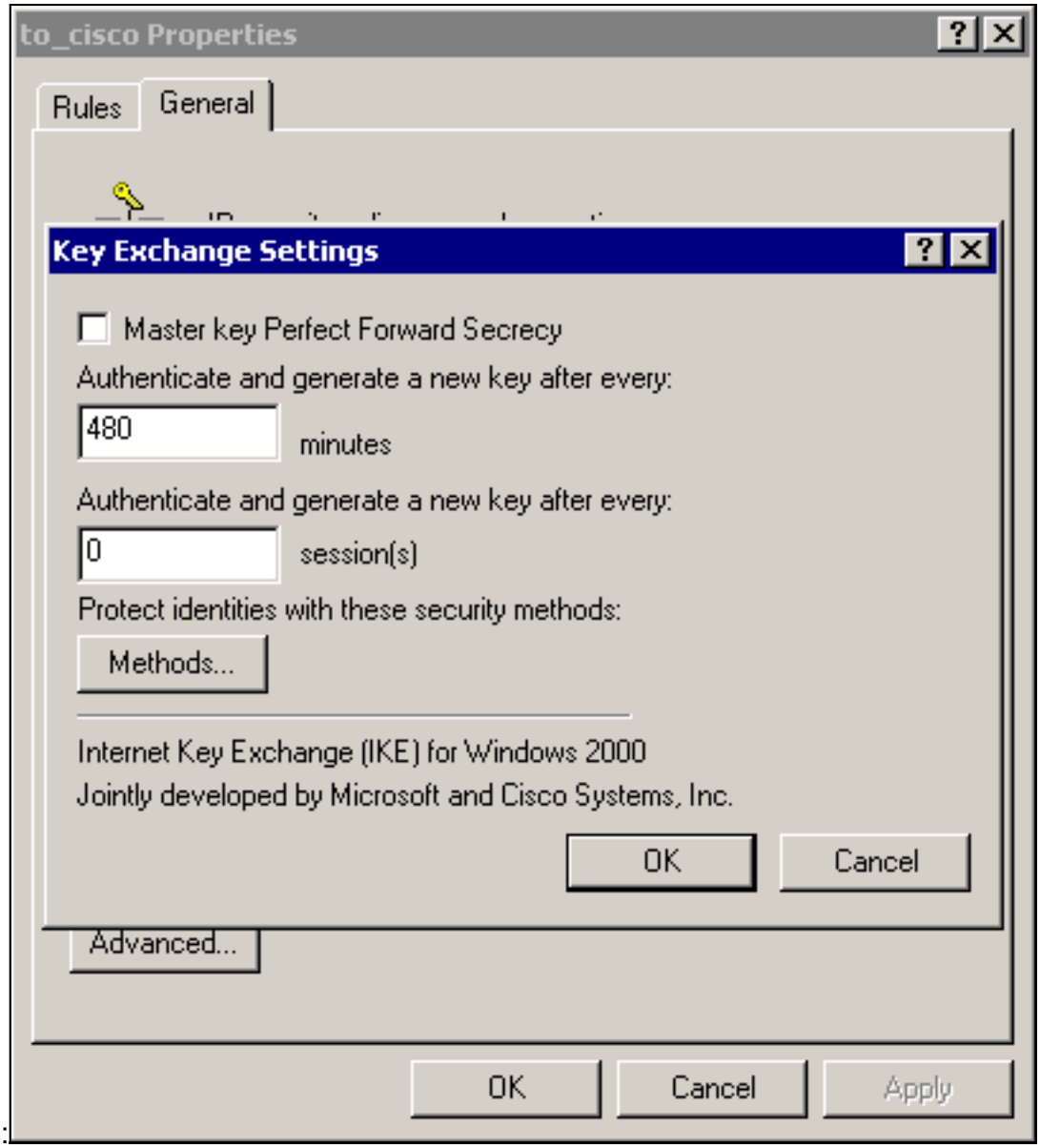
Microsoft.

3. Selecteer de beveiligingsregel van Cisco-Microsoft IP en klik vervolgens op **Bewerken** om de IP-filterlijsten te bekijken/toevoegen of



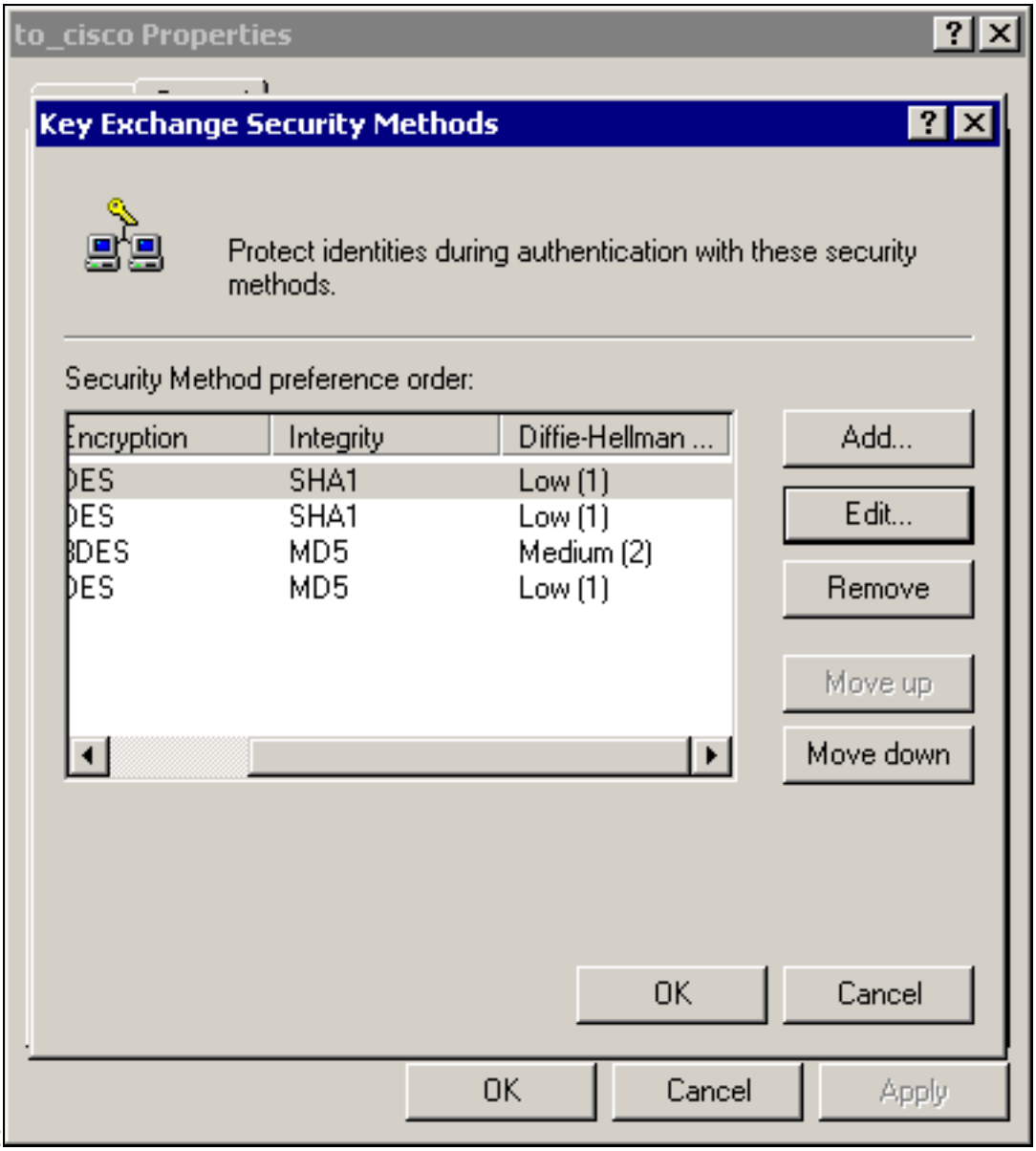
bewerken.

4. Het **tabblad General > Advanced** heeft de **IKE-levensduur** (480 minuten = 28800



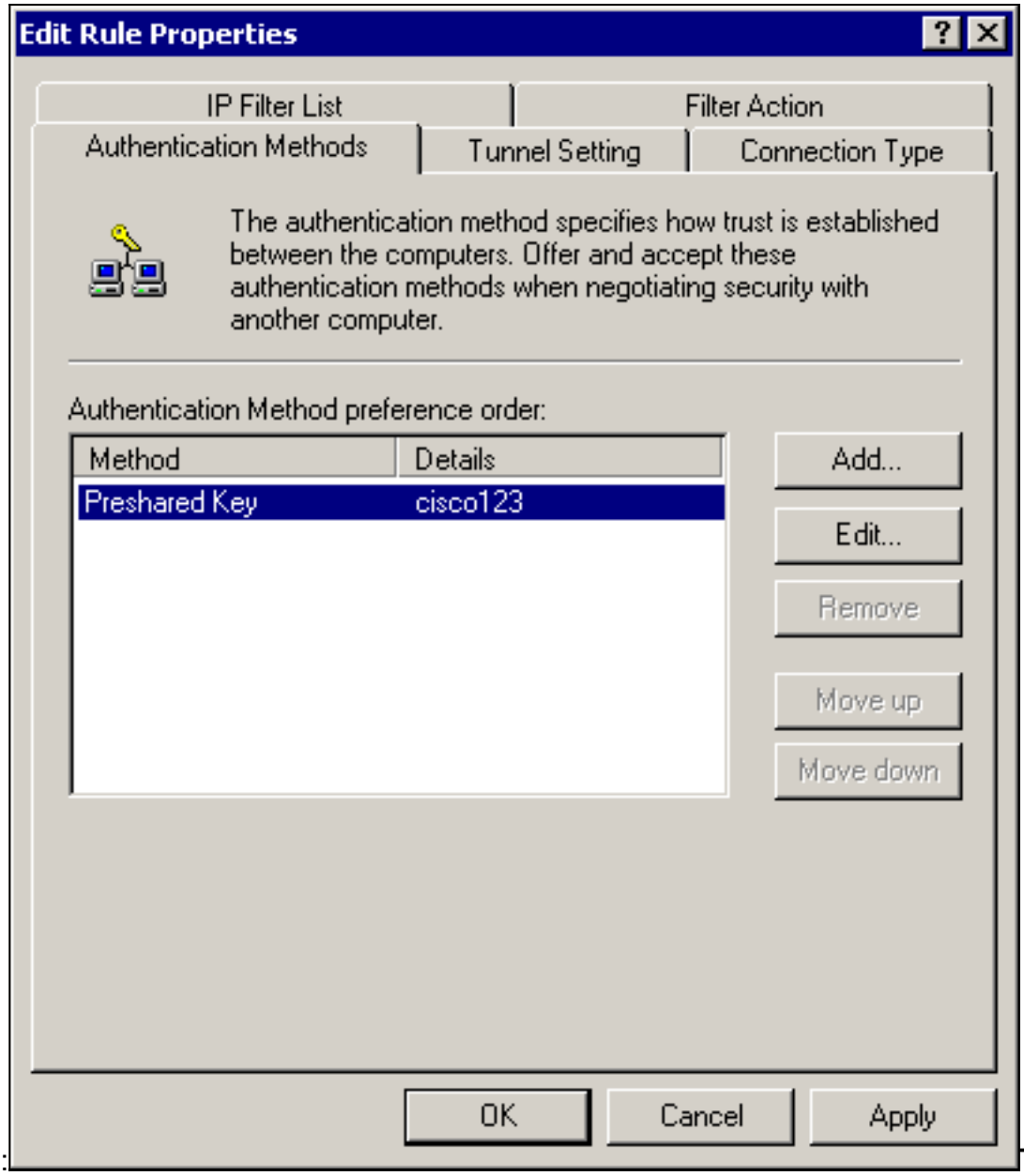
seconden):

5. Het **tabblad General > Advanced > Methods** heeft de **IKE-encryptiemethode** (DES), **IKE hashing** (SHA1) en de **groep Diffie-Helman**

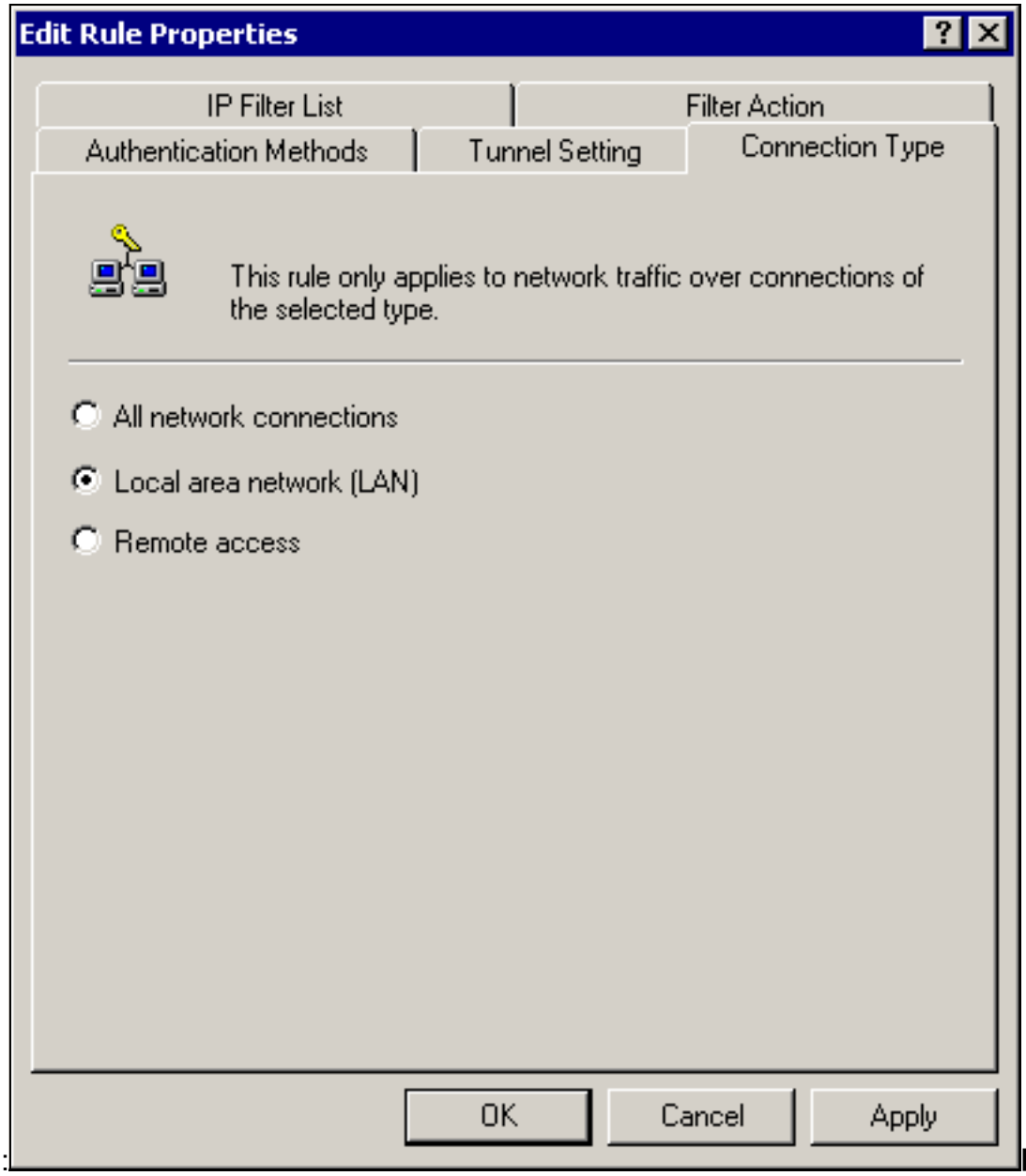


(Laag(1)):

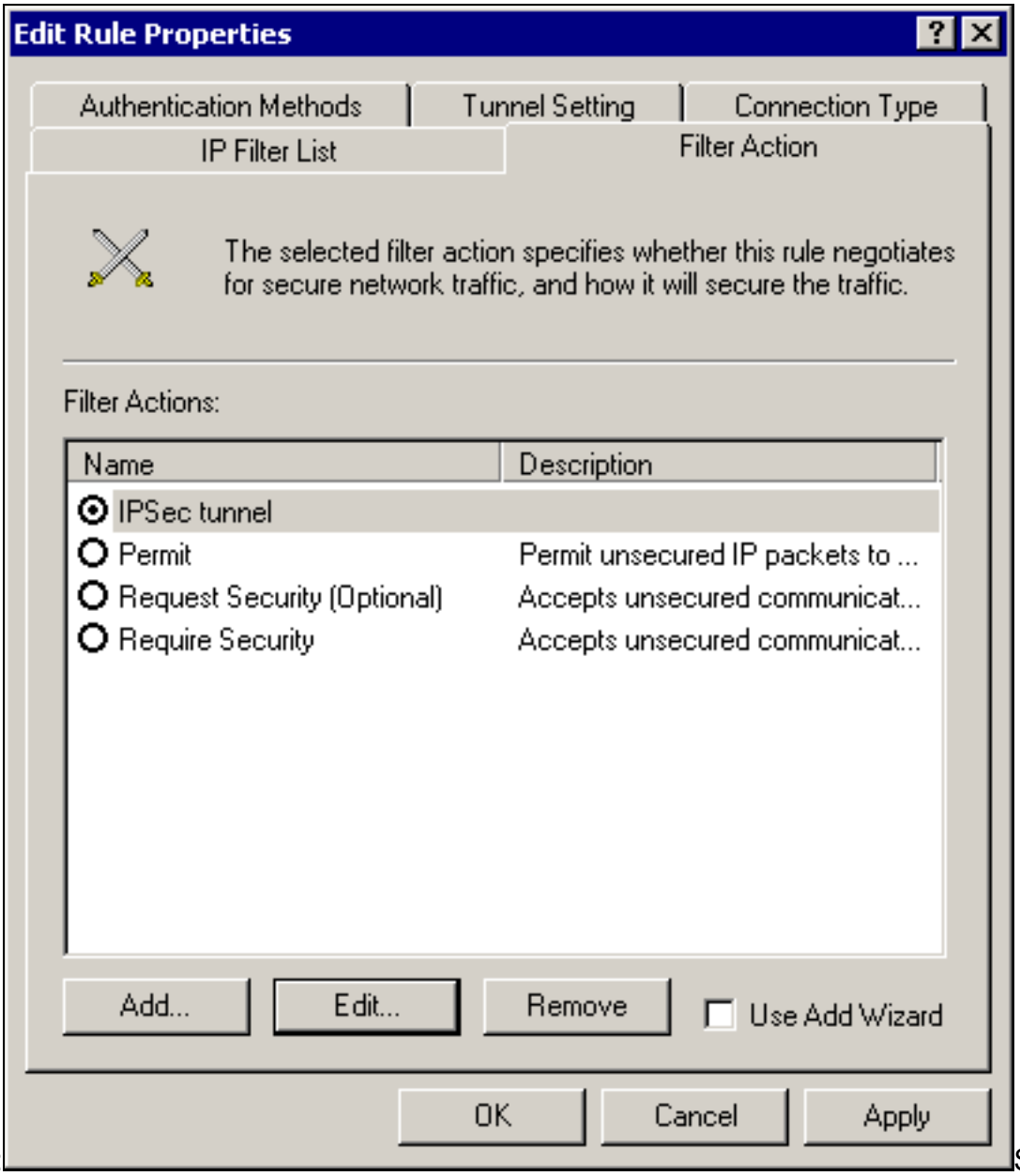
6. Elk filter heeft 5 tabbladen:**Verificatiemethoden** (PreShared keys voor internet Key Exchange



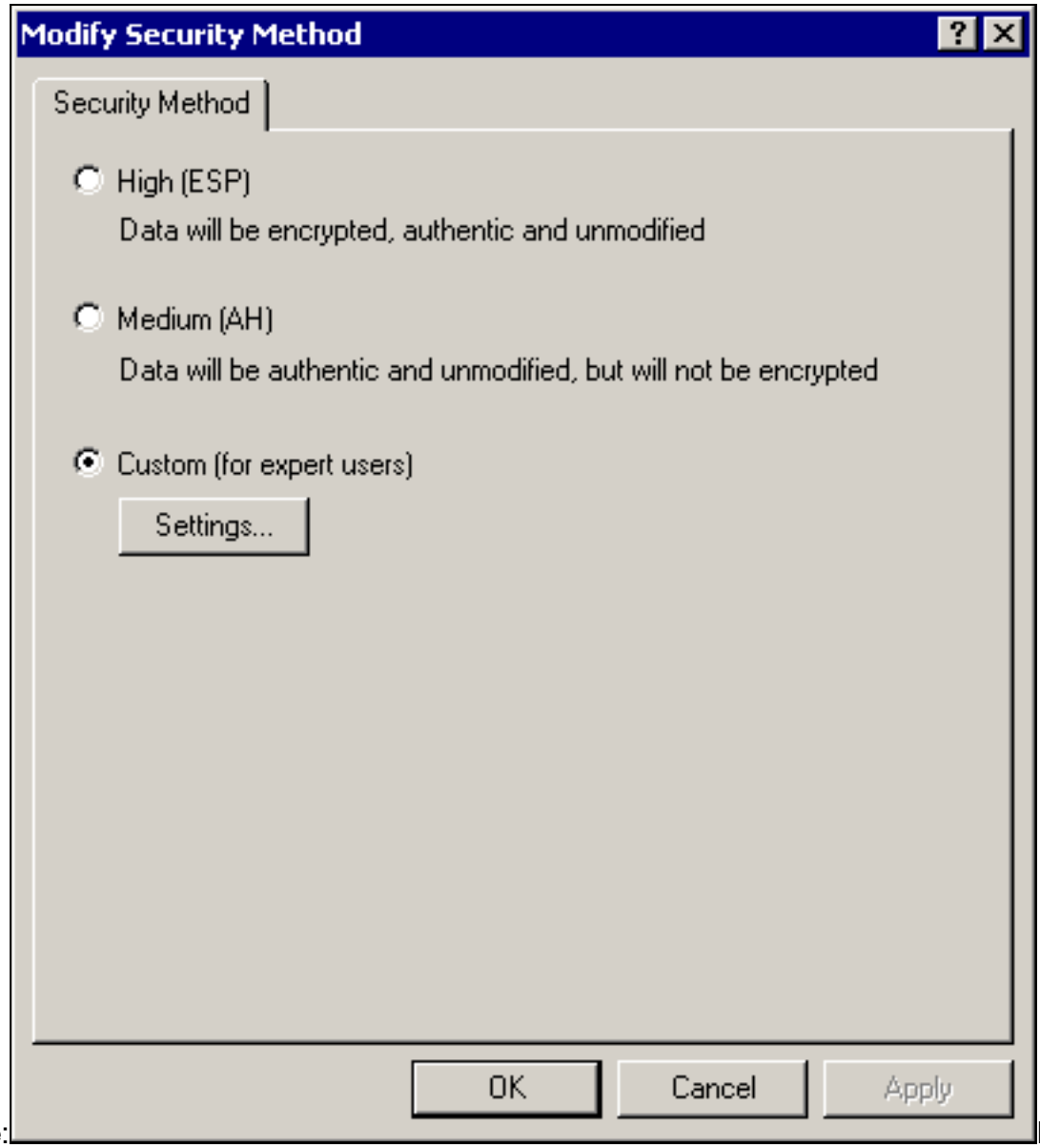
[IKE]): **Type verbinding**



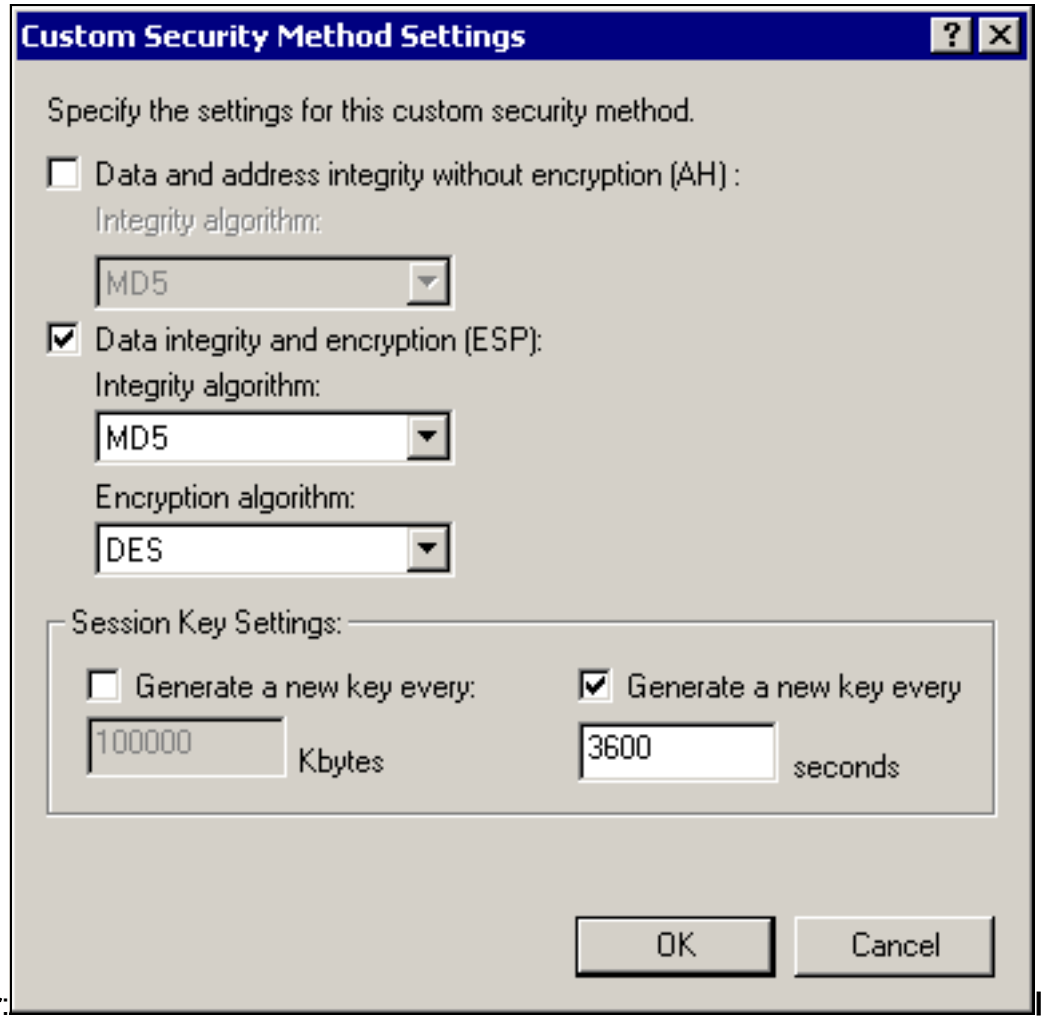
(LAN): **Filteractie**



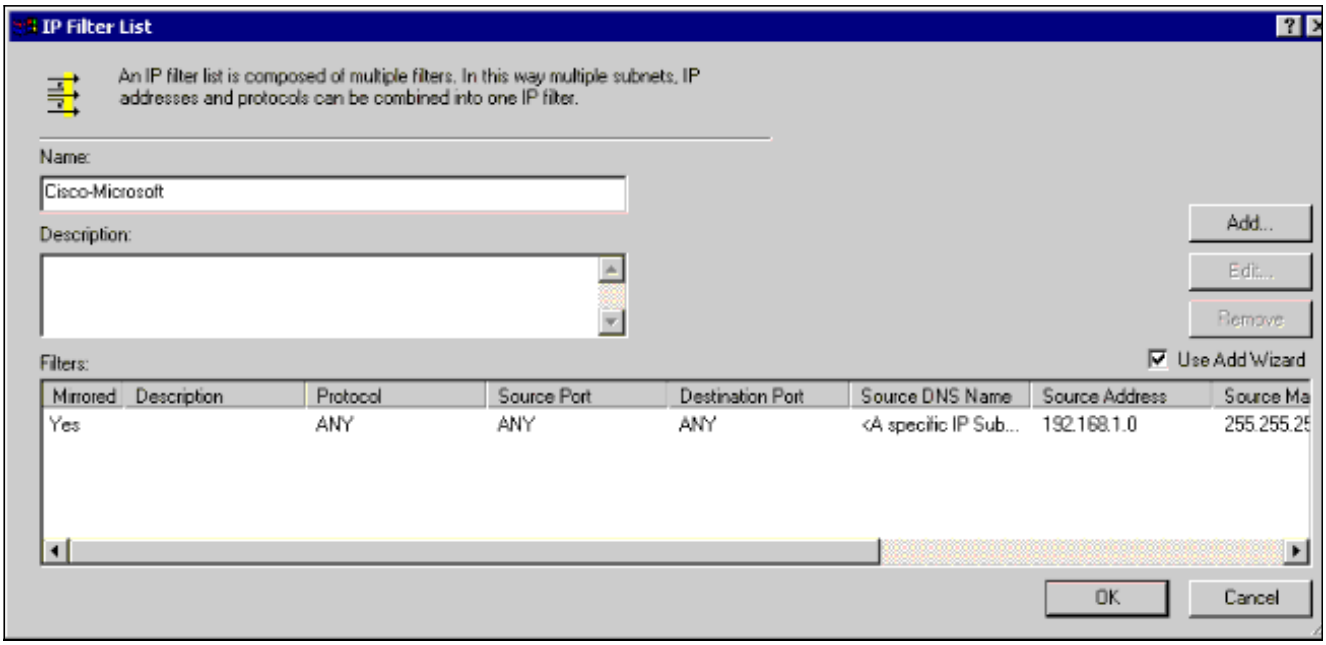
(IPSec): Selecteer **Filteractie > IPSec-tunnel > Bewerken > Bewerken** en klik op



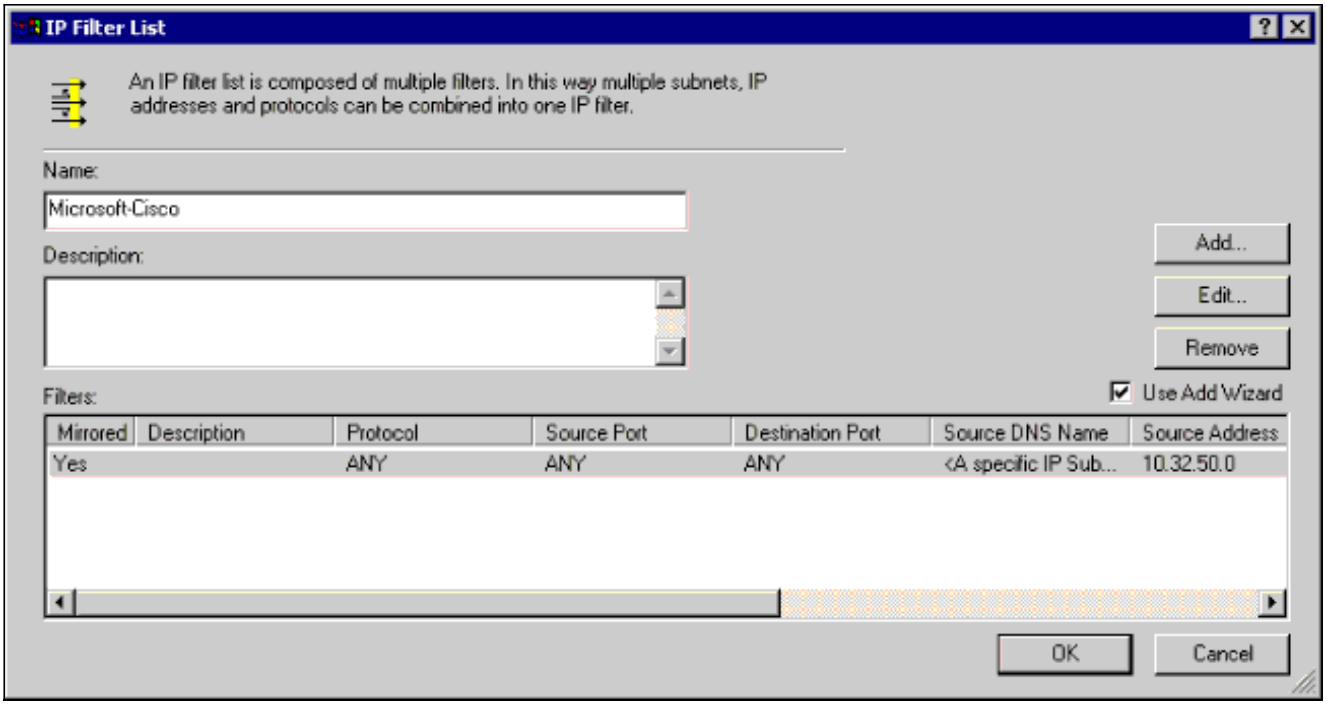
Aangepaste:Klik op **Instellingen - IPSec**-transformaties en **IPSec-**



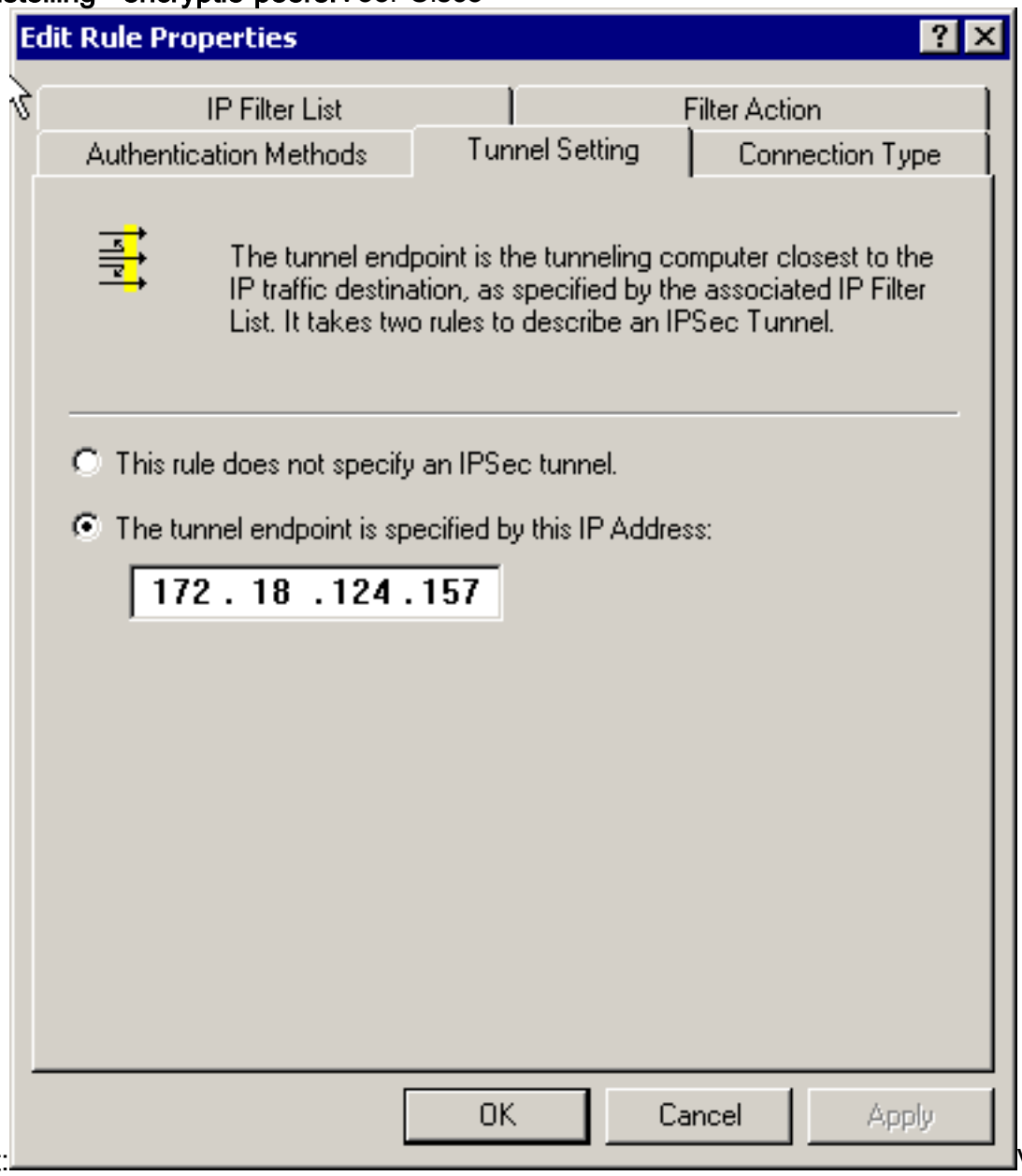
levensduur:**IP-filterlijst - bron**- en **doelnetwerken** die moeten worden versleuteld:Voor Cisco-Microsoft:



Voor Microsoft-Cisco:

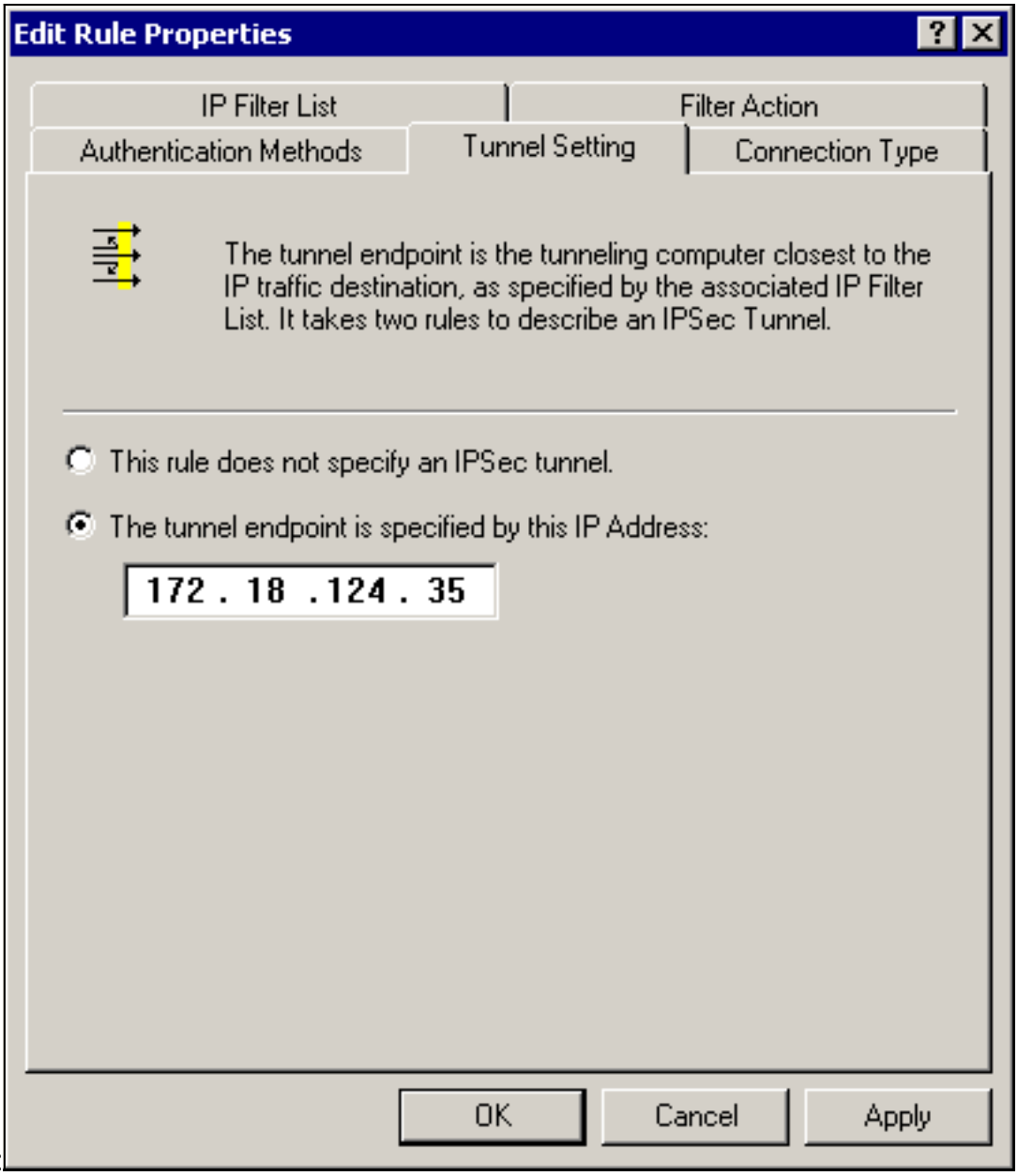


Tunnel instelling - encryptie-peers: Voor Cisco-



Microsoft:Voor

Microsoft-Cisco:



De Cisco-apparaten configureren

Configureer de router, PIX en VPN-concentrators van Cisco zoals in de onderstaande voorbeelden wordt weergegeven.

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

Cisco 3640 router configureren

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 configureren

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
```

De VPN-concentratie configureren 3000

Gebruik de menuopties en de parameters die hieronder worden weergegeven om de VPN-centrator zo nodig te configureren.

- Als u een IKE-voorstel wilt toevoegen, selecteert u **Configuration > System > Tunneling Protocols > IPSec > IKE-voorstellen > Add a voorstel.**

  ```
  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
  ```

- Om de LAN-to-LAN tunnel te definiëren, selecteert u **Configuration > System > Tunneling-protocollen > 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
```

- Als u de beveiligingsassociatie wilt wijzigen, selecteert u **Configuration > Policy Management > Traffic Management > Security Associations > Wijzigen.**

```
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
```

De VPN 5000-concentratie configureren

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.
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen op te lossen in uw configuraties.

Opdrachten voor troubleshooting

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met **show genereren.**

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

Cisco 3640 router

- **debug - crypto motor** - toont debug - berichten over crypto motoren, die encryptie en decryptie uitvoeren.
- **debug crypto isakmp** - Geeft berichten over IKE gebeurtenissen weer.
- **debug van crypto ipsec** - Geeft gebeurtenissen van IPSec weer.
- **toon crypto isakmp sa** - laat alle huidige IKE security associaties (SA's) bij een peer zien.
- **toon crypto ipsec sa** - toont de instellingen die door huidige veiligheidsassociaties worden gebruikt.
- **duidelijke crypto isakmp** - (vanaf de configuratiemodus) reinigt alle actieve IKE-verbindingen.
- **duidelijke crypto sa** - (van configuratiewijze) verwijdert alle IPSec security associaties.

PIX

- **debug crypto ipsec** - toont de IPSec-onderhandelingen van fase 2.
- **debug crypto isakmp** - toont de onderhandelingen over fase 1 van de Internet Security Association en Key Management Protocol (ISAKMP).
- **debug-encryptie** - Geeft het versleutelde verkeer weer.
- **toon crypto ipsec sa** - toont de fase 2 veiligheidsassociaties .
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties .
- **duidelijke crypto isakmp** - (van configuratie mode) Clears Internet Key Exchange (IKE) - veiligheidsassociaties.
- **duidelijke crypto ipsec sa** - (van configuratie mode) reinigt IPSec security associaties.

VPN 3000 Concentrator

- - Start het VPN 3000 Concentrator-debug door **Configuration > System > Events > Classes > Change** (Severity to Log=1-13, Severity to Console=1-3) te selecteren: IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE
- - Het logbestand van de gebeurtenis kan worden gewist of opgehaald door de optie **Monitoring > Event Log** te selecteren.
- - Het LAN-to-LAN tunnelverkeer kan worden gevolgd bij **bewaking > sessies**.
- - De tunnel kan worden geklaard in **Beheer > Zessies beheren > LAN-to-LAN sessies > Handelingen - Uitlijning.**

VPN 5000 Concentrator

- **vpn-traceringstool** - Geeft informatie over alle bijbehorende VPN-verbindingen weer, inclusief

informatie over de tijd, het VPN-nummer, het echte IP-adres van de peer, de scripts die zijn uitgevoerd en in het geval van een fout, het routine- en regelnummer van de software-code waar de fout is opgetreden.
- **vpn statistieken tonen** - toont de volgende informatie voor gebruikers, Partners, en het Totaal voor beide. (Voor modulaire modellen bevat de weergave een gedeelte voor elke modulesleuf.) Actief - de huidige actieve verbindingen. In Negot - De huidige onderhandelingsverbindingen. Hoog water - het hoogste aantal gelijktijdige actieve verbindingen sinds de laatste herstart. Totaal uitvoeren - Het totale aantal succesvolle verbindingen sinds de laatste herstart. Tunnel start - het aantal tunnels start. Tunnel OK - het aantal tunnels waarvoor geen fouten waren. Tunnelfout - het aantal tunnels met fouten.
- **show vpn statistics breedband** - toont onderhandelingsstatistieken van ISAKMP en veel meer actieve verbindingsstatistieken.

Gerelateerde informatie

- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning - Cisco-systemen