# Een IPSec-tunnels configureren tussen een Cisco Secure PIX-firewall en een checkpoint NG-firewall

## Inhoud



# Inleiding

Dit document toont aan hoe u een IPsec-tunnel met pre-gedeelde sleutels kunt configureren om tussen twee particuliere netwerken te communiceren. In dit voorbeeld zijn de communicerende netwerken het 192.168.10.x privé-netwerk binnen de Cisco Secure PIX-firewall en het 10.32.x.x privé-netwerk binnen CheckpointTM Next Generation (NG)-firewall.

# Voorwaarden

## Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- verkeer van binnen de PIX en binnen het checkpointTM naar het internet (hier weergegeven door de 172.18.124.x-netwerken) moet plaatsvinden voordat u deze configuratie start.
- Gebruikers moeten bekend zijn met de onderhandeling over IPsec. Dit proces kan in vijf stappen worden opgesplitst, waaronder twee IKE-fasen (Internet Key Exchange).Een IPsec-

tunnel wordt geïnitieerd door interessant verkeer. Het verkeer wordt als interessant beschouwd wanneer het tussen de IPsec-peers reist.In IKE Fase 1 onderhandelen de IPsec-peers over het vastgestelde beleid van de IKE Security Association (SA). Zodra de peers echt zijn bevonden, wordt er een beveiligde tunnel aangemaakt met behulp van Internet Security Association en Key Management Protocol (ISAKMP).In IKE Fase 2, gebruiken de IPsec peers de geauthenticeerde en veilige tunnel om IPsec SA transformaties te onderhandelen. De onderhandelingen over het gedeelde beleid bepalen hoe de IPsec-tunnel tot stand wordt gebracht.De IPsec-tunnel wordt gecreëerd en er worden gegevens tussen de IPsec-peers overgebracht, op basis van de IPsec-parameters die zijn ingesteld in de transformatiesets van IPsec.De IPsec-tunnel eindigt wanneer de IPsec SA's worden verwijderd of wanneer hun levensduur verlopen.

## Gebruikte componenten

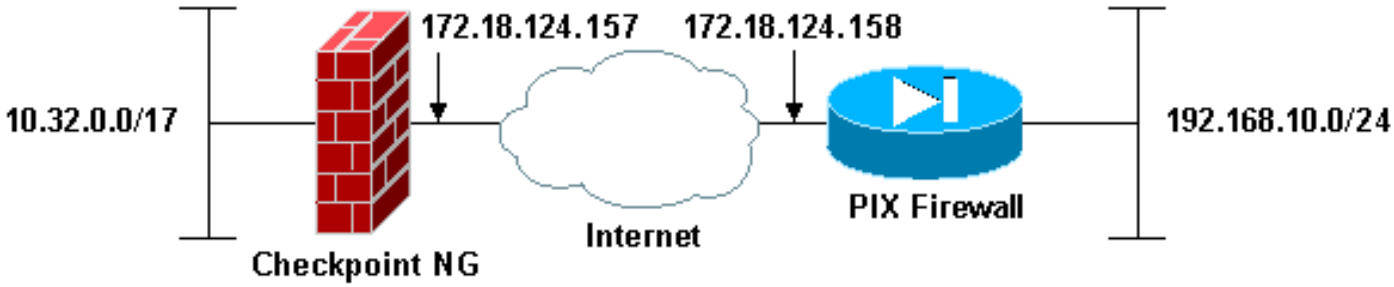
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-softwarerelease 6.2.1
- CheckpointTM-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.

## Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:




## Conventies

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

# PIX configureren

In deze sectie wordt u voorzien van de informatie om de functies te configureren die in dit document worden beschreven.

| PIX-configuratie |
| --- |
| `PIX Version 6.2(1)` |

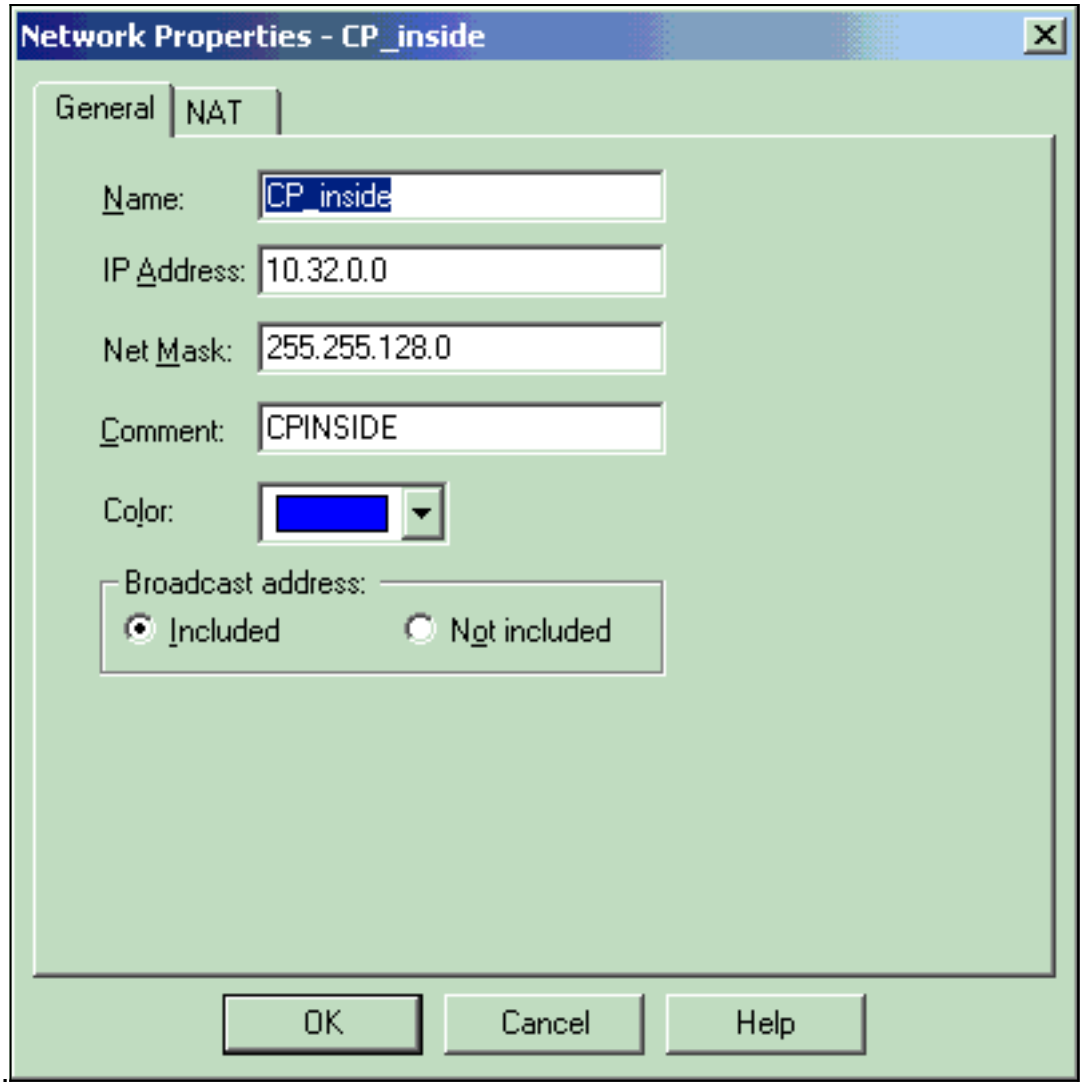
```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIXRTPVPN
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
!--- Interesting traffic to be encrypted to the
Checkpoint™ NG. access-list 101 permit ip 192.168.10.0
255.255.255.0 10.32.0.0 255.255.128.0
!--- Do not perform Network Address Translation (NAT) on
traffic to the Checkpoint™ NG. access-list nonat permit
ip 192.168.10.0 255.255.255.0 10.32.0.0 255.255.128.0
pager lines 24
interface ethernet0 10baset
interface ethernet1 10full
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.158 255.255.255.0
ip address inside 192.168.10.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
!--- Do not perform NAT on traffic to the Checkpoint™
NG. nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.1 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
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Permit all inbound IPsec authenticated cipher
sessions. sysopt connection permit-ipsec
no sysopt route dnat
!--- Defines IPsec encryption and authentication
algorithms. crypto ipsec transform-set rtptac esp-3des
esp-md5-hmac
!--- Defines crypto map. crypto map rtprules 10 ipsec-
isakmp
crypto map rtprules 10 match address 101
crypto map rtprules 10 set peer 172.18.124.157
crypto map rtprules 10 set transform-set rtptac
```

```
!--- Apply crypto map on the outside interface. crypto
map rtprules interface outside
isakmp enable outside
!--- Defines pre-shared secret used for IKE
authentication. isakmp key ******** address
172.18.124.157 netmask 255.255.255.255
!--- Defines ISAKMP policy. isakmp policy 1
authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:089b038c8e0dbc38d8ce5ca72cf920a5
: end
```

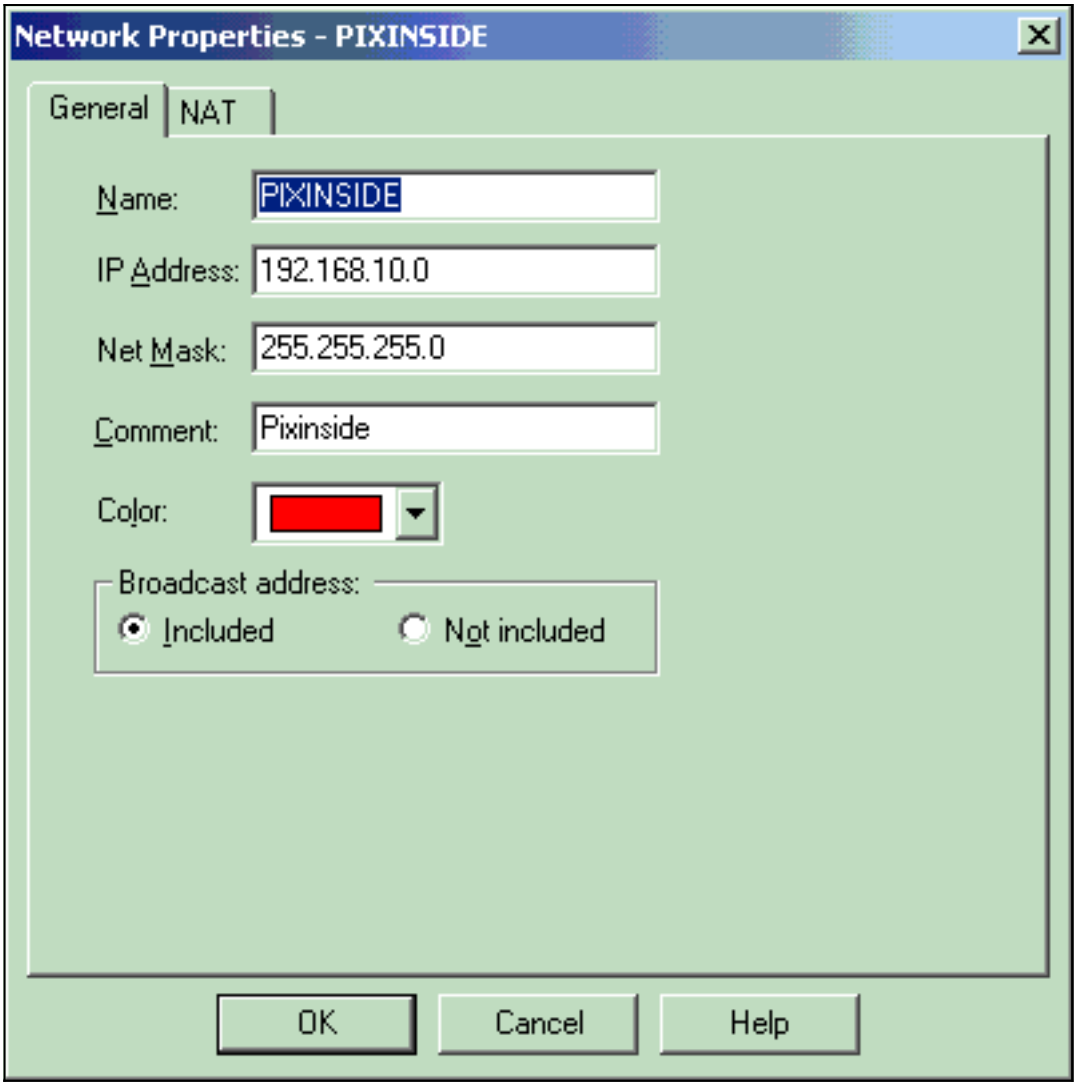
## Het selectieteken configureren

De objecten en regels van het netwerk worden op CheckpointTM NG gedefinieerd om het beleid op te stellen dat betrekking heeft op de te instellen VPN-configuratie. Dit beleid wordt vervolgens geïnstalleerd met behulp van de editor van checkpointTM om de glanskant van de configuratie te voltooien.

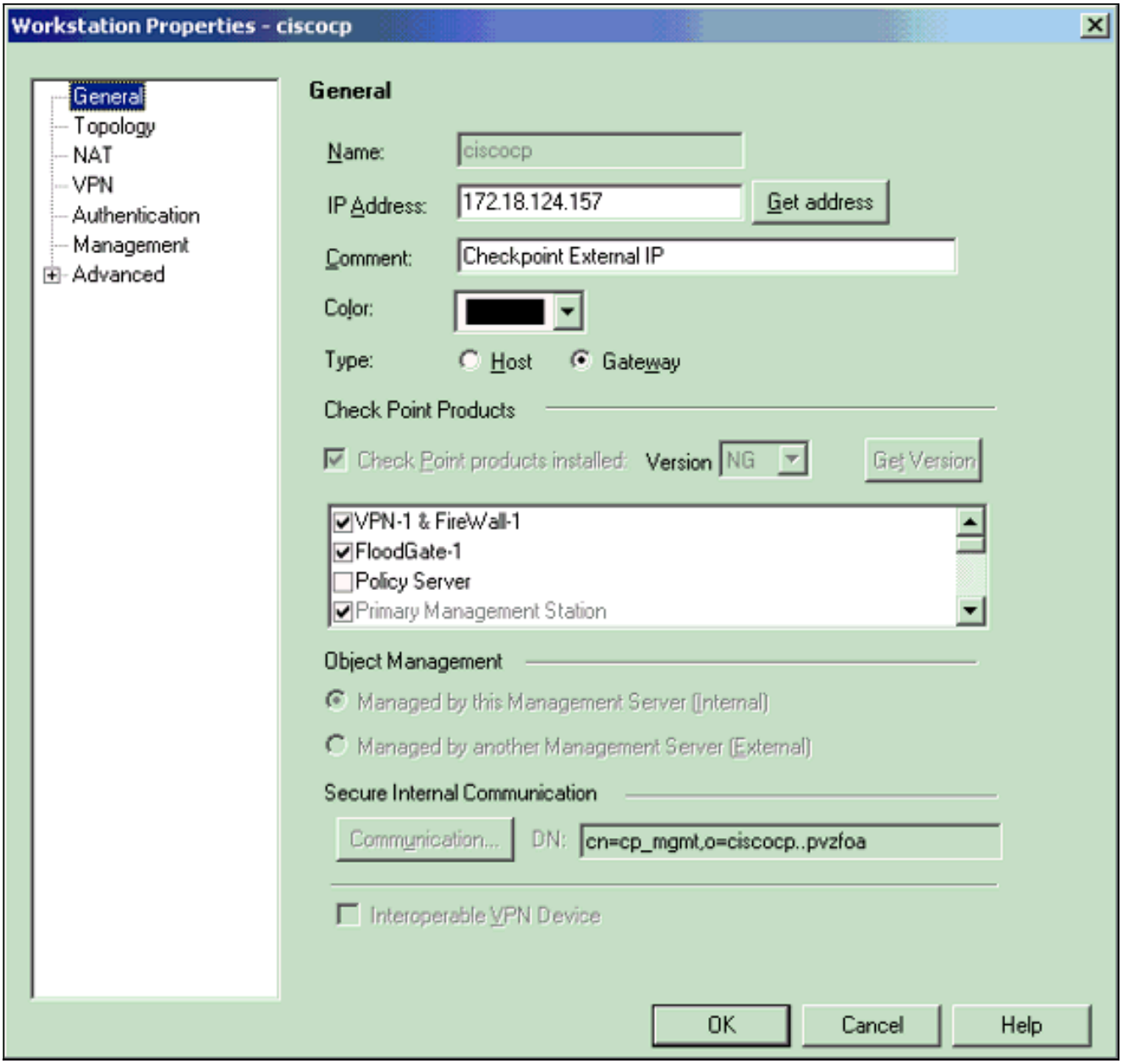
1. Maak de twee netwerkobjecten voor het netwerk van het Selectietwerk en het netwerk van de PIX-firewall die het interessante verkeer versleutelen.Om dit te doen, selecteert u **Bewerken > Netwerkobjecten** en vervolgens selecteert u **Nieuw > Netwerk**. Voer de juiste netwerkinformatie in en klik vervolgens op **OK**.Deze voorbeelden tonen een set van netwerkobjecten CP_Inside (binnen netwerk van CheckpointTM NG) en PIXINSIDE (binnen netwerk van

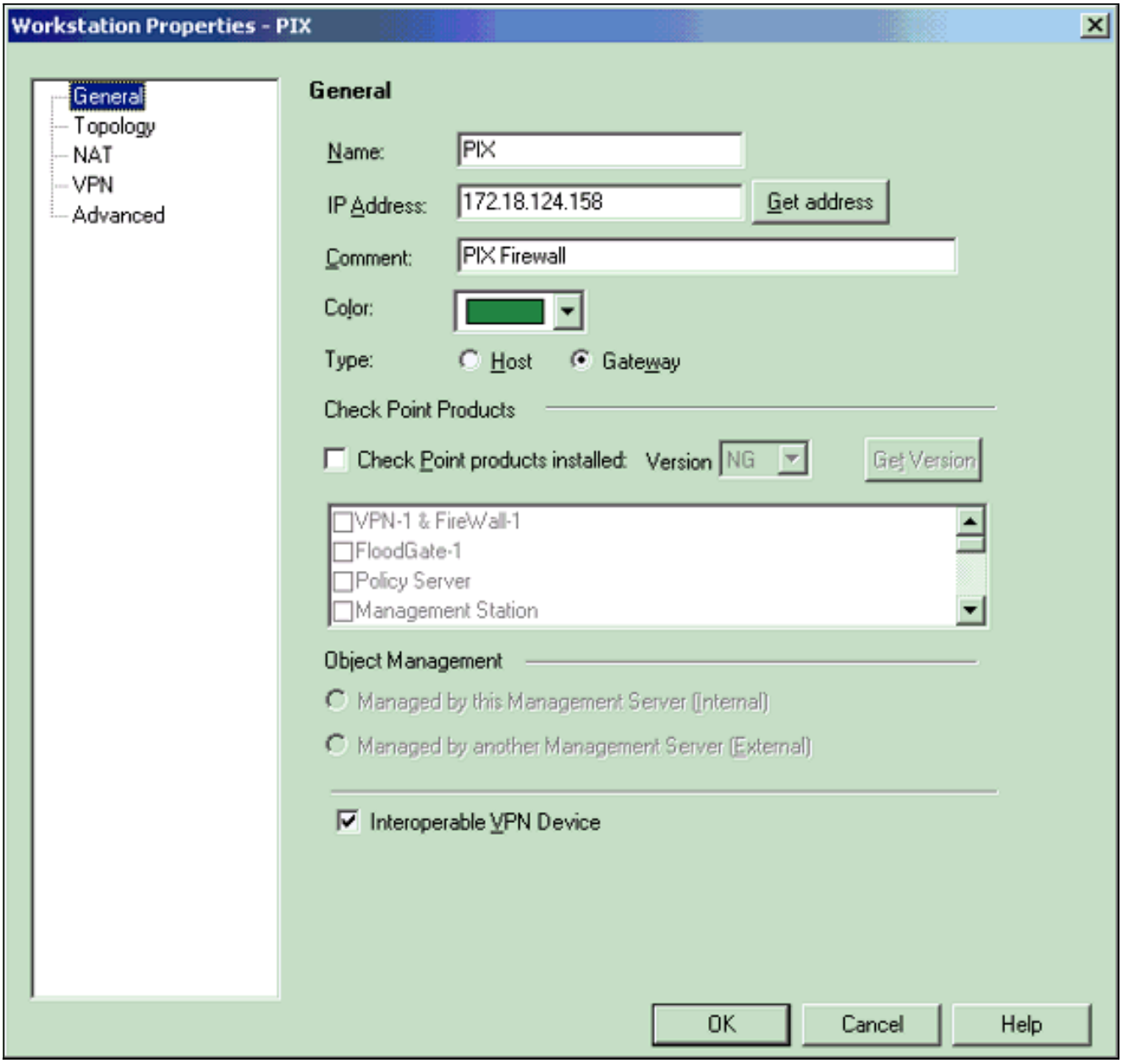

Network Properties - CP_inside
General
NAT
Name:
CP_inside
IP Address:
10.32.0.0
Net Mask:
255.255.128.0
Comment:
CPINSIDE
Color:
Broadcast address:
Included
Not included
OK
Cancel
Help

PIX).

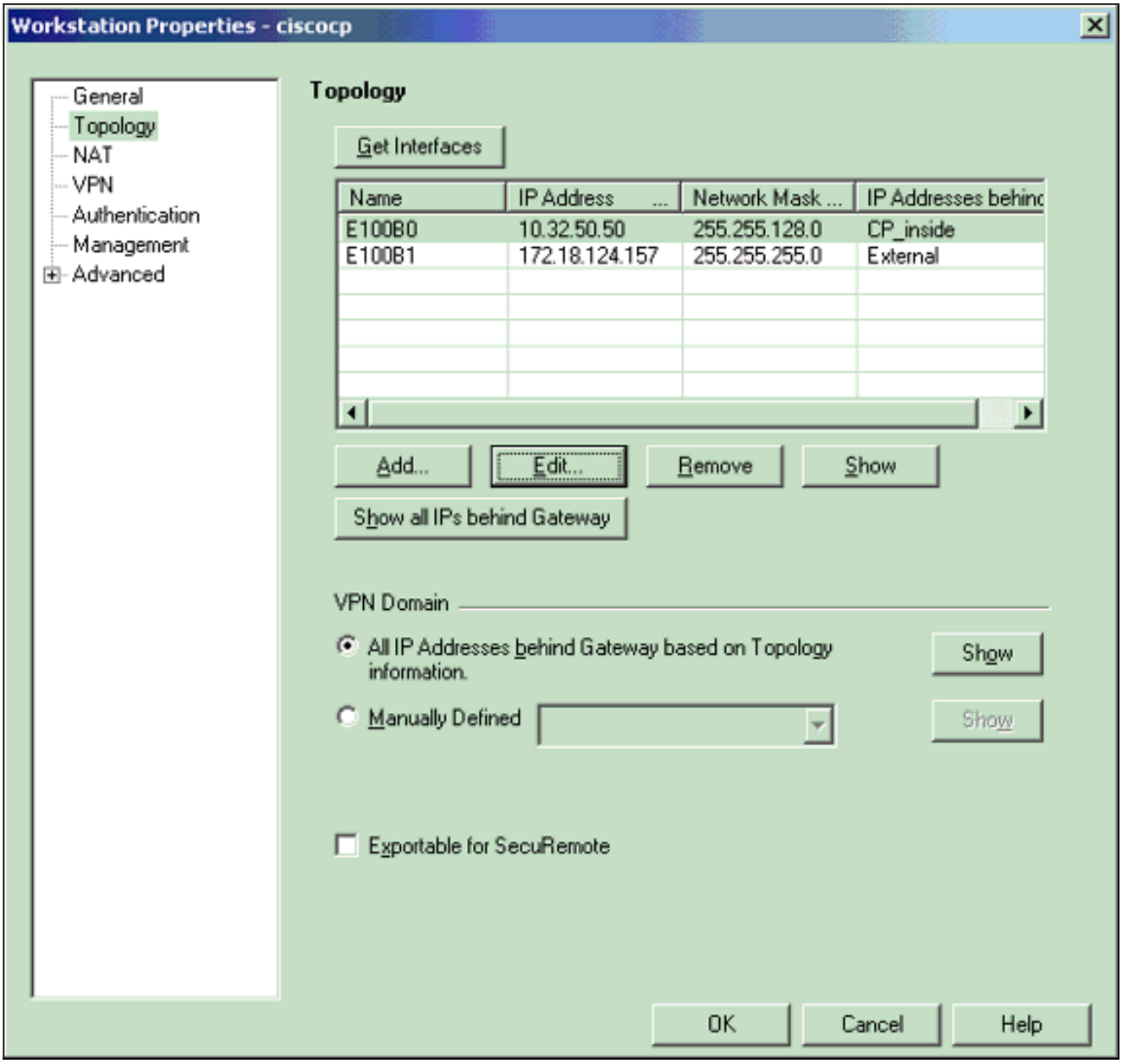



2. Maak werkstationobjecten voor CheckpointTM NG en PIX. Om dit te doen, selecteert u **Bewerken > Netwerkobjecten > Nieuw > Werkstation**.Let op dat u het object CheckpointTM NG-werkstation kunt gebruiken dat is gemaakt tijdens de eerste checkpointTM-instelling. Selecteer de opties om het werkstation in te stellen als Gateway en Interoperable VPN-apparaat en klik vervolgens op **OK**.Deze voorbeelden tonen een verzameling objecten, ciscoop (**CheckpointTM** NG) en PIX (PIX Firewall).

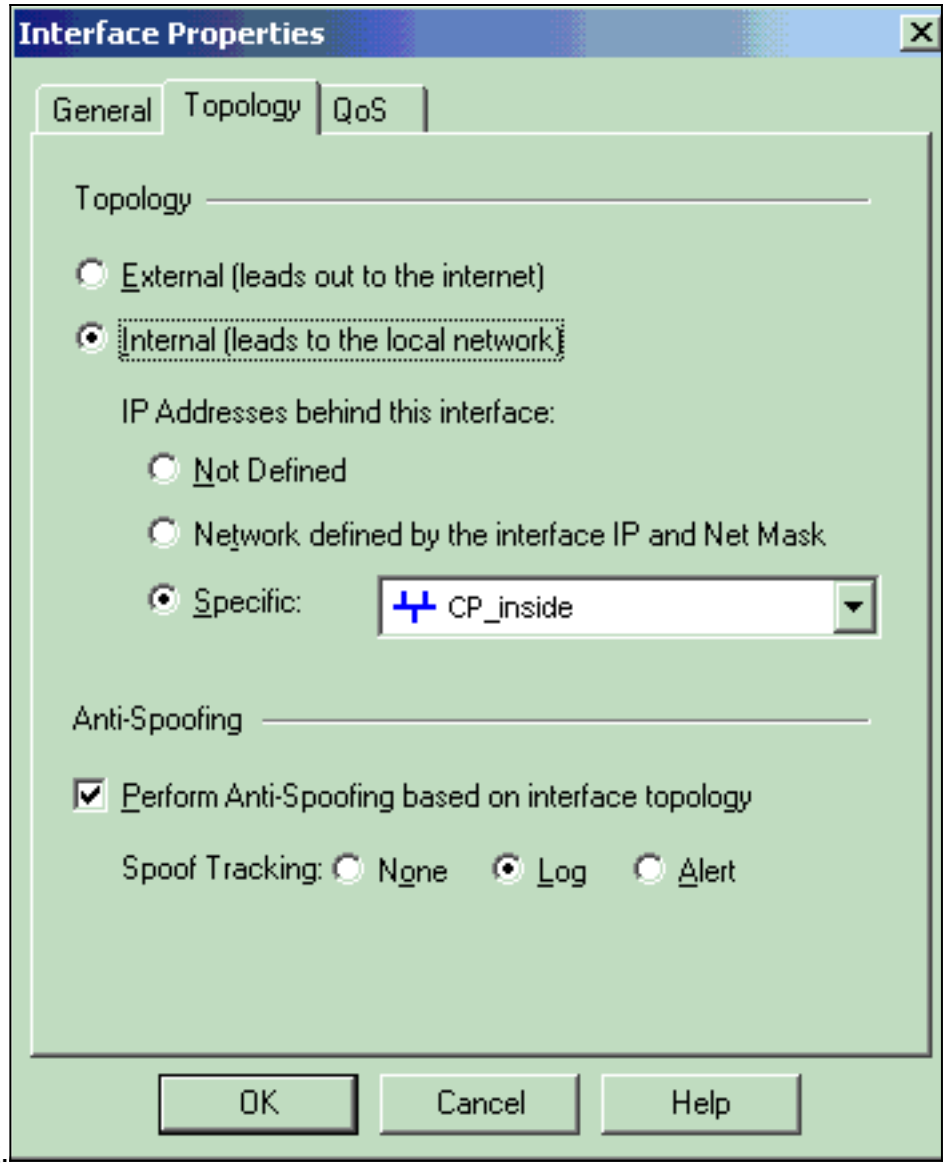

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help




3. Selecteer **Bewerken > Netwerkobjecten > Bewerken** om het venster Workstation Properties te openen voor CheckpointTM NG-werkstation (ciscop in dit voorbeeld).Selecteer **Topologie** uit de keuzes aan de linkerkant van het venster en selecteer vervolgens het netwerk dat moet worden versleuteld. Klik op **Bewerken** om de interfaceeigenschappen in te stellen.

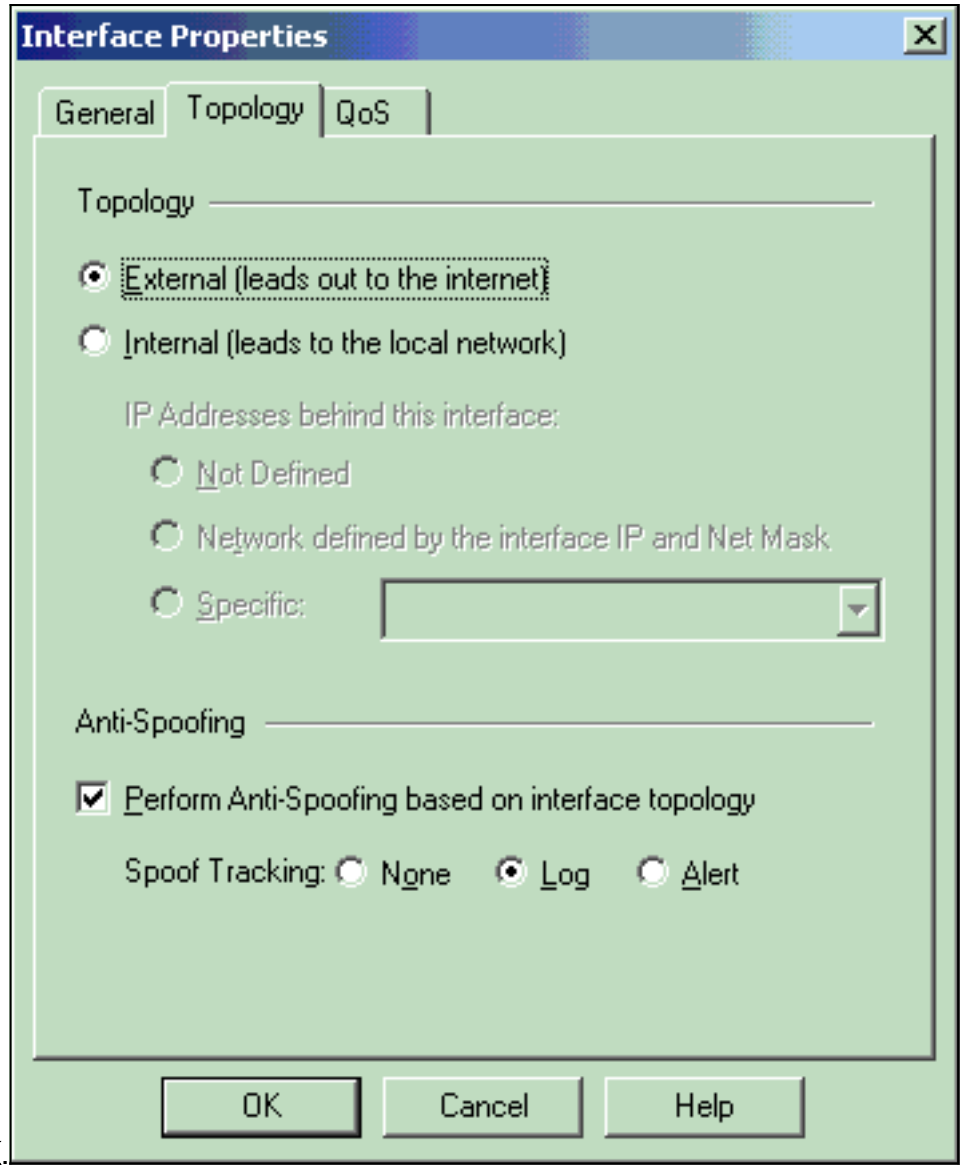



4. Selecteer de optie om het werkstation als intern aan te wijzen en geef vervolgens het juiste IP-adres op. Klik op **OK**.In deze configuratie is CP_interne het interne netwerk van CheckpointTM NG. De topologie selectie wordt hier getoond wijst het werkstation aan als intern en specificeer het adres als



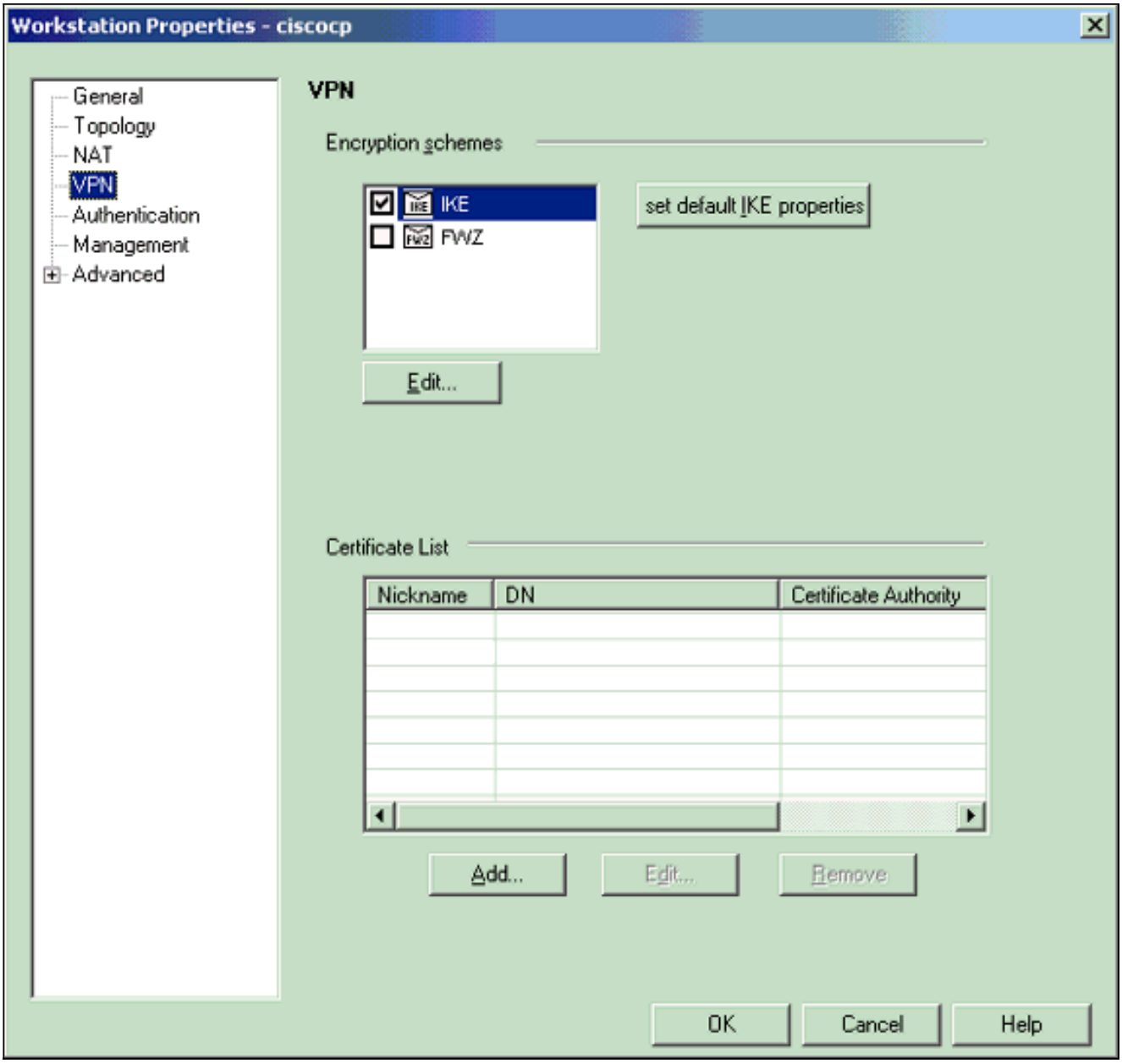

CP_binnenkant.

5. Selecteer in het venster Werkstations Properties de externe interface van de CheckpointTM NG die naar het internet leidt en klik vervolgens op **Bewerken** om de interfaceeigenschappen in te stellen. Selecteer de optie om de topologie als extern aan te wijzen, dan klik op

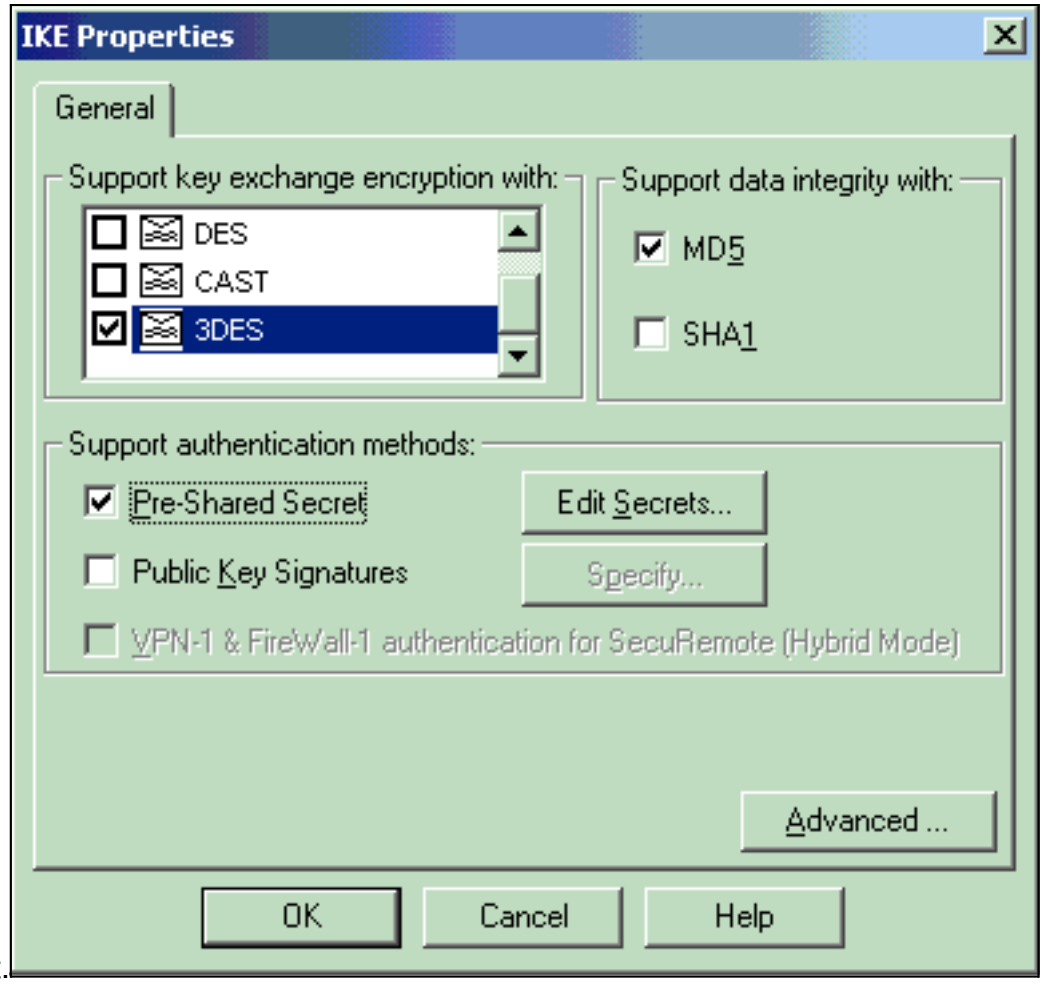



**OK**.

6. Selecteer vanuit het venster Workstation Properties op CheckpointTM NG **VPN** van de keuzes aan de linkerkant van het venster en selecteer vervolgens IKE-parameters voor encryptie en authenticatie algoritmen. Klik op **Bewerken** om de IKE-eigenschappen te configureren.

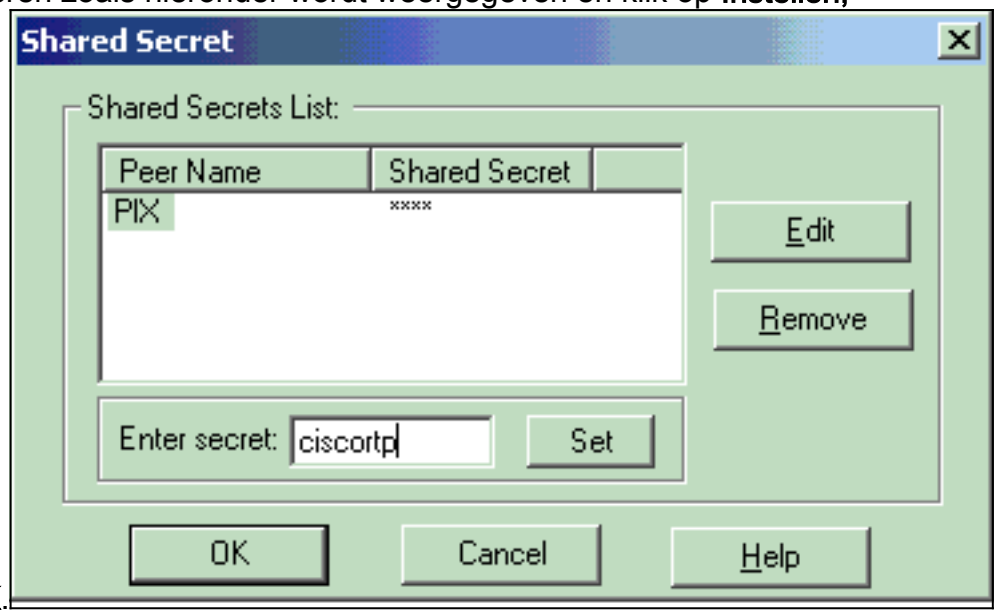



7. Configuratie van de IKE-eigenschappen:Selecteer de optie voor **3DES**-encryptie zodat de IKE-eigenschappen compatibel zijn met de opdracht **isakmp-beleid # encryptie 3des**.Selecteer de optie voor **MD5** zodat de IKE-eigenschappen compatibel zijn met het **crypto-**isakmp-**beleid # hash md5**



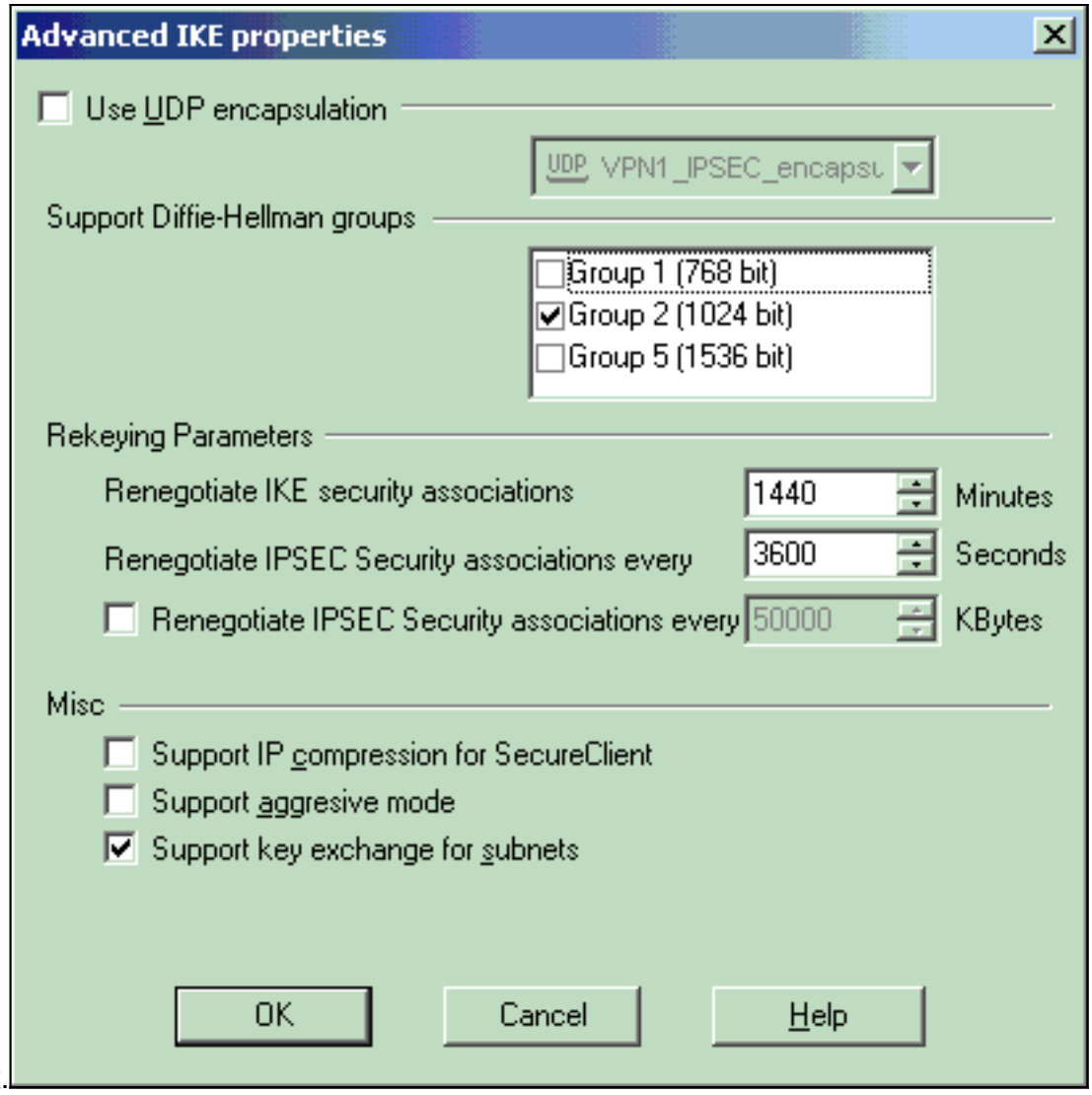

opdracht.

8. Selecteer de authenticatieoptie voor **Vooraf gedeelde geheimen** en klik vervolgens op **Geheimen bewerken** om de voorgedeelde sleutel in te stellen die compatibel is met het PIX-opdracht **ISakmp *key* adres *adres* netmask netmask.** Klik op **Bewerken** om de toets in te voeren zoals hieronder wordt weergegeven en klik op **Instellen,**



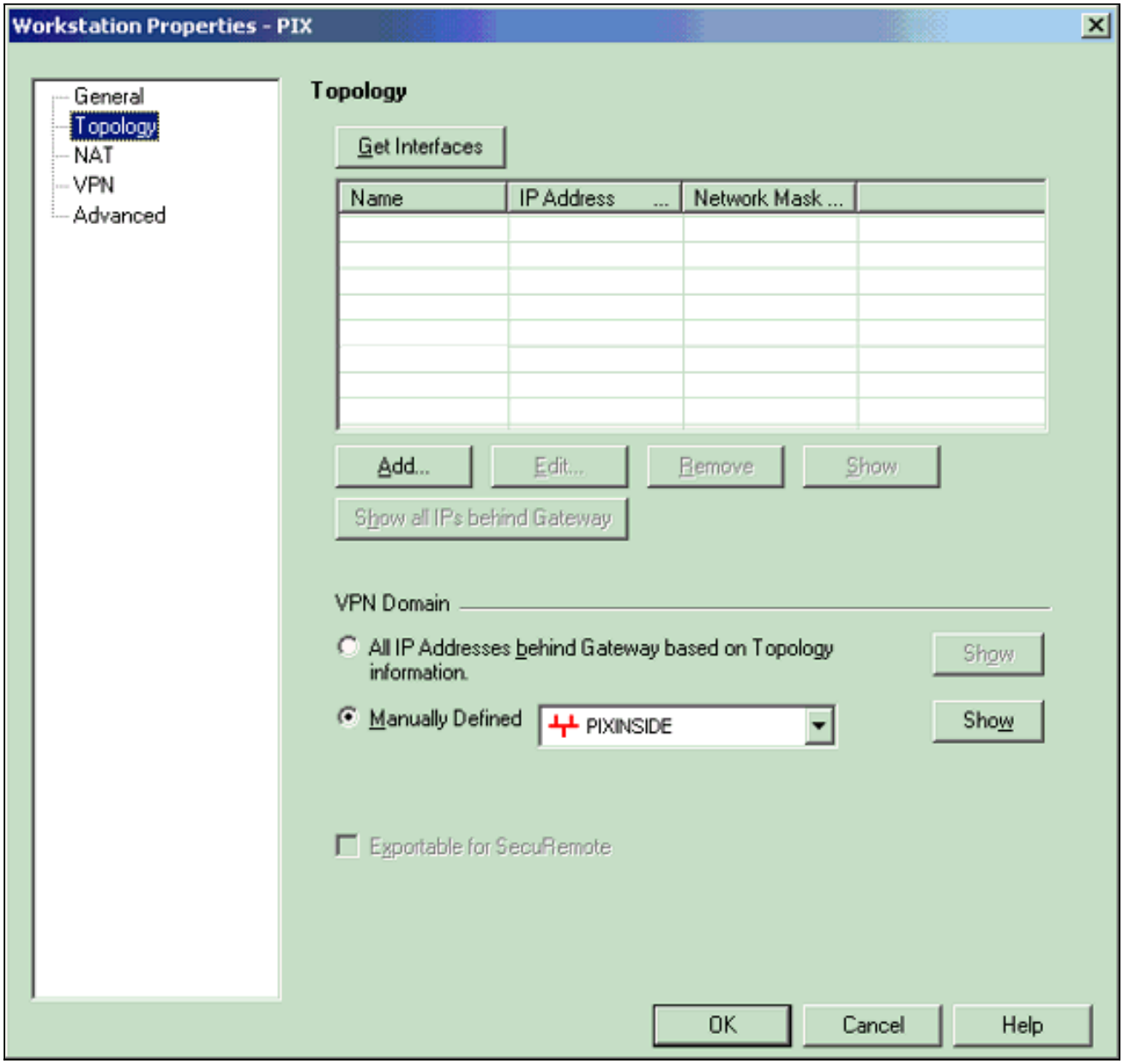

**OK**.

9. Klik in het venster IKE-eigenschappen op **Geavanceerd...** en wijzig deze instellingen:Deselecteer de optie voor **Support agressief modus**.Selecteer de optie voor de **Support-toets voor subnetten**.Klik op **OK** wanneer u klaar

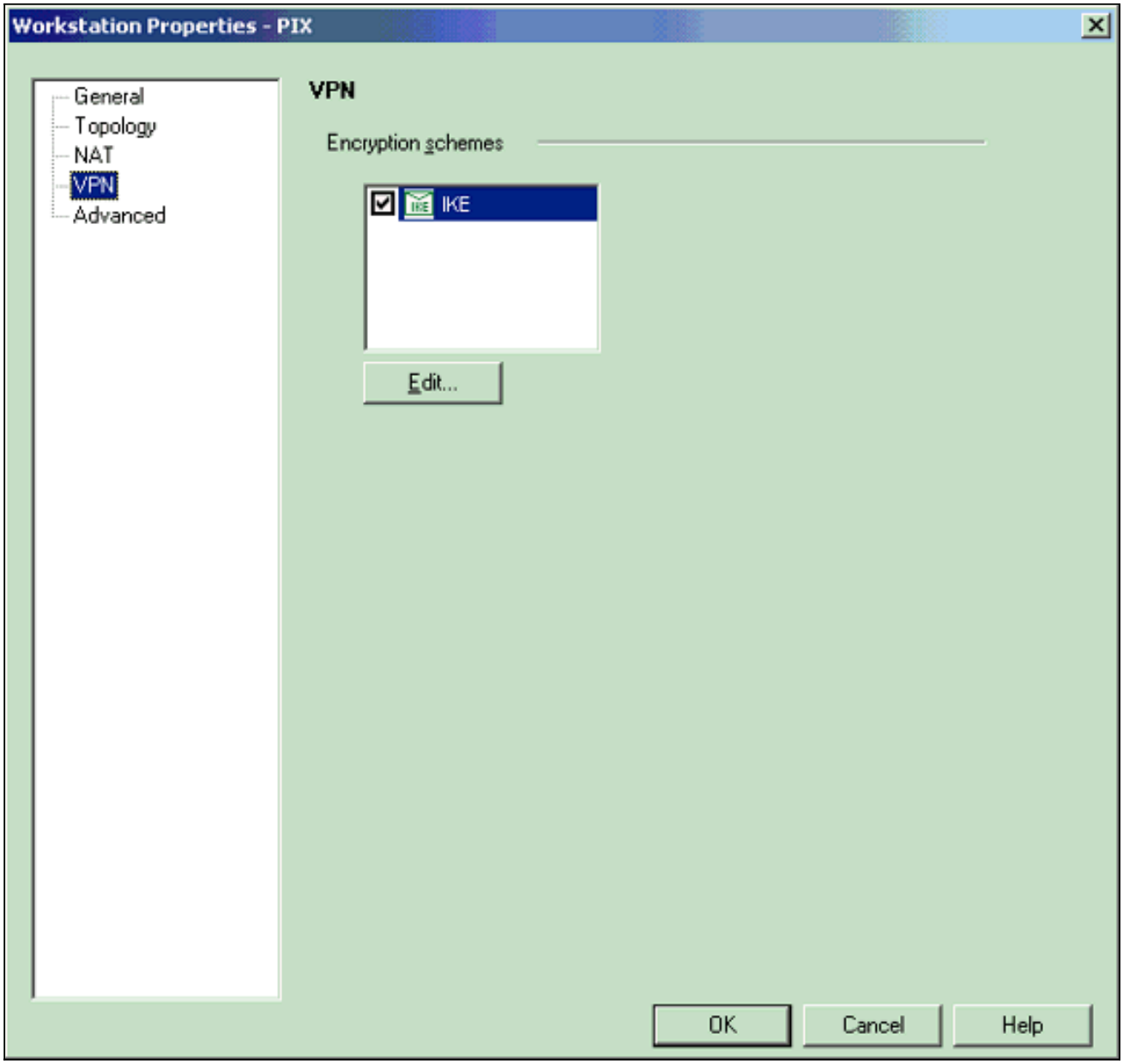


bent.

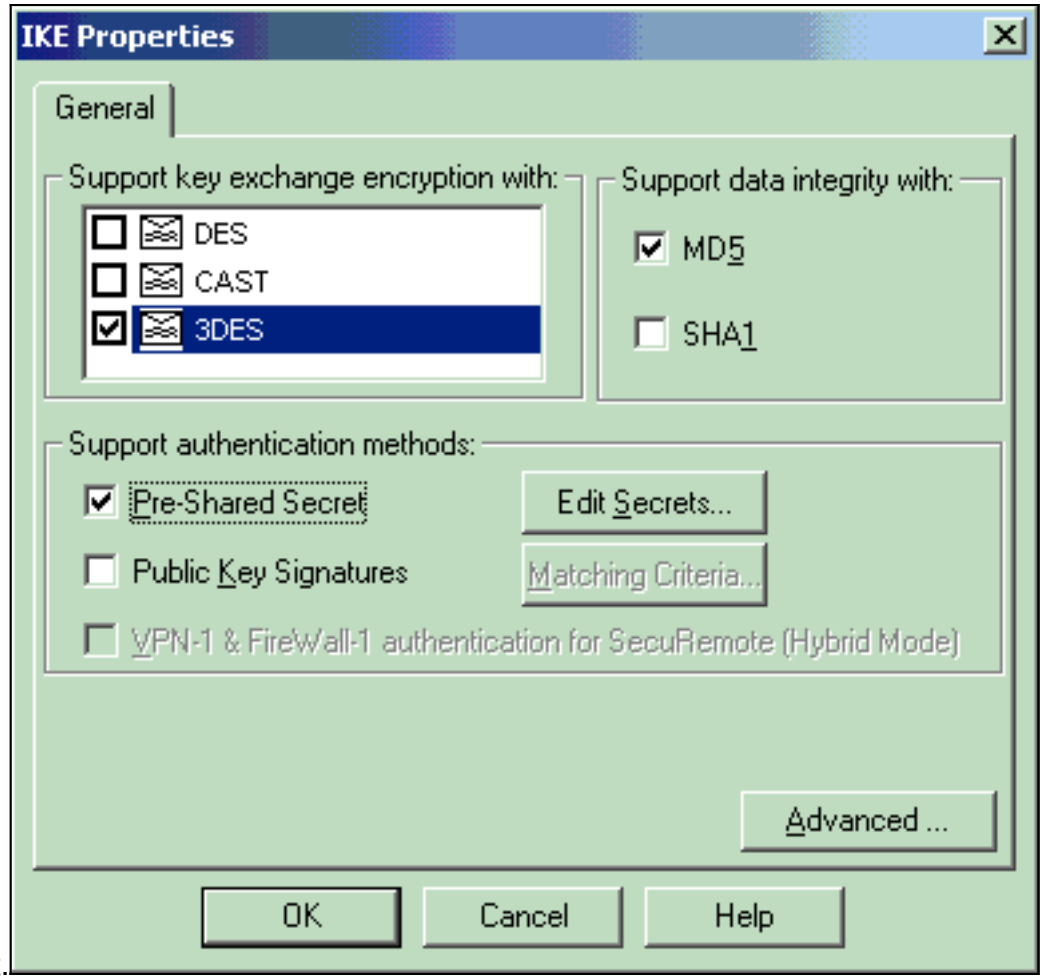
10. Selecteer **Manager** > **Netwerkobjecten** > **Bewerken** om het venster Werkstationeigenschappen voor de PIX te openen. Selecteer **Topologie** uit de keuzes aan de linkerkant van het venster om het VPN-domein handmatig te definiëren.In deze configuratie wordt PIXINSIDE (binnen netwerk van PIX) gedefinieerd als het VPN-domein.




11. Selecteer **VPN** vanuit de bestandsindelingen aan de linkerkant van het venster en selecteer IKE als coderingsschema. Klik op **Bewerken** om de IKE-eigenschappen te configureren.

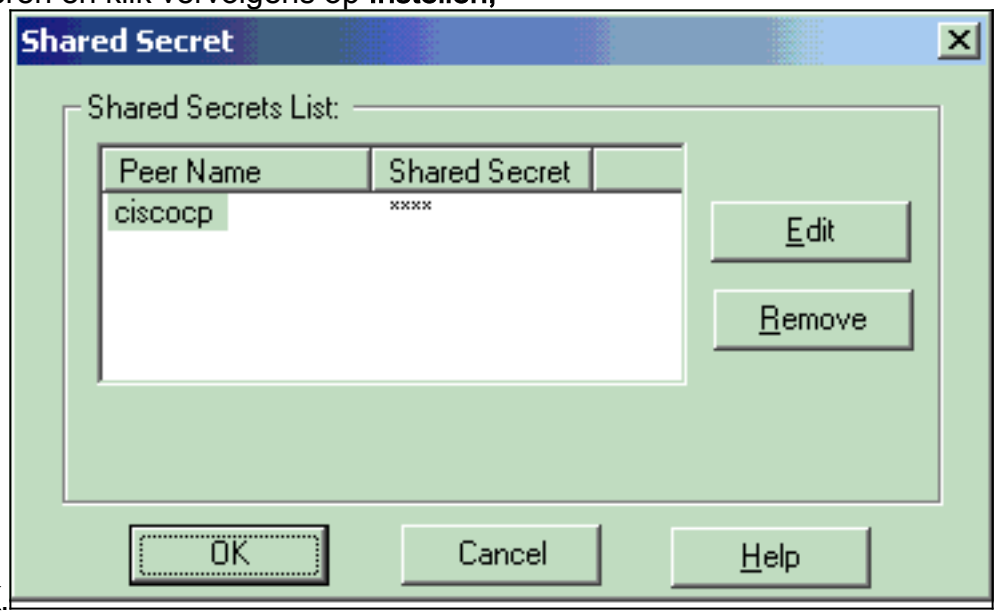



12. Configureer de IKE-eigenschappen zoals hier wordt getoond:Selecteer de optie voor **3DES**-encryptie zodat de IKE-eigenschappen compatibel zijn met de opdracht **isakmp-beleid # encryptie 3des**.Selecteer de optie voor **MD5** zodat de IKE-eigenschappen compatibel zijn met het **crypto-**isakmp-**beleid # hash md5**



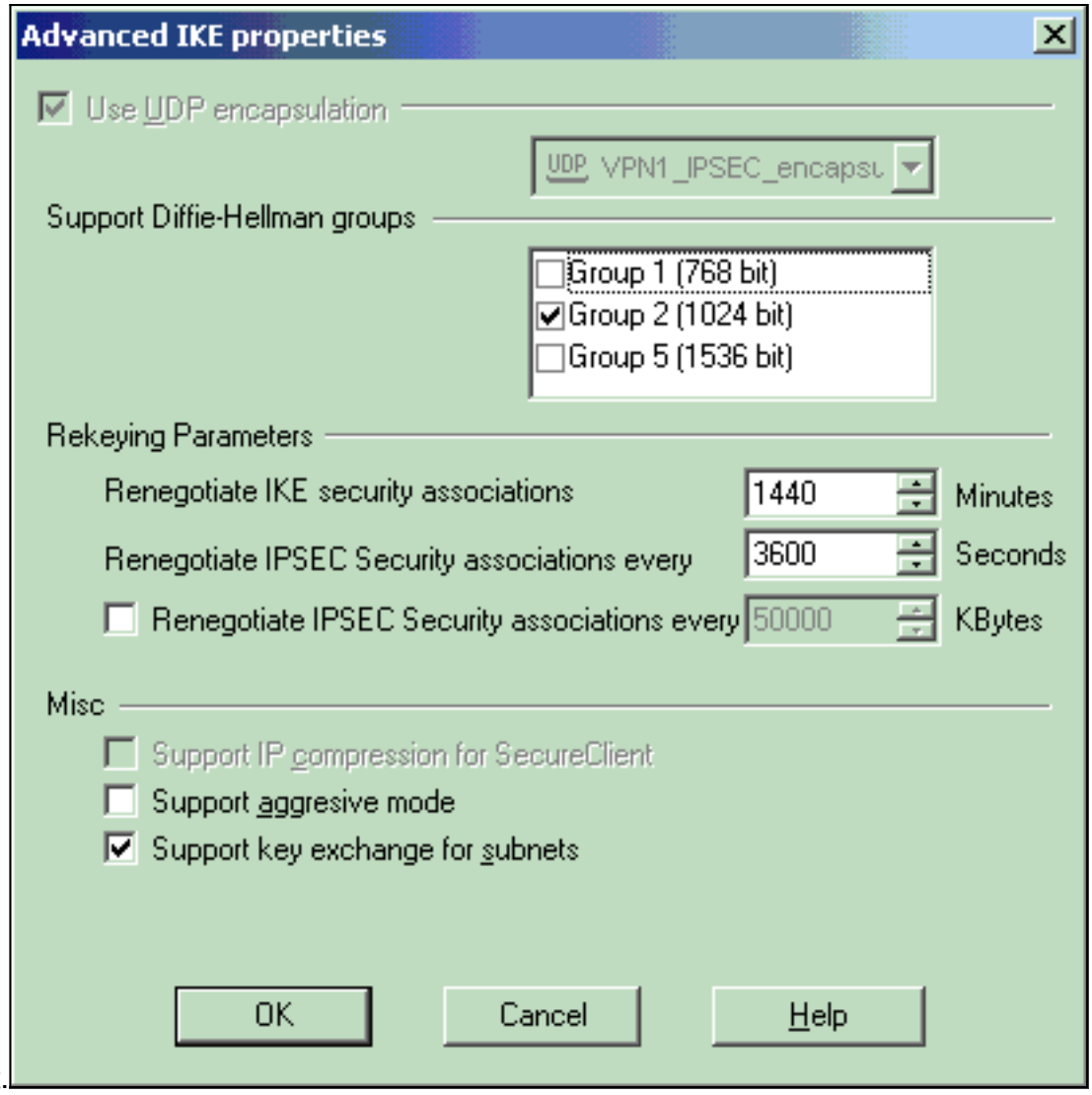

opdracht.

13. Selecteer de authenticatieoptie voor **Vooraf gedeelde geheimen** en klik vervolgens op **Geheimen bewerken** om de voorgedeelde sleutel in te stellen die compatibel is met het PIX-opdracht **isakmp key *address* netmask adresmasker.** Klik op **Bewerken** om de toets in te voeren en klik vervolgens op **Instellen,**



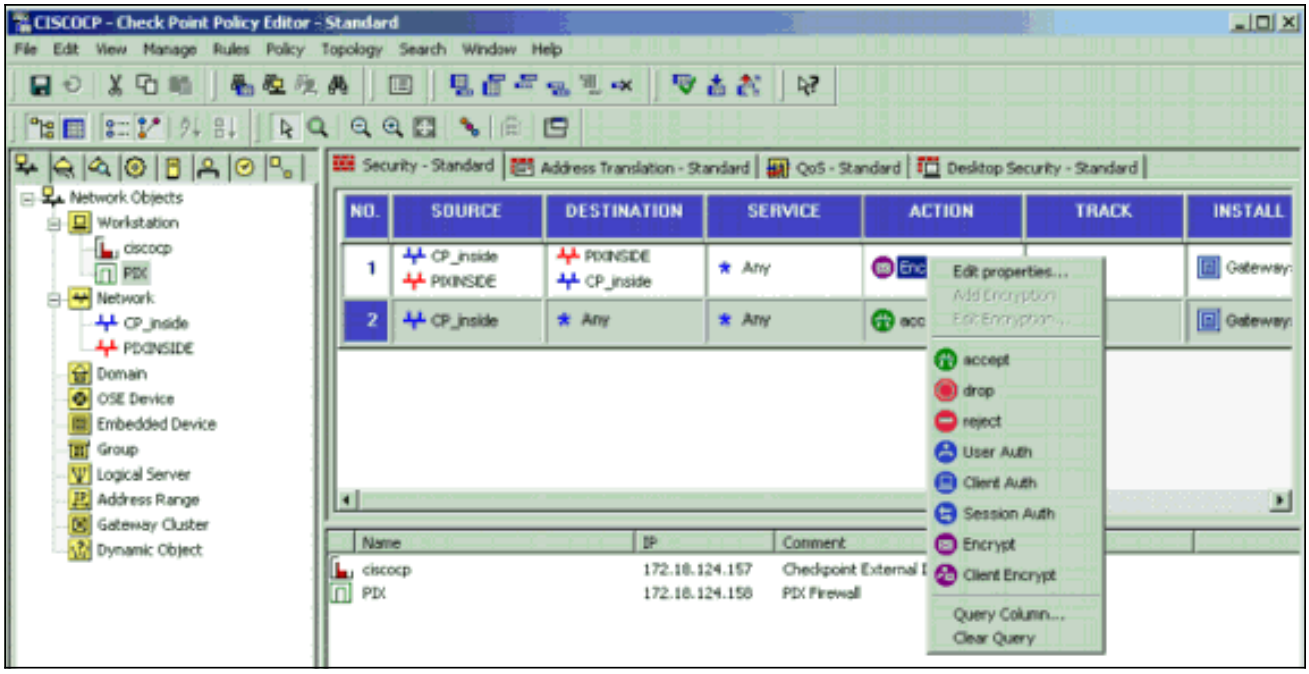

**OK**.

14. Klik in het venster IKE-eigenschappen op **Geavanceerd...** en verander deze instellingen.Selecteer de groep Diffie-Hellman die geschikt is voor IKE-eigenschappen.Deselecteer de optie voor **Support agressief modus**.Selecteer de optie voor de **Support-toets voor subnetten**.Klik op **OK, OK** als u klaar

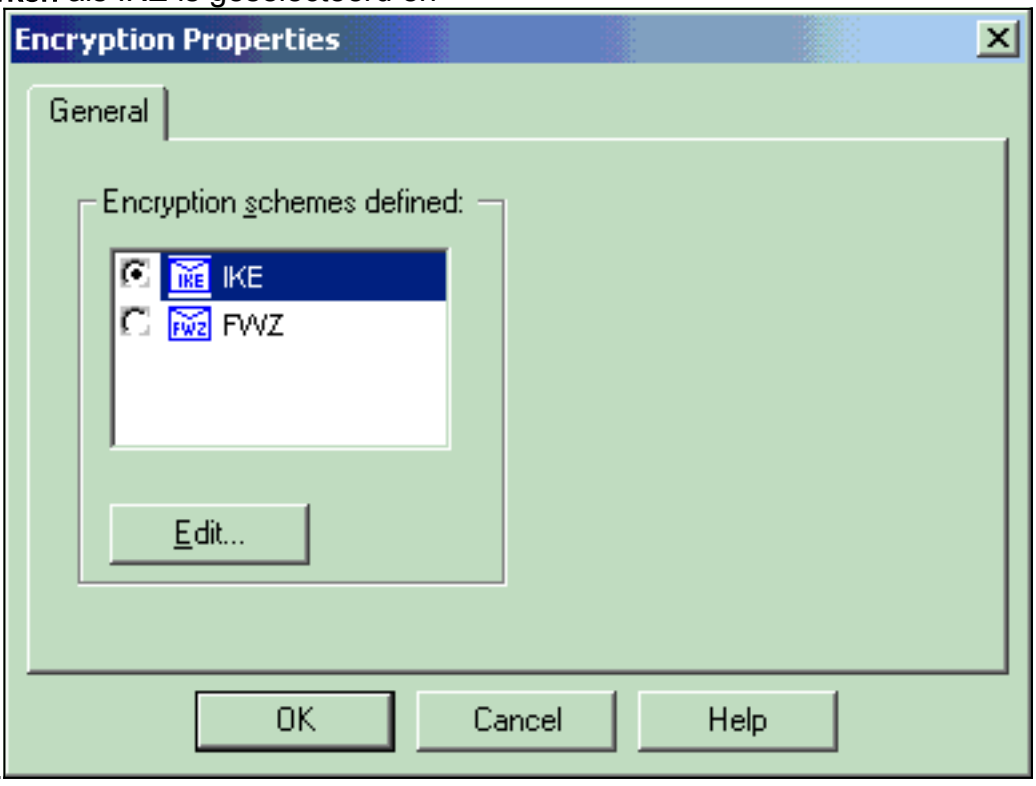



bent.

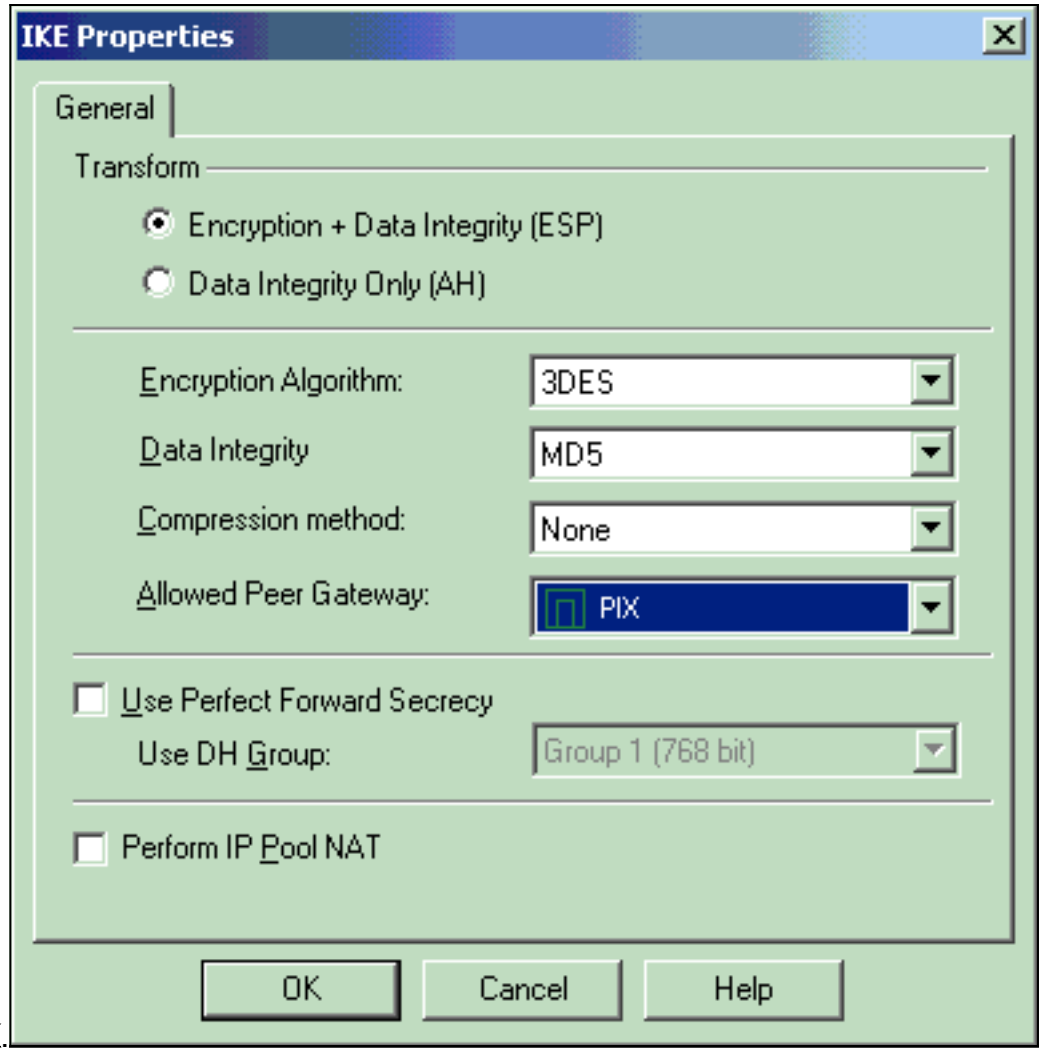
15. Selecteer **Regels** > **Regels** toevoegen > **Boven** om de coderingsregels voor het beleid te configureren.Plaats in het venster Policy Editor een regel met een bron van CP_interne (binnen netwerk van het checkpoint ™ NG) en PIXINSIDE (binnen netwerk van de PIX) op zowel de bron- als de doelkolommen. Stel waarden voor **Service = Any**, **Actie = Encrypt** en **Track = Log in**. Wanneer u het gedeelte Encrypt Action van de regel hebt toegevoegd, klikt u met de rechtermuisknop op **Actie** en vervolgens selecteert u **Eigenschappen bewerken**.




16. Klik op **Bewerken** als IKE is geselecteerd en geselecteerd.

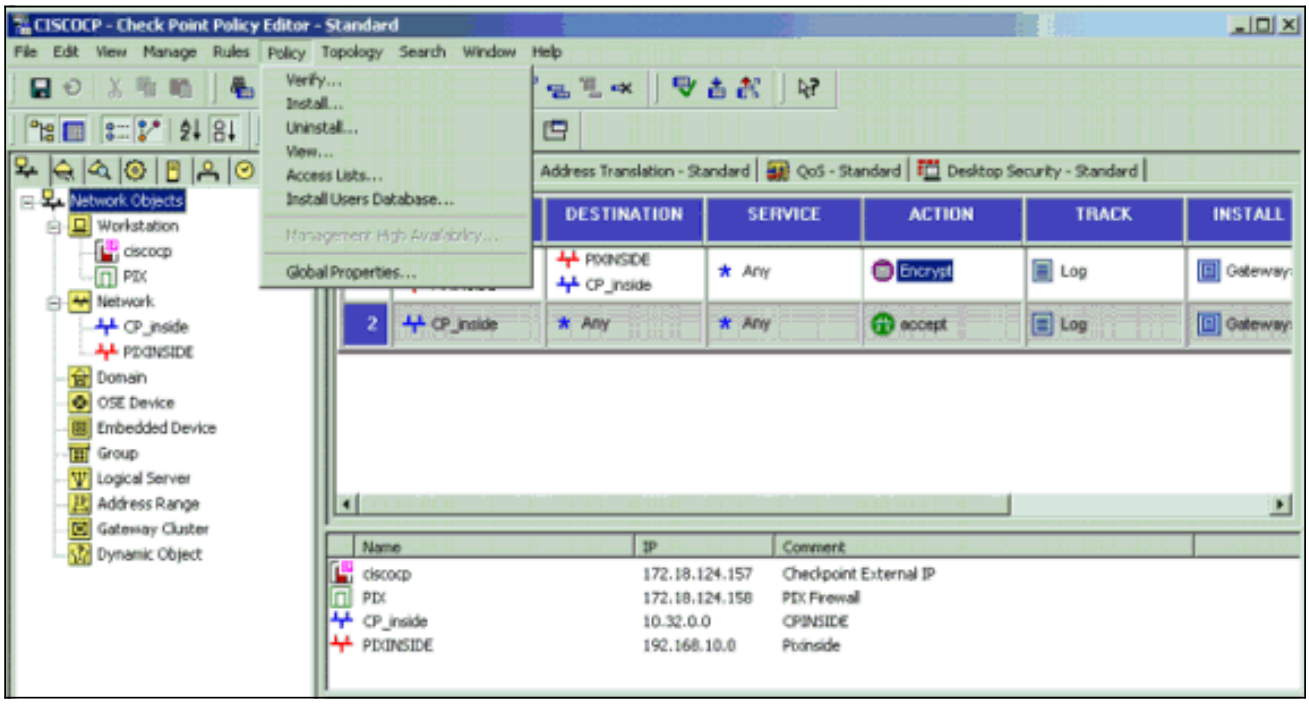



17. Wijzig in het venster IKE Properties de eigenschappen om in te stemmen met de PIX IPsec transformaties in de **crypto ipsec transformatie-set rtptac esp-3des esp-md5-hmac** opdracht.Stel de optie Omzetten in op **Encryption + Data Integrity (ESP)**, stel Encryption Algorithm in op **3DES**, stel Data Integrity in op **MD5** en stel de toegestane Peer Gateway in om de externe PIX-gateway (hier PIX genoemd) te benaderen. Klik op

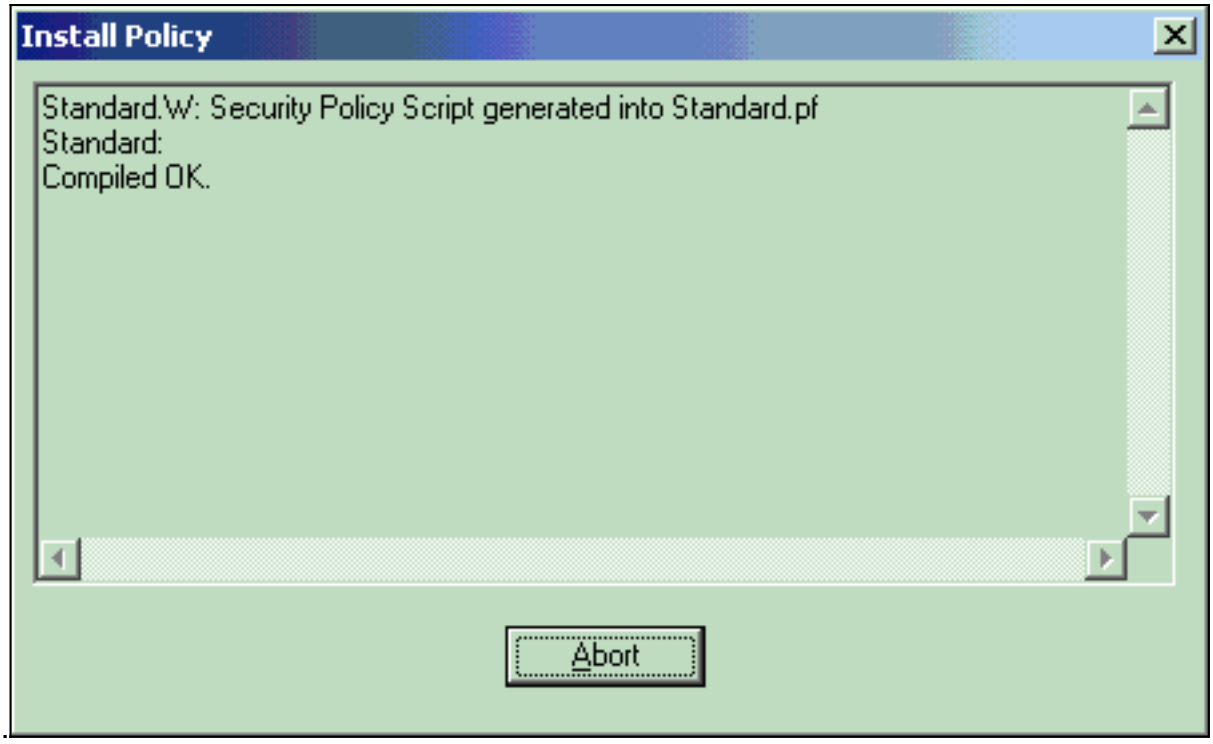



**OK**.

18. Nadat u het checkpointTM hebt ingesteld, slaat u het beleid op en selecteert u **Beleidsbeleid** > **Installeer** om het **kinderslot** in te schakelen.

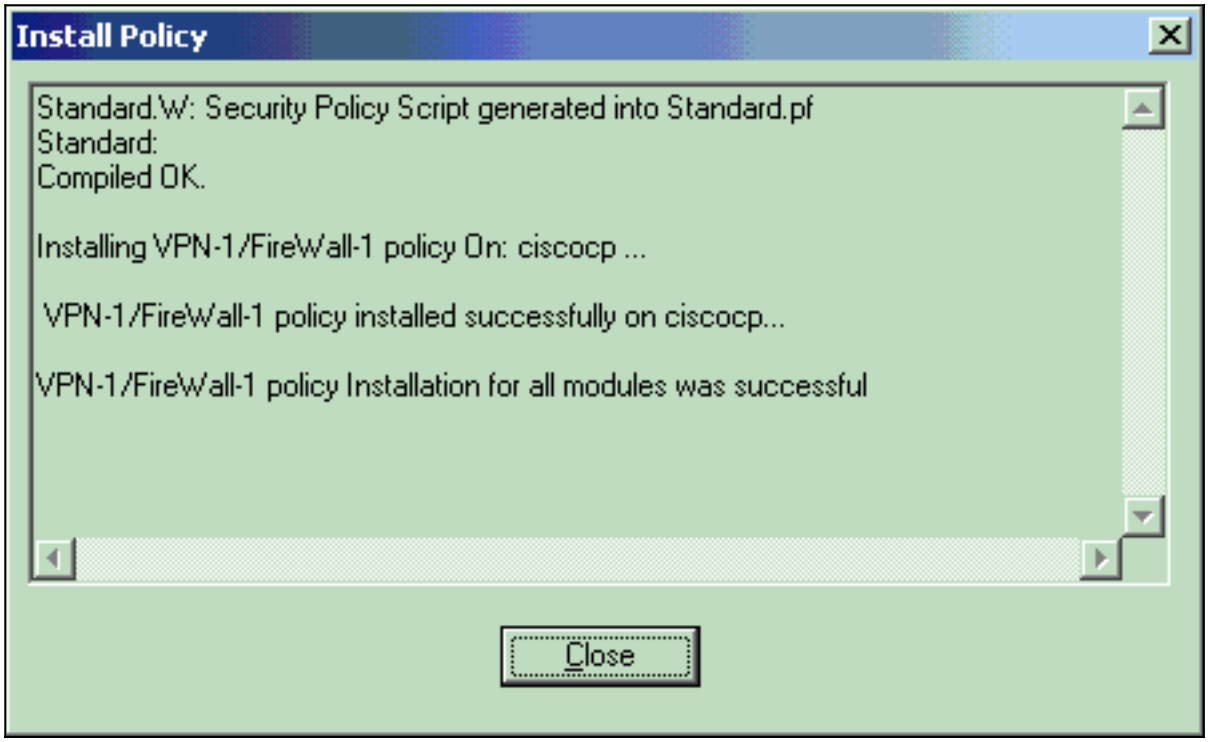



Het installatievenster toont voortgangsnoten bij het samenstellen van het




beleid.

Wanneer het installatievenster aangeeft dat de beleidsinstallatie is voltooid. Klik op **Sluiten** om de procedure te
voltooien.




# Verifiëren

## Controleer de PIX-configuratie

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

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

Initieer een ping van één van de privé netwerken aan het andere privé netwerk om communicatie tussen de twee privé netwerken te testen. In deze configuratie werd een ping van de PIX-zijde (192.168.10.2) naar het interne netwerk CheckpointTM (10.32.50.51) verzonden.

- **toon crypto isakmp sa**-Toont alle huidige IKE SAs bij een peer.

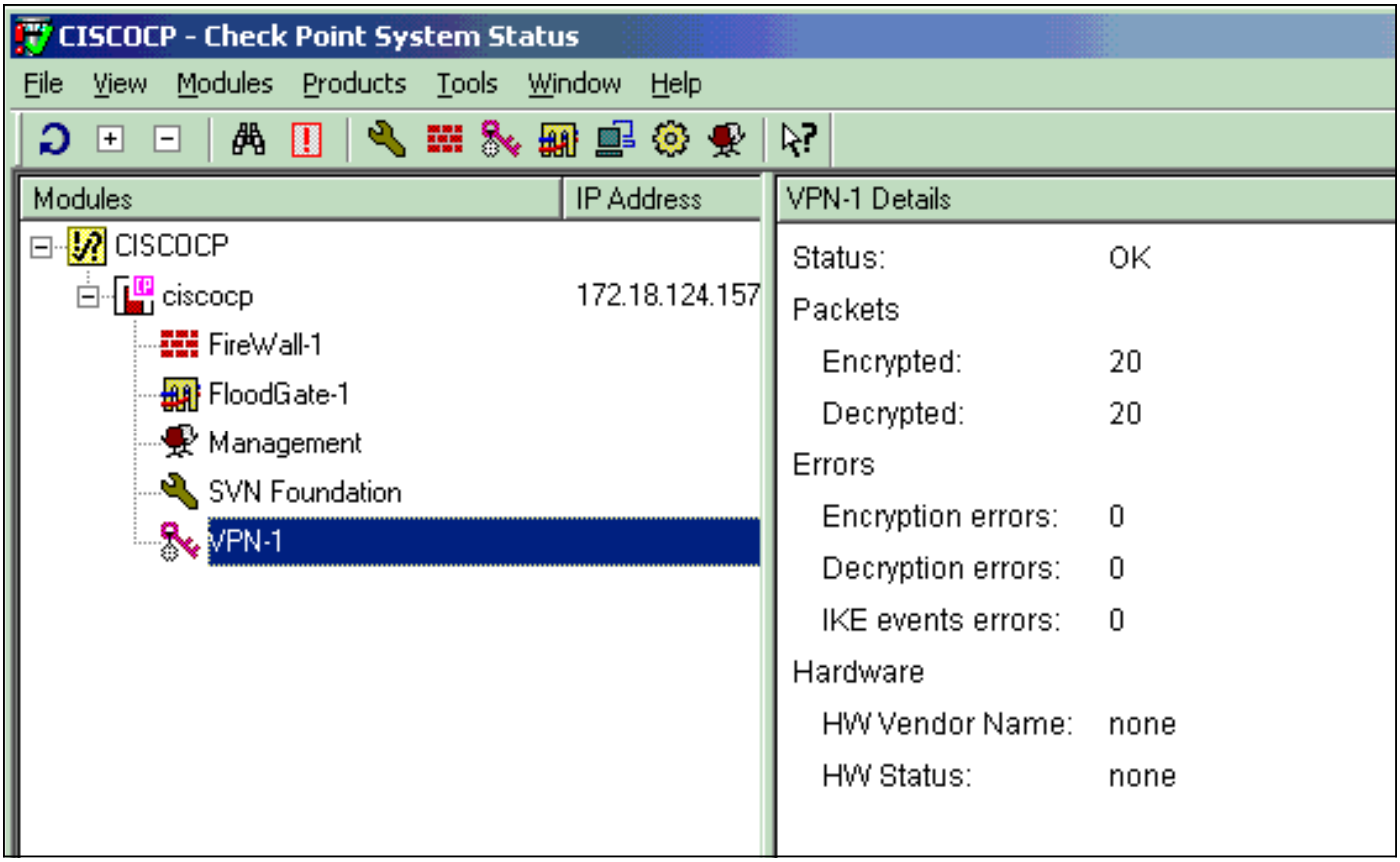
```
show crypto isakmp sa
Total     : 1
Embryonic : 0
             dst                 src                 state     pending   created
  172.18.124.157   172.18.124.158   QM_IDLE          0           1
```

- **Laat crypto ipsec sa**-displays de instellingen die worden gebruikt door de huidige SAs.

```
PIX501A#show cry ipsec sa

interface: outside
    Crypto map tag: rtprules, local addr. 172.18.124.158

   local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.0.0/255.255.128.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 19, #pkts encrypt: 19, #pkts digest 19
    #pkts decaps: 19, #pkts decrypt: 19, #pkts verify 19
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

     local crypto endpt.: 172.18.124.158, remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 6b15a355

     inbound esp sas:
      spi: 0xced238c7(3469883591)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: rtprules
        sa timing: remaining key lifetime (k/sec): (4607998/27019)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:
     inbound pcp sas:

     outbound esp sas:
      spi: 0x6b15a355(1796580181)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 4, crypto map: rtprules
        sa timing: remaining key lifetime (k/sec): (4607998/27019)
        IV size: 8 bytes
        replay detection support: Y


     outbound ah sas:

     outbound pcp sas:
```

## Tunnelstatus op checkpoint NG bekijken

Ga naar de Policy Editor en selecteer **Windows > System Status** om de tunnelstatus te bekijken.




# Problemen oplossen

## Probleemoplossing voor de PIX-configuratie

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.

Gebruik deze opdrachten om uiteinden in de PIX-firewall in te schakelen.

- **debug van crypto motor**-displays debug-berichten over crypto motoren, die encryptie en decryptie uitvoeren.
- **debug van crypto isakmp**-displays over IKE gebeurtenissen.

```
VPN Peer: ISAKMP: Added new peer: ip:172.18.124.157 Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.124.157 Ref cnt incremented to:1 Total VPN Peers:1
ISAKMP (0): beginning Main Mode exchange
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP: encryption 3DES-CBC
ISAKMP: hash MD5
ISAKMP: default group 2
ISAKMP: auth pre-share
ISAKMP: life type in seconds
ISAKMP: life duration (VPI) of 0x0 0x1 0x51 0x80
ISAKMP (0): atts are acceptable. Next payload is 0
```

```
ISAKMP (0): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP (0): processing NONCE payload. message ID = 0
ISAKMP (0): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated
ISAKMP (0): beginning Quick Mode exchange, M-ID of 322868148:133e93b4 IPSEC(key_engine): got a
queue event...
IPSEC(spi_response): getting spi 0xced238c7(3469883591) for SA
from 172.18.124.157 to 172.18.124.158 for prot 3
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
ISAKMP (0): sending INITIAL_CONTACT notify
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.158
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 322868148
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_3DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC-MD5
ISAKMP (0): atts are acceptable. IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.157, src= 172.18.124.158,
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
ISAKMP (0): processing NONCE payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing ID payload. message ID = 322868148
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): processing NOTIFY payload 24576 protocol 3
spi 3469883591, message ID = 322868148
ISAKMP (0): processing responder lifetime
ISAKMP (0): Creating IPSec SAs
inbound SA from 172.18.124.157 to 172.18.124.158 (proxy 10.32.0.0 to 192.168.10.0)
has spi 3469883591 and conn_id 3 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 172.18.124.158 to 172.18.124.157 (proxy 192.168.10.0 to 10.32.0.0)
has spi 1796580181 and conn_id 4 and flags 4
```

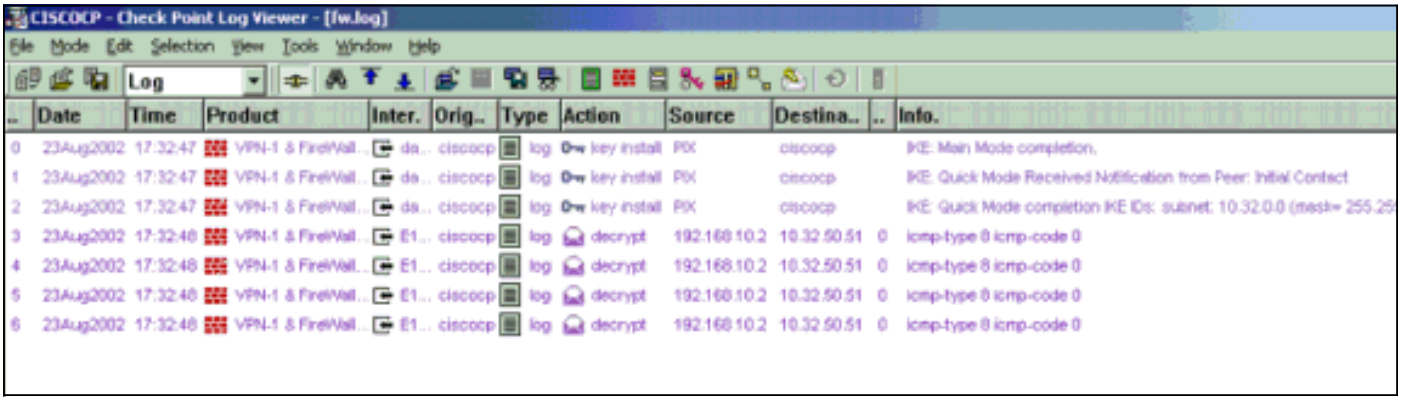
```
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 172.18.124.158, src= 172.18.124.157,
dest_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
src_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xced238c7(3469883591), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.158, dest= 172.18.124.157,
src_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
dest_proxy= 10.32.0.0/255.255.128.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x6b15a355(1796580181), conn_id= 4, keysize= 0, flags= 0x4
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.124.157 Ref cnt incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

## 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 crypto access control list (ACL) op de PIX niet is geconfigureerd om 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.

## Controllereleases op NGO-sites bekijken

Selecteer **Venster > Log Viewer** om de logbestanden te bekijken.




# Gerelateerde informatie

- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems