Een IPsec-tunnels configureren - Cisco VPN 5000 Concentrator om controlepunt 4.1-firewall te configureren

Inhoud

Inleiding

Dit document toont aan hoe u een IPsec-tunnel met pre-Shared Toetsen kunt vormen om zich aan twee particuliere netwerken aan te sluiten. Het sluit zich aan bij een privaat netwerk binnen Cisco VPN 5000 Concentrator (192.168.1.x) aan een privaat netwerk binnen de Checkpoint 4.1 Firewall (10.32.50.x). Er wordt aangenomen dat het verkeer van binnen de VPN-centrator en binnen het checkpoint naar het internet (in dit document weergegeven door de 172.18.124.x-netwerken) toeneemt voordat u deze configuratie start.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator-softwareversie 5.2.19.001
- Control-point 4.1-firewall

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

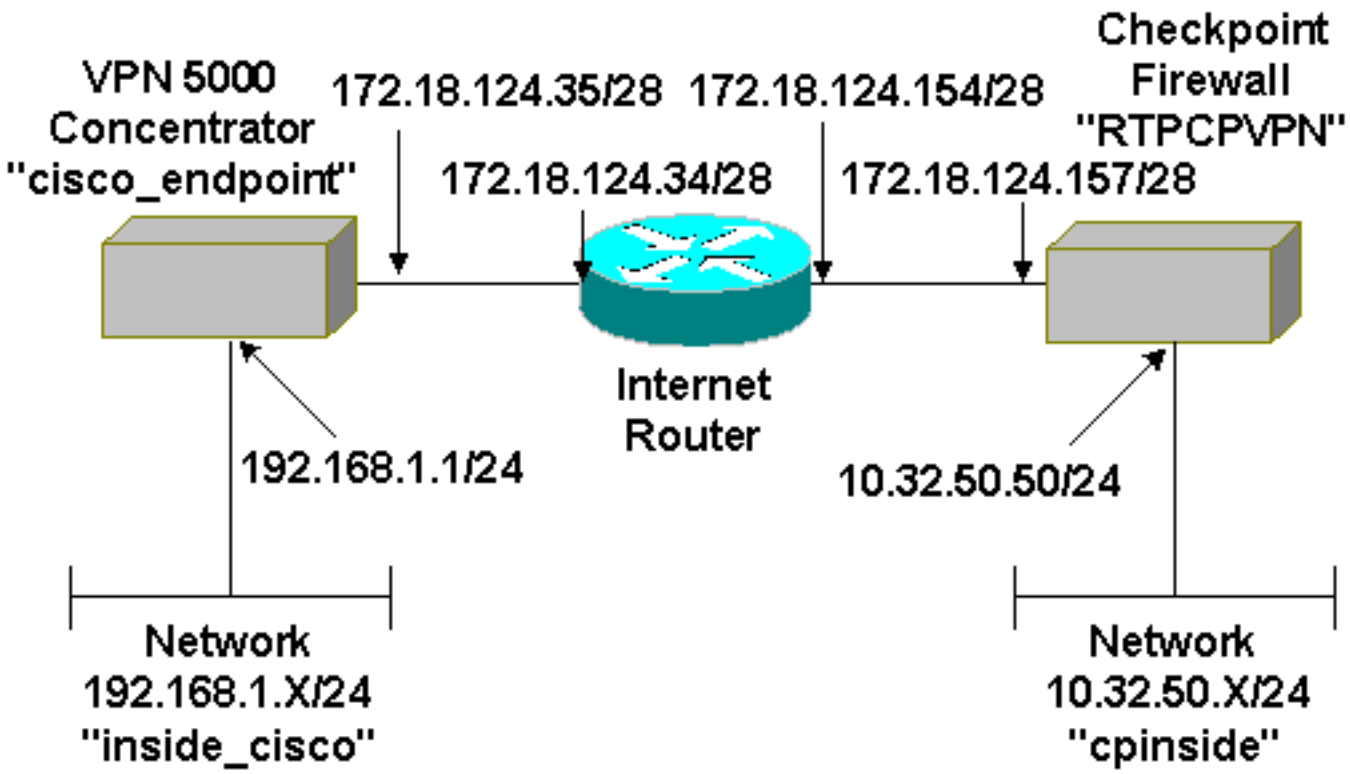
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuratie.

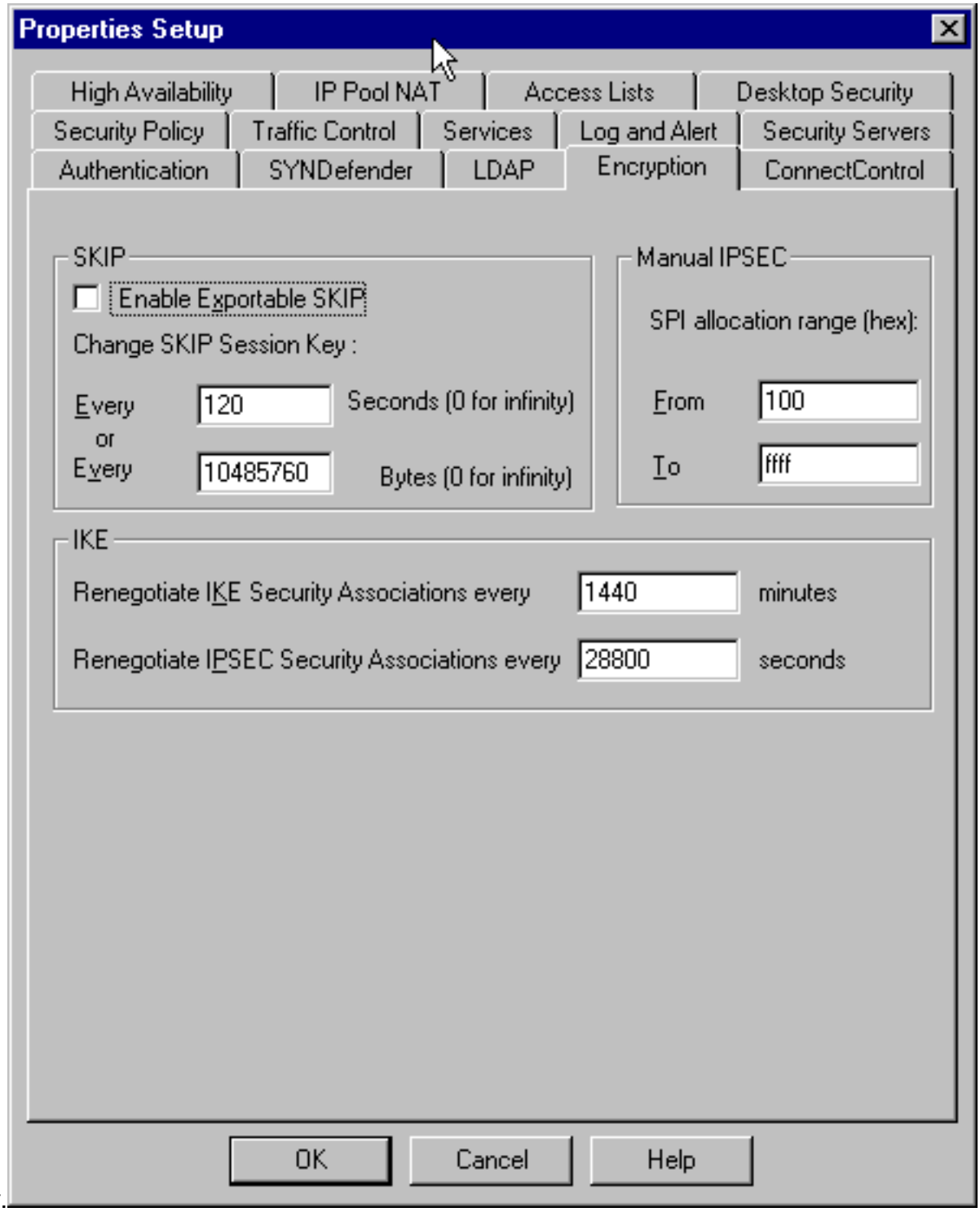
Cisco VPN 5000 Concentrator

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Control-point 4.1-firewall

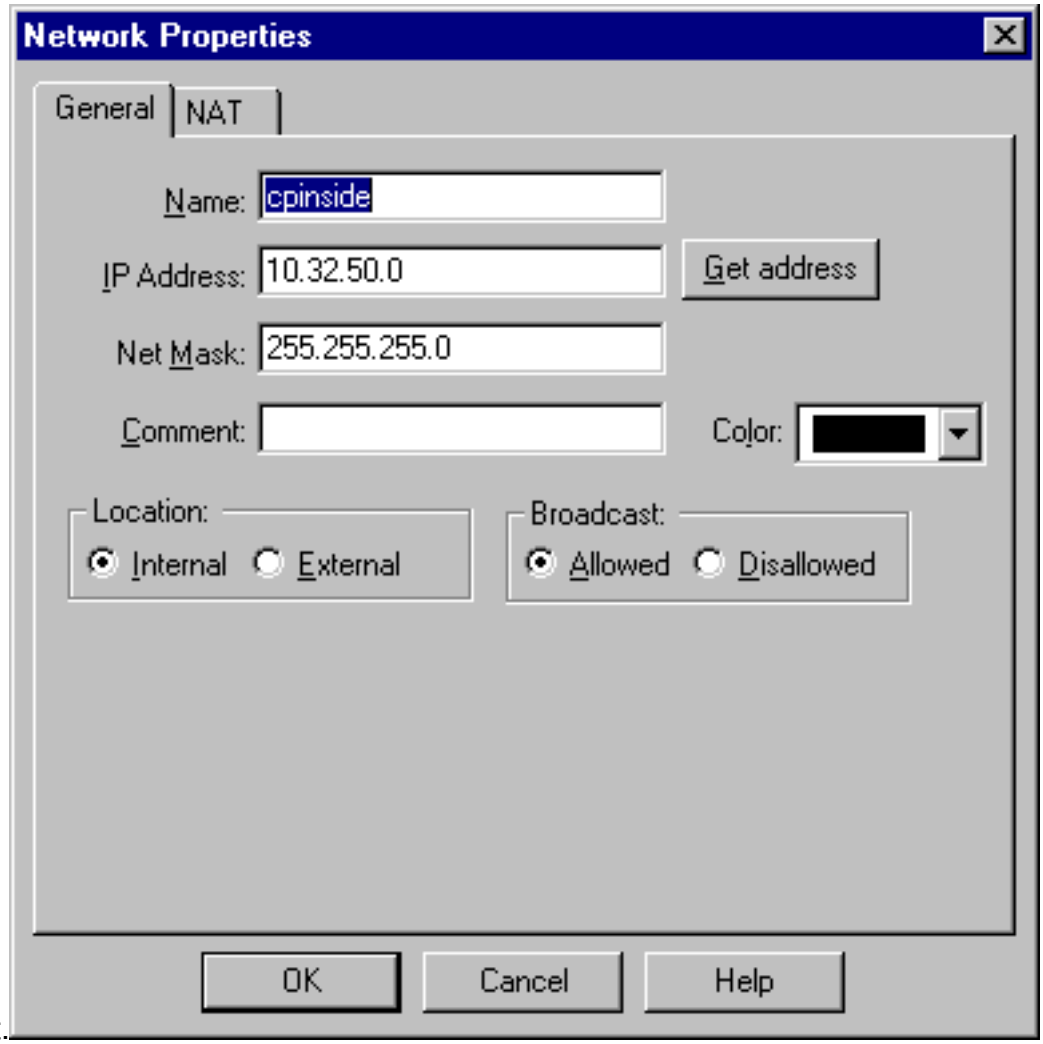
Volg deze stappen om de firewall van checkpoint 4.1 te configureren.

1. Selecteer **Properties > Encryption** om het checkpoint IPsec-reddingstijden in te stellen om met de **KeyLifeSecs-**opdracht **overeen te komen**: 28800 VPN Concentrator.**Opmerking:** Laat de IKE (Checkpoint Internet Key Exchange)-levensduur bij de standaardinstelling



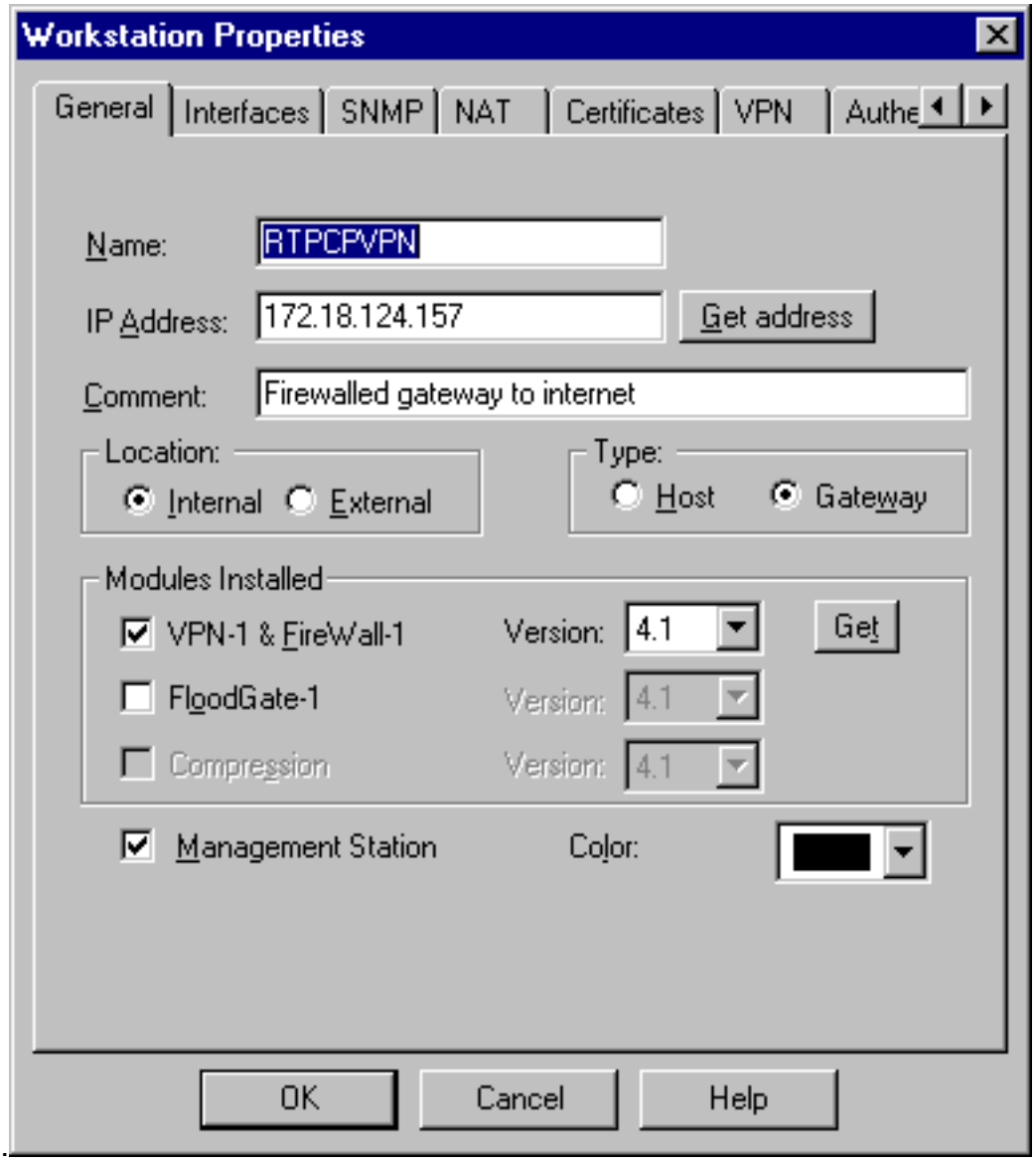
achter.

2. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het interne netwerk ("component") achter het Selectieteken te configureren. Dit moet overeenkomen met de **peer = "10.32.50.0/24"** VPN Concentrator



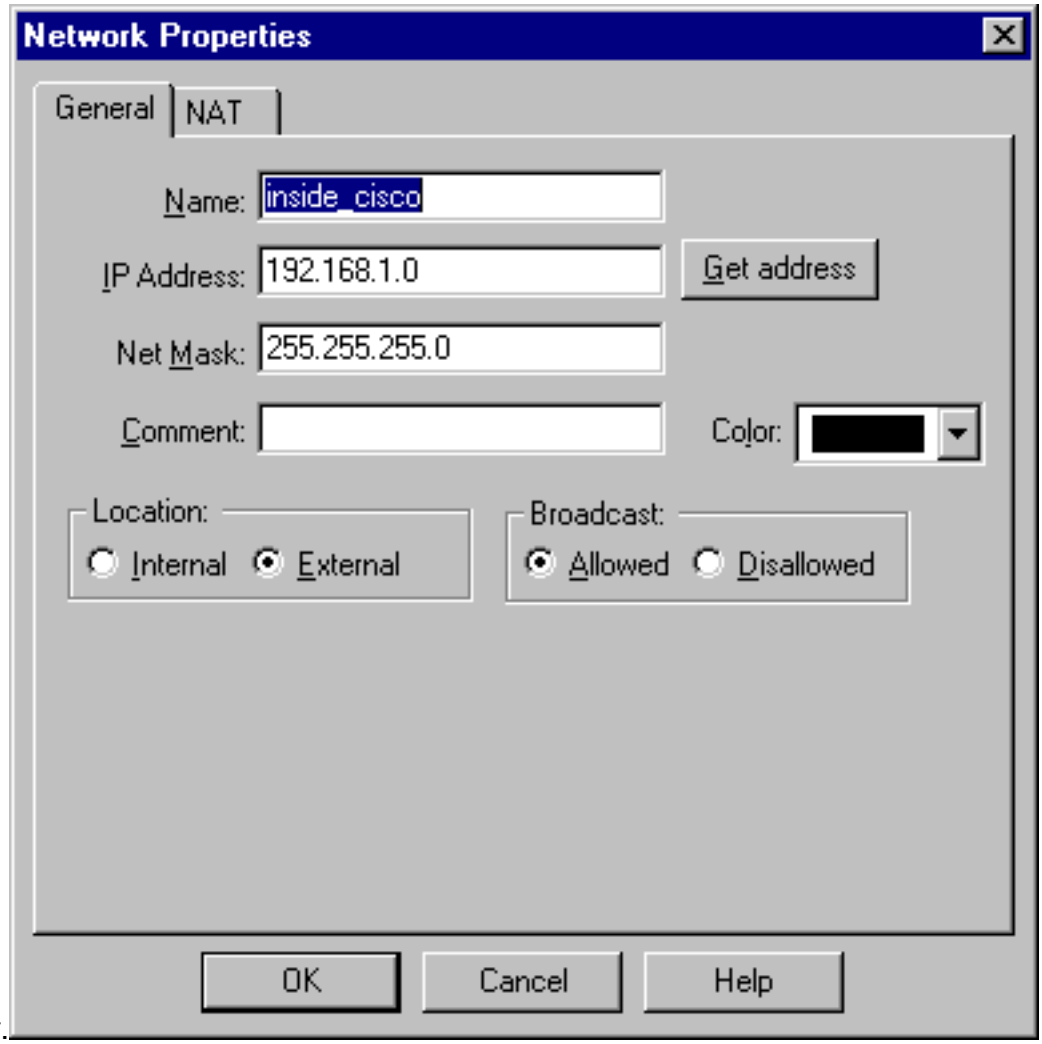
opdracht.

3. Selecteer **Manager > Netwerkobjecten > Bewerken** om het object te bewerken voor het eindpunt van de gateway ("RTPC VPN"-controle) waarnaar de VPN-Concentrator in de **partner = <ip>** opdracht wijst.Selecteer **Intern** onder Locatie.Selecteer **Gateway** voor type.Controleer **VPN-1 en FireWall-1** en **beheerstation** onder de geïnstalleerde



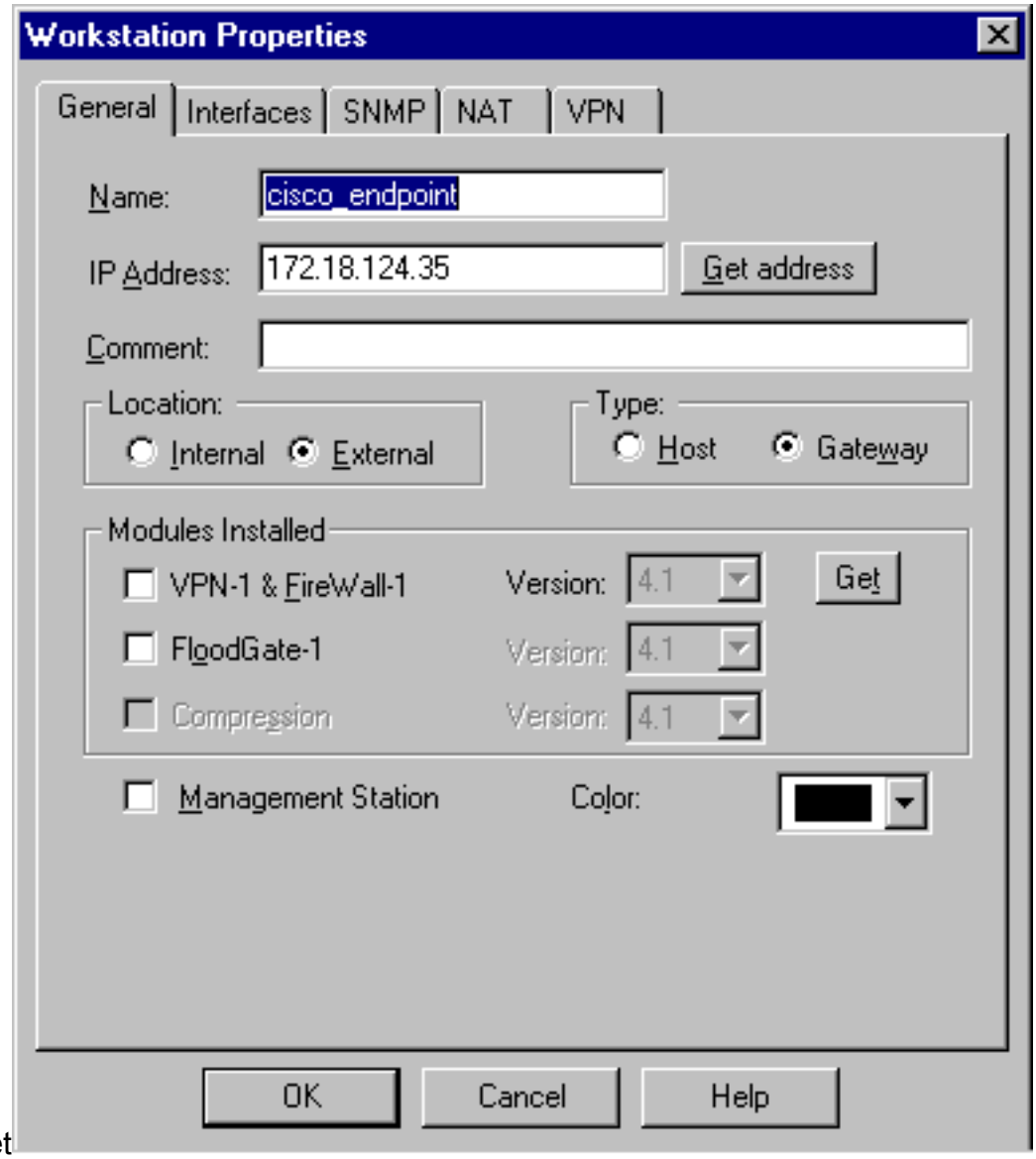
modules.

4. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het externe netwerk ("interne_cisco") achter de VPN-centrator te configureren.Dit moet overeenkomen met de **opdracht LocalAccess = <192.168.1.0/24>**VPN



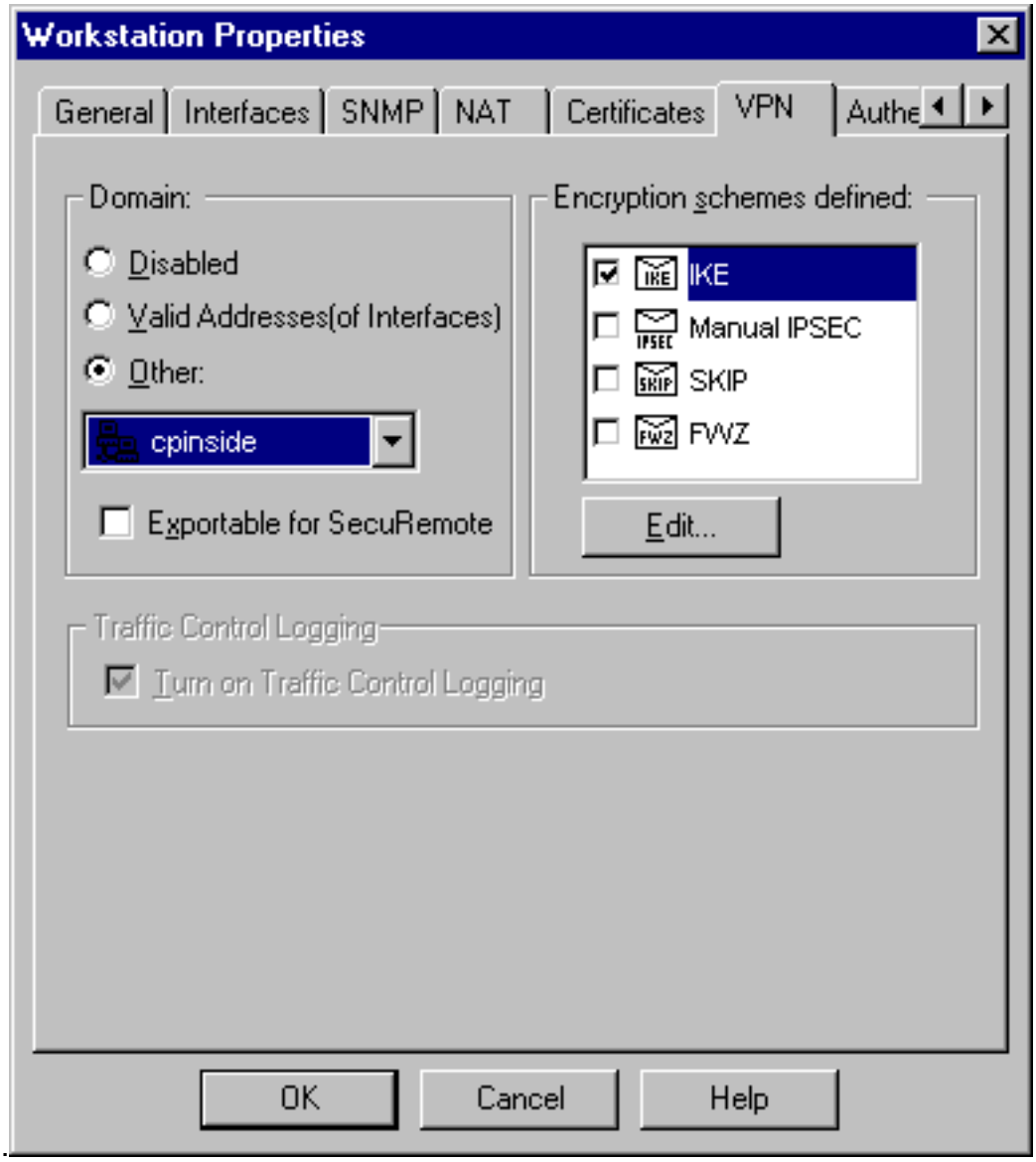
Concentrator.

5. Selecteer **Manager > Netwerkobjecten > Nieuw > Workstation** om een object voor de externe ("cisco_endpoints") VPN Concentrator-gateway toe te voegen.Dit is de "buiten" interface van de VPN-Concentrator met connectiviteit op het Selectieteken (in dit document is 172.18.124.35 het IP-adres in het **IPA-adres = <ip>**opdracht).Selecteer **Extern** onder Locatie. Selecteer **Gateway** voor type.**Opmerking:** controleer VPN-1/FireWall-1



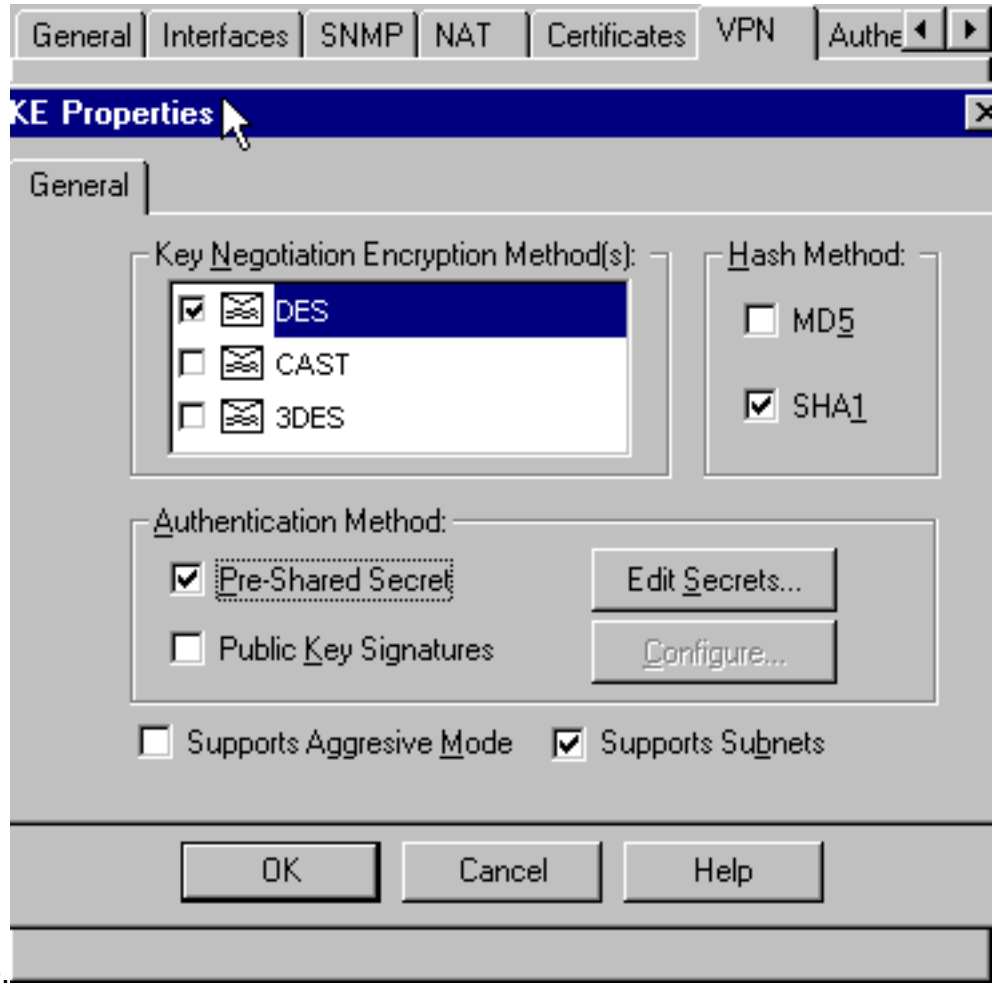
niet

6. Selecteer **Manager > Netwerkobjecten > Bewerken** om het tabblad Selectiepunt te bewerken (genaamd "RTPVPN") VPN-tabblad. Selecteer onder Domain, **Andere** en selecteer dan de binnenkant van het Checkpoint netwerk (genoemd "component") in de vervolgkeuzelijst. Selecteer onder Encryption schemes die worden gedefinieerd **IKE** en klik vervolgens op



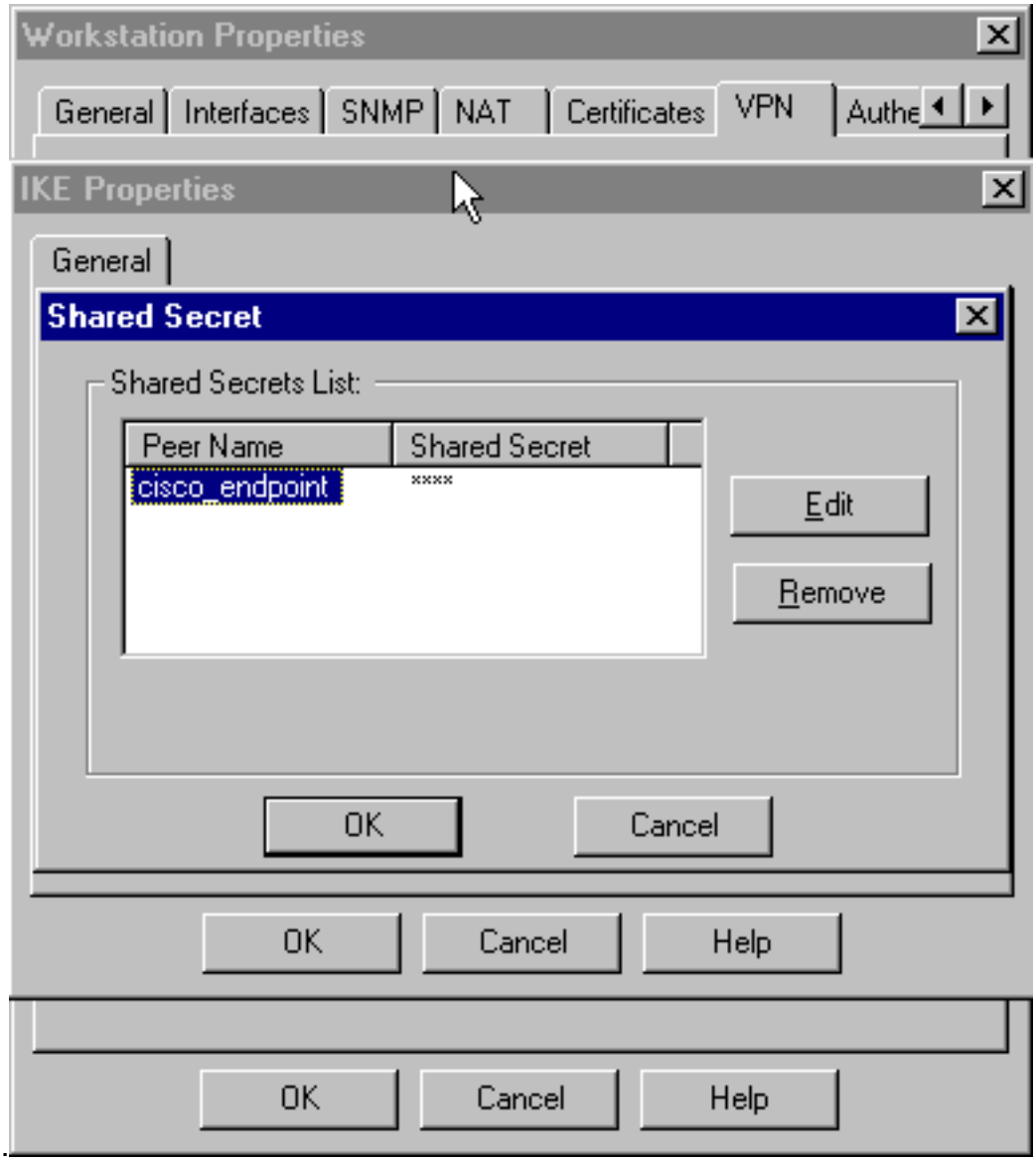
Bewerken.

7. Verander de IKE eigenschappen in **DES** encryptie en **SHA1** hashing om met de opdracht **SHA_DES_G2** VPN Concentrator akkoord te gaan.**Opmerking:** The "G2" verwijst naar Diffie-Hellman groep 1 of 2. Bij testen werd ontdekt dat het checkpoint ofwel "G2" ofwel "G1" accepteert.Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder



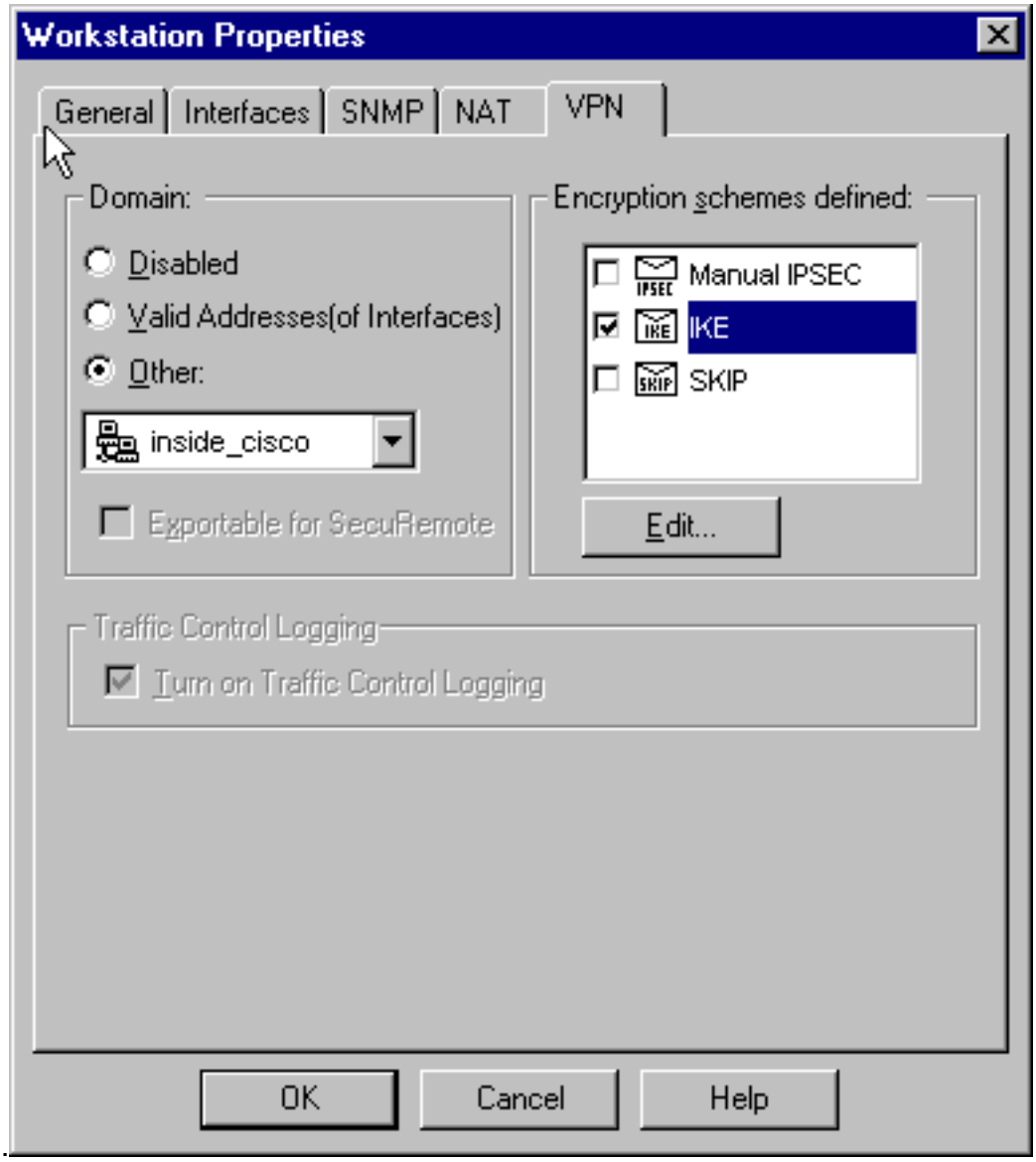
verificatiemethode.

8. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de **SharedKey = <key>**VPN Concentrator-opdracht akkoord te



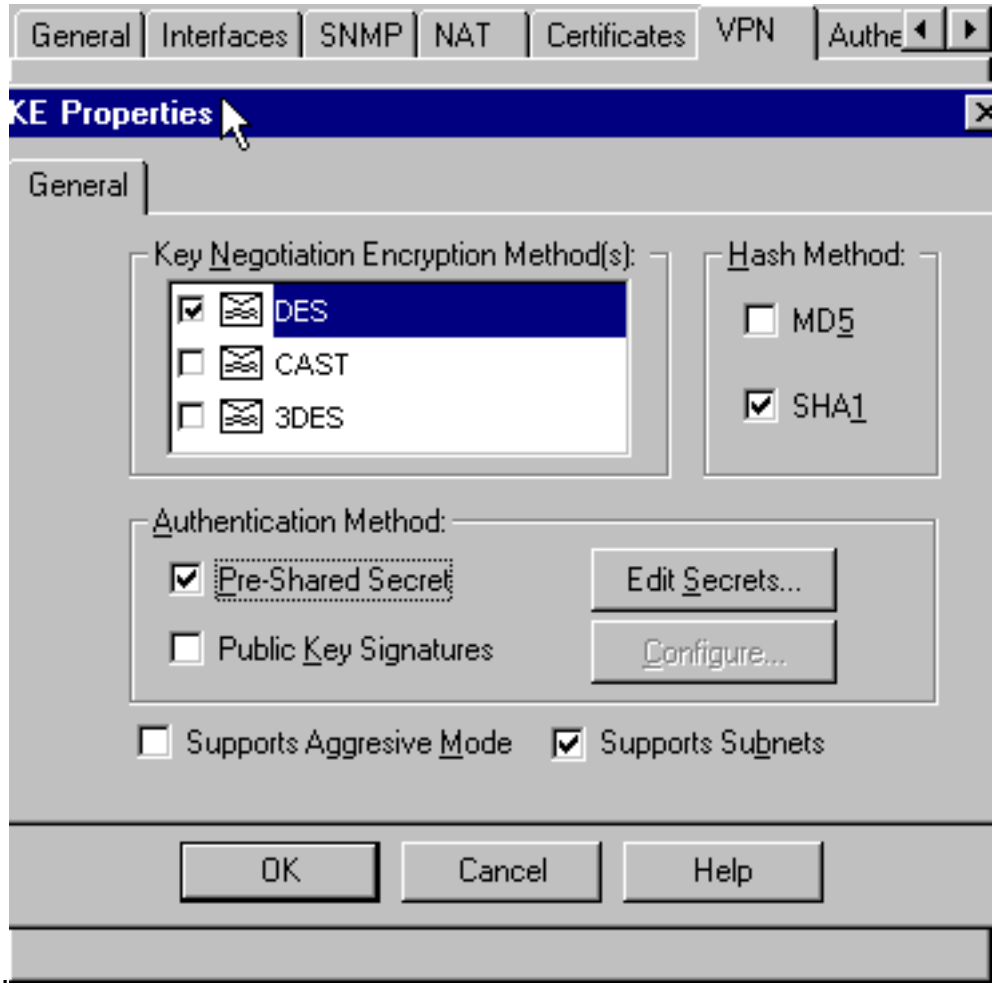
gaan.

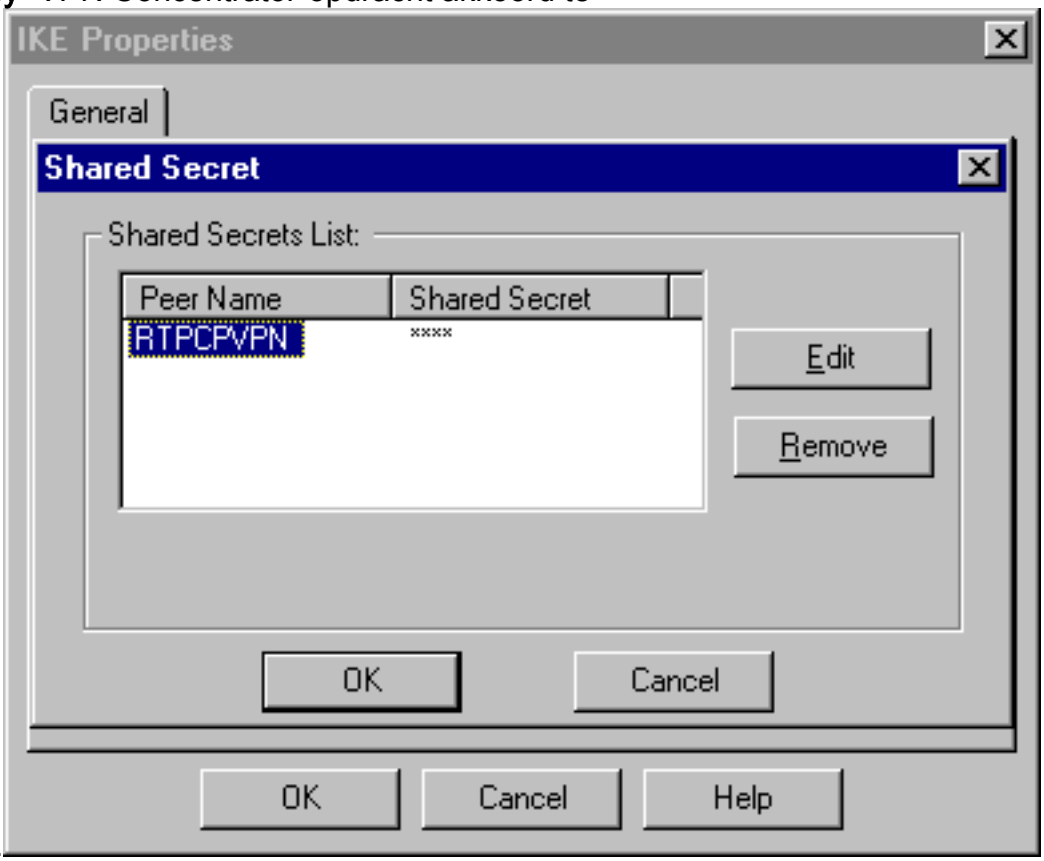
9. Selecteer **Manager > Netwerkobjecten > Bewerken** om het tabblad "cisco_end" VPN te bewerken. Selecteer onder Domain, **Andere**, en selecteer dan de binnenkant van het netwerk van de VPN Concentrator (genoemd "binnenkant_cisco"). Selecteer onder Encryption schemes die worden gedefinieerd **IKE** en klik vervolgens op



Bewerken.

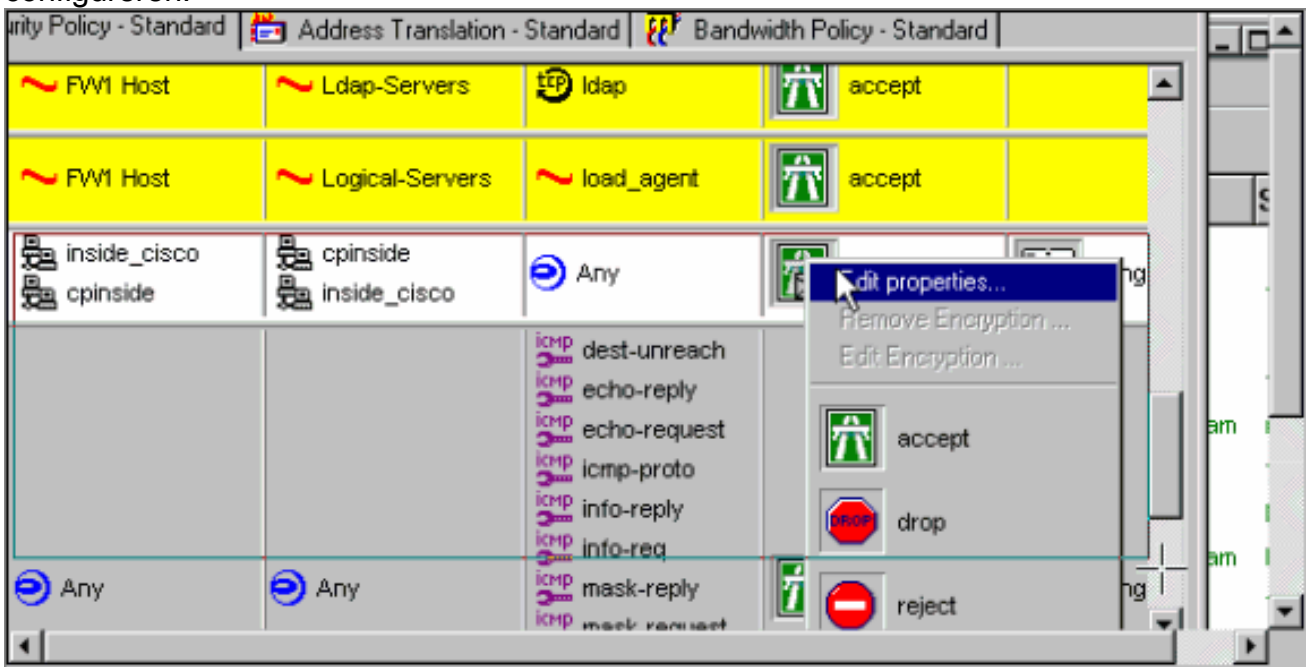
10. Verander de IKE eigenschappen in **DES** encryptie en **SHA1** hashing om met de opdracht **SHA_DES_G2** VPN Concentrator akkoord te gaan.**Opmerking:** The "G2" verwijst naar Diffie-Hellman groep 1 of 2. Bij testen bleek dat het checkpoint ofwel "G2" ofwel "G1" accepteert.Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder

verificatiemethode. 

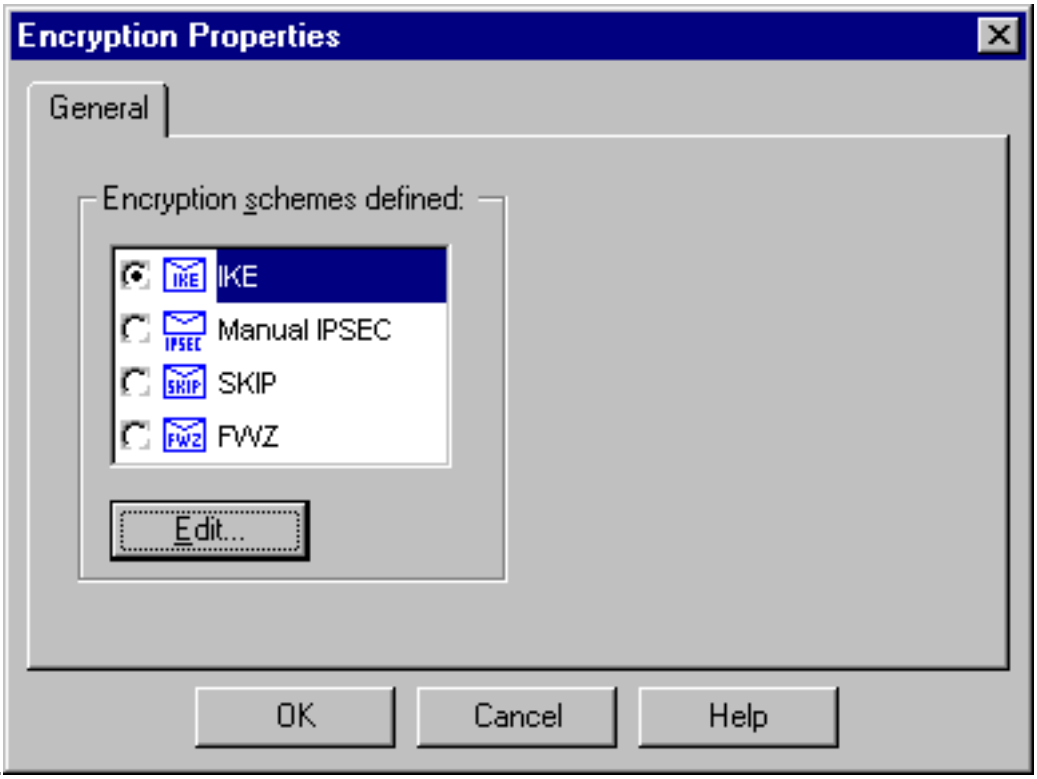
11. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de **SharedKey = <key>**VPN Concentrator-opdracht akkoord te gaan. 

12. Typ in het venster Policy Editor een regel met zowel Bron als Destination als "interne_cisco" en "cpinto" (bidirectioneel). **Service=Any** instellen, **Action=Encrypt** en **Track=Long**.

13. Klik onder het kopje Actie op het pictogram groene **versleuteling** en selecteer **Eigenschappen bewerken** om het coderingsbeleid te configureren.

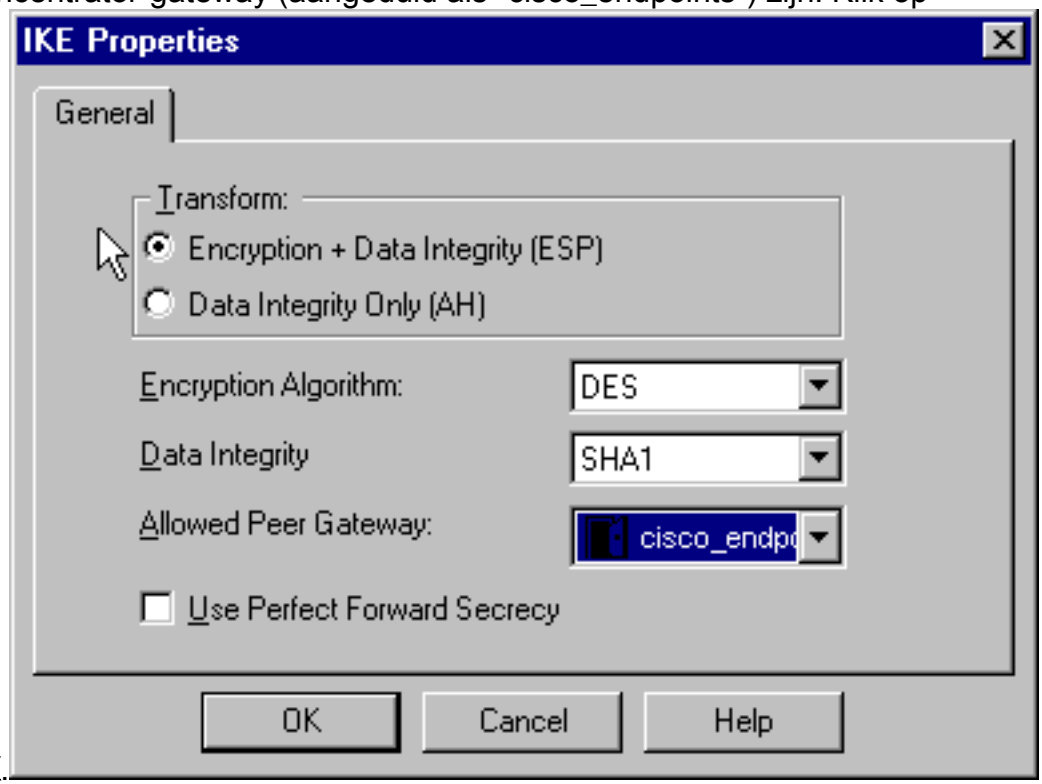


14. Selecteer **IKE** en klik op



Bewerken.

15. Wijzig deze eigenschappen in het venster IKE Properties om het **af** te stemmen met de opdracht **Transformer = SSP(sha,des)** VPN Concentrator.Selecteer onder Omzetten de optie **Encryption + Data Integrity (ESP)**. Het Encryption Algorithm moet **DES** zijn, de gegevensintegriteit moet **SHA1** zijn en de toegestane peer Gateway moet de externe VPN Concentrator-gateway (aangeduid als "cisco_endpoints") zijn. Klik op



OK.

16. Nadat u het selectieteken aanpast, selecteert u **Beleidsbeleid > Installatie** in het menu Selectieteken om de wijzigingen van kracht te laten worden.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Opdrachten voor VPN 5000 Concentrator probleemoplossing

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **vpn-scan-alles**-Geeft informatie over alle bijbehorende VPN-verbindingen, 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.
- **Geeft de systeemlogbuffer weer** — toont de inhoud van de interne logbuffer.
- **vpn statistieken tonen** - toont deze informatie voor gebruikers, partners, en het totaal voor beide. (Voor modulaire modellen bevat de weergave een gedeelte voor elke modulesleuf. Raadpleeg het gedeelte Uitvoer van monster.)`Huidige actieve`-de huidige actieve verbindingen.`In het niets`—de op dit moment onderhandelende verbindingen.`Hoog water`: het hoogste aantal gelijktijdige actieve verbindingen sinds de laatste herstart.`Totaal uitvoeren`: het totale aantal succesvolle verbindingen sinds de laatste herstart.`Tunnel OK` - Het aantal tunnels waarvoor geen fouten waren.`Tunnel start`—het aantal tunnels start.`Tunnelfout`-het aantal tunnels met fouten.
- **toon VPN statistiek breedband** - toont ISAKMP onderhandelingsstatistieken, en veel meer actieve verbindingsstatistieken.

Netwerksamenvatting

Wanneer meerdere aangrenzende interne netwerken zijn geconfigureerd in het encryptiedomein op het Selectieteken, kan het apparaat deze automatisch samenvatten met betrekking tot interessant verkeer. Als de VPN Concentrator niet is geconfigureerd om aan elkaar te koppelen, zal de tunnel waarschijnlijk falen. Als bijvoorbeeld de binnennetwerken van 10.0.0.0/24 en 10.0.1.0/24 zodanig zijn geconfigureerd dat ze in de tunnel worden opgenomen, kunnen ze worden samengevat tot 10.0.0.0/23.

Checkpoint 4.1 Firewall debug

Dit was een Microsoft Windows NT-installatie. Omdat de tracering `lang` is ingesteld in het venster Policy Editor (zoals weergegeven in Stap 12), moet het ontkende verkeer in het logvenster rood verschijnen. Meer breedaardige debug is te verkrijgen door:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

en in een ander venster:

```
C:\WINNT\FW1\4.1\fwstart
```

Geef deze opdrachten uit om de Security Associations (SA's) op de selectieteken te wissen:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

Antwoord **ja** op de `Zijn jullie zeker?` .

Voorbeeld van output van foutopsporing

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0
```

```
IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped              13
Unwrapped             9
BadEncap              0
BadAuth               0
BadEncrypt            0
rx IP                 9
rx IPX                0
rx Other              0
tx IP                13
tx IPX                0
tx Other              0
IKE rekey             0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
```

```
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
```

```
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0
```

Gerelateerde informatie

- Cisco VPN 5000 Series Concentrators end-of-sale aankondiging
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems