Een IPsec-tunnel configureren - Cisco-router om firewall 4.1 te controleren

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Conventies](#)
[Configureren](#)
[Netwerkdiagram](#)
[Configuraties](#)
[Verifiëren](#)
[Problemen oplossen](#)
[Opdrachten voor troubleshooting](#)
[Netwerksamenvatting](#)
[Selectieteken](#)
[Voorbeeld van output van foutopsporing](#)
[Gerelateerde informatie](#)

Inleiding

Dit document toont aan hoe u een IPsec-tunnel met vooraf gedeelde toetsen kunt vormen om zich aan twee particuliere netwerken aan te sluiten: het privé-netwerk van 192.168.1.x binnen de router van Cisco en het privé-netwerk van 10.32.50.x binnen het Selectietekenfirewall.

Voorwaarden

Vereisten

Deze voorbeeldconfiguratie veronderstelt dat het verkeer van binnen de router en binnen het Selectieteken naar het Internet (hier weergegeven door de netwerken 172.18.124.x) stroomt voordat u de configuratie start.

Gebruikte componenten

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

- Cisco 3600 router
- Cisco IOS®-software (C3640-JO3S56I-M), release 12.1(5)T, RELEASE-SOFTWARE (FC1)

- Checkpoint Firewall 4.1

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.

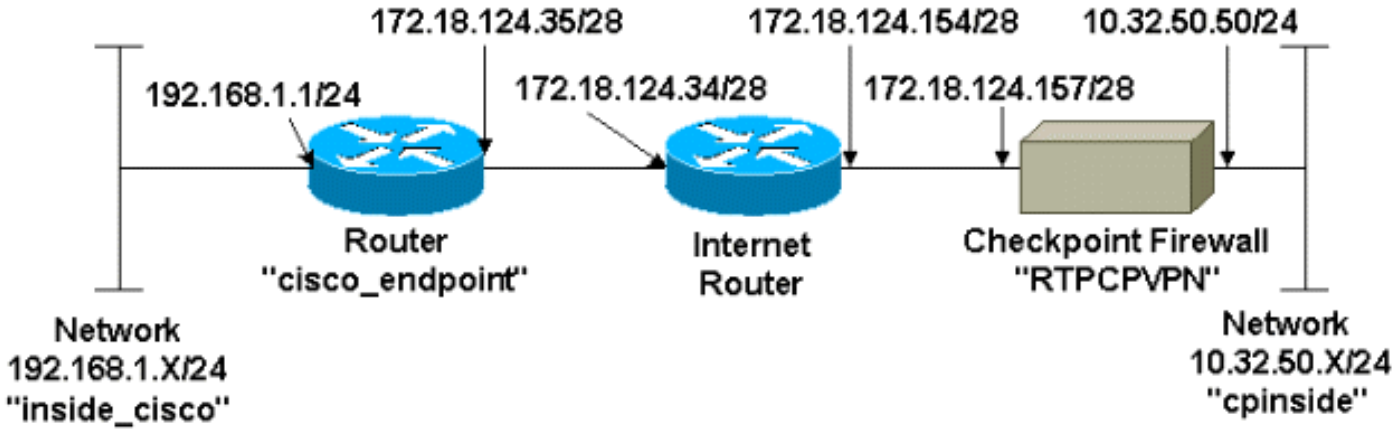
Configureren

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 configuraties.

- Routerconfiguratie
- Configuratie van checkpoint firewall

Routerconfiguratie

Cisco 3600 routerconfiguratie

`Current configuration : 1608 bytes`
`!`
`version 12.1`

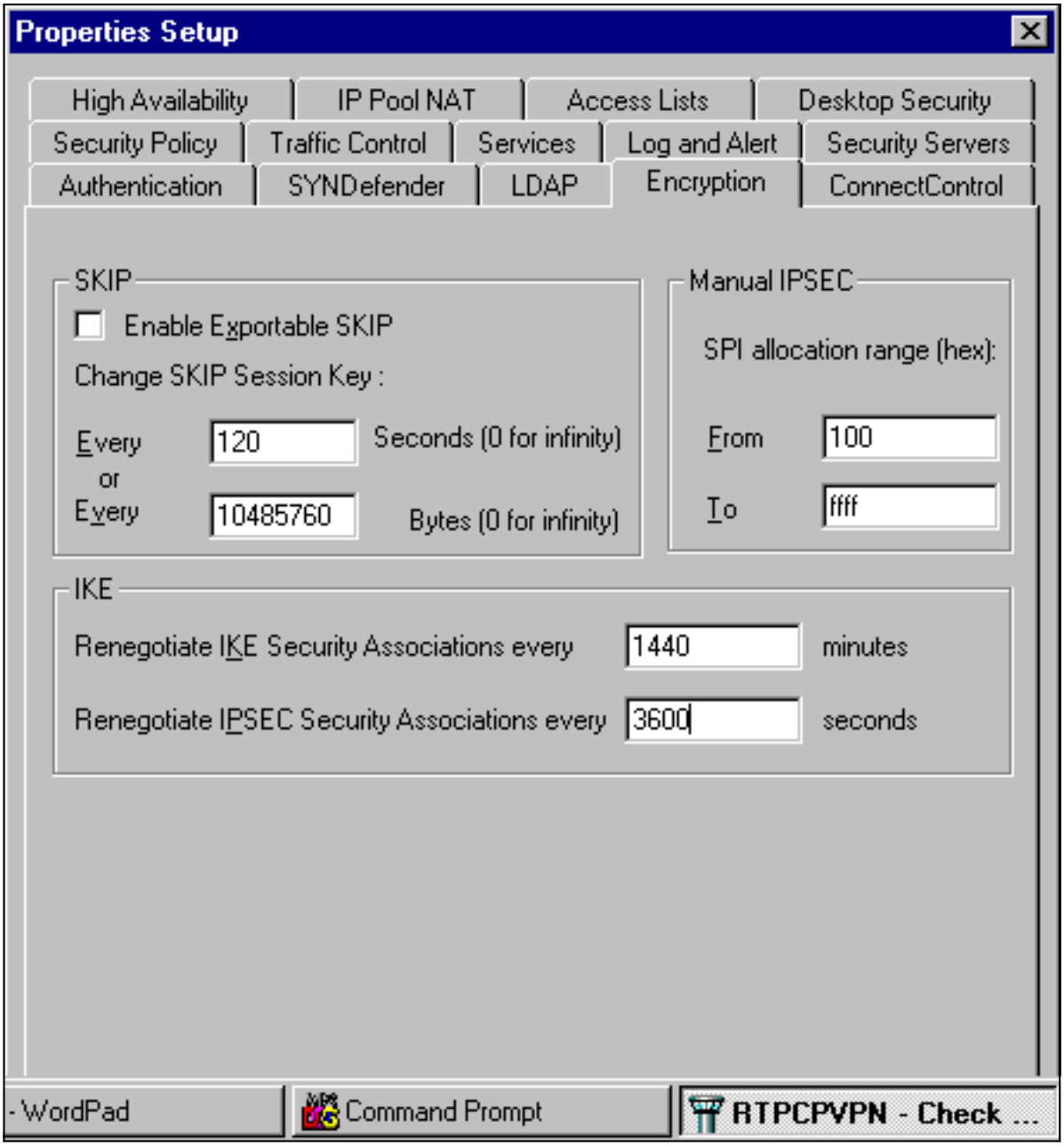
```
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
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
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
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

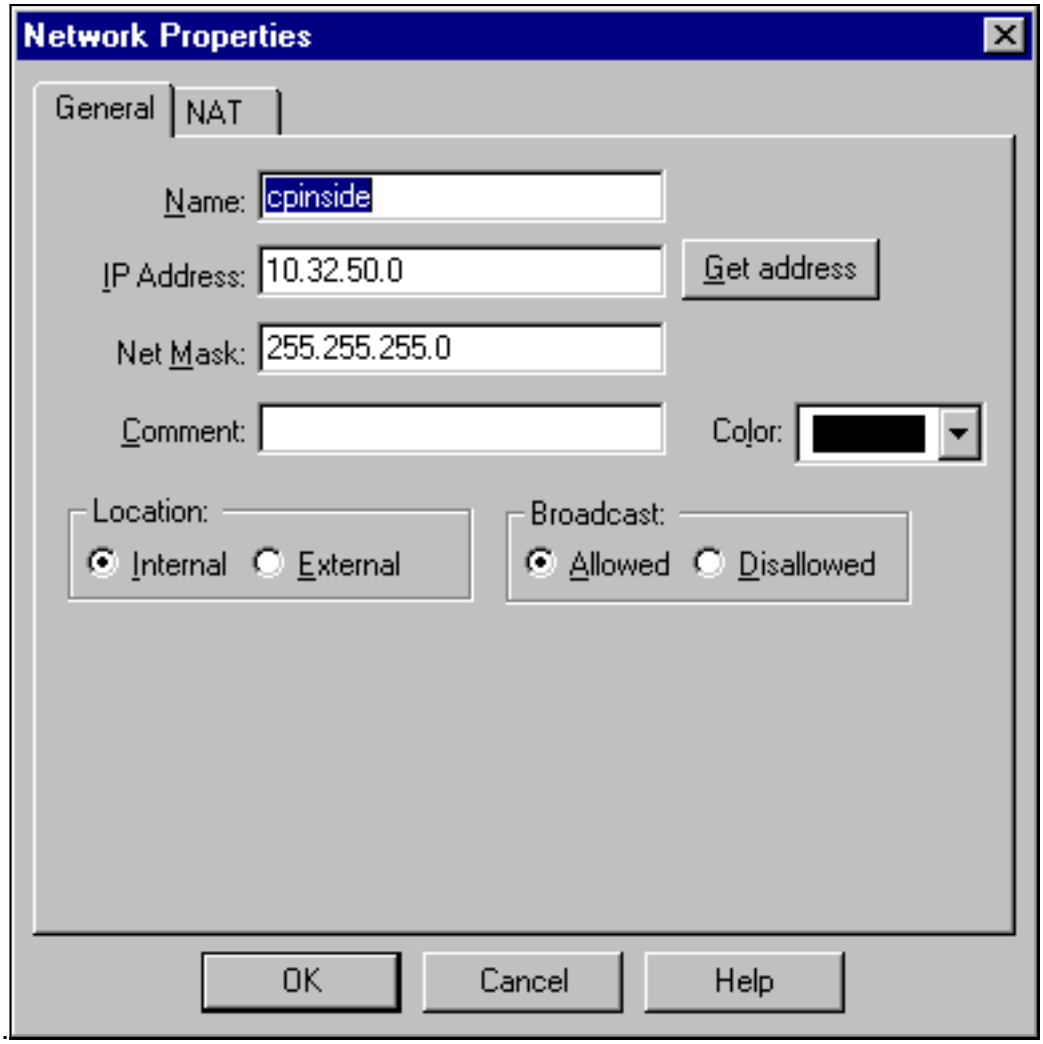
Configuratie van checkpoint firewall

Volg deze stappen om de Firewall van het Selectieteken te configureren.

1. Aangezien de standaard IKE- en IPsec-levens van elke verkoper verschillen, selecteert u **Eigenschappen > Encryptie** om de standaardwaarden voor de reddingsduur van het checkpoint in te stellen om met Cisco akkoord te gaan.De standaard IKE-levensduur van Cisco is 86400 seconden (= 1440 minuten) en kan door deze opdrachten worden gewijzigd:**beleid van crypto isakmp #levensduur #**De configureerbare Cisco IKE-levensduur is van 60-8640 seconden. Het leven van Cisco standaard IPsec is 3600 seconden en kan worden aangepast door de **crypto ipsec security-associatie levenslang seconden #**opdracht.Het configureerbare Cisco IPsec-leven komt van 120-8640 seconden.

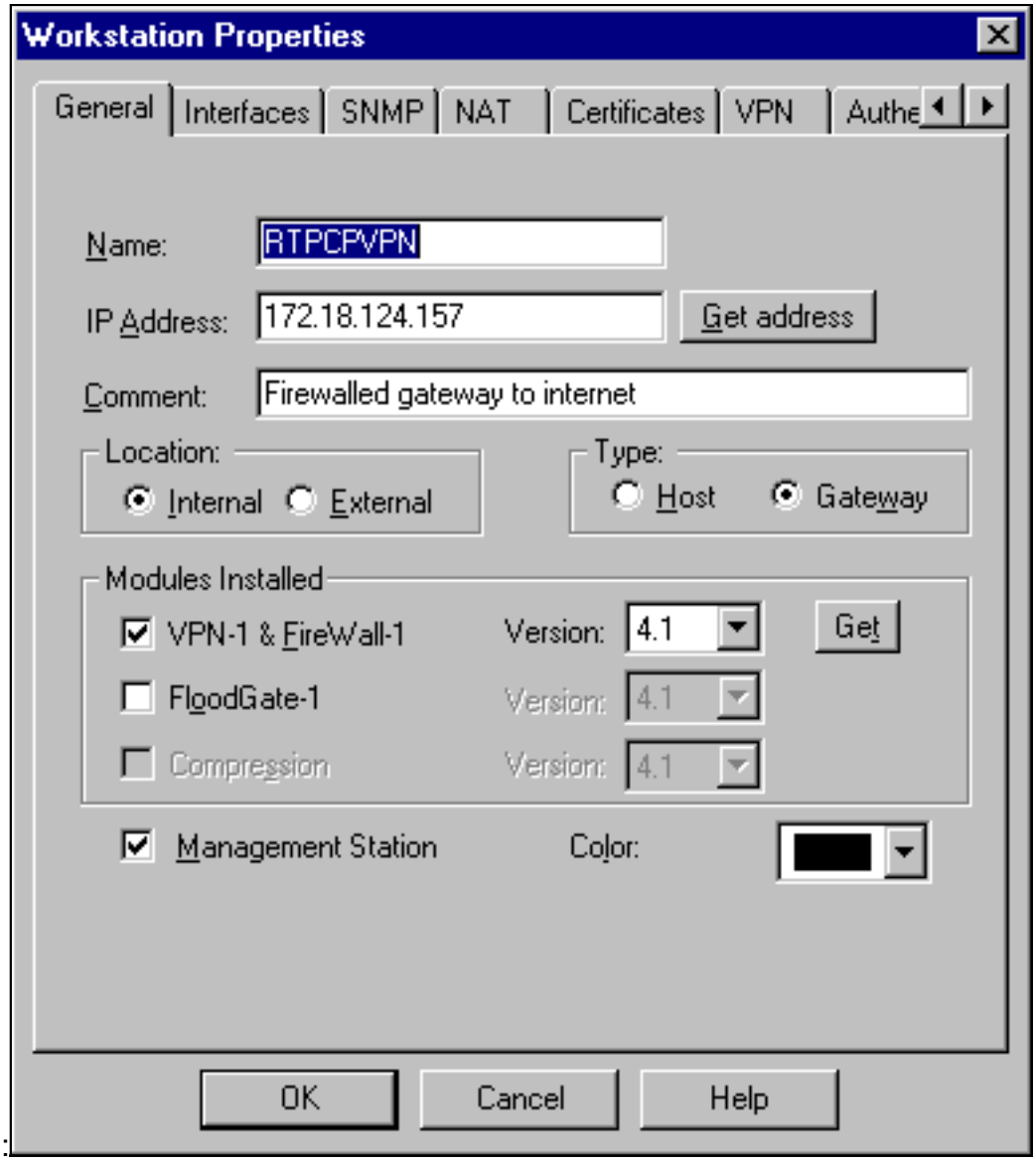


2. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het interne netwerk te configureren (aangeduid als "component") achter het Selectieteken.Dit moet overeenkomen met het bestemmings- (tweede) netwerk in de Cisco **toegangslijst 115**, **ip 192.168.1.0 0.0.255 10.32.50.0 0.0.255** opdracht.Selecteer **Intern** onder



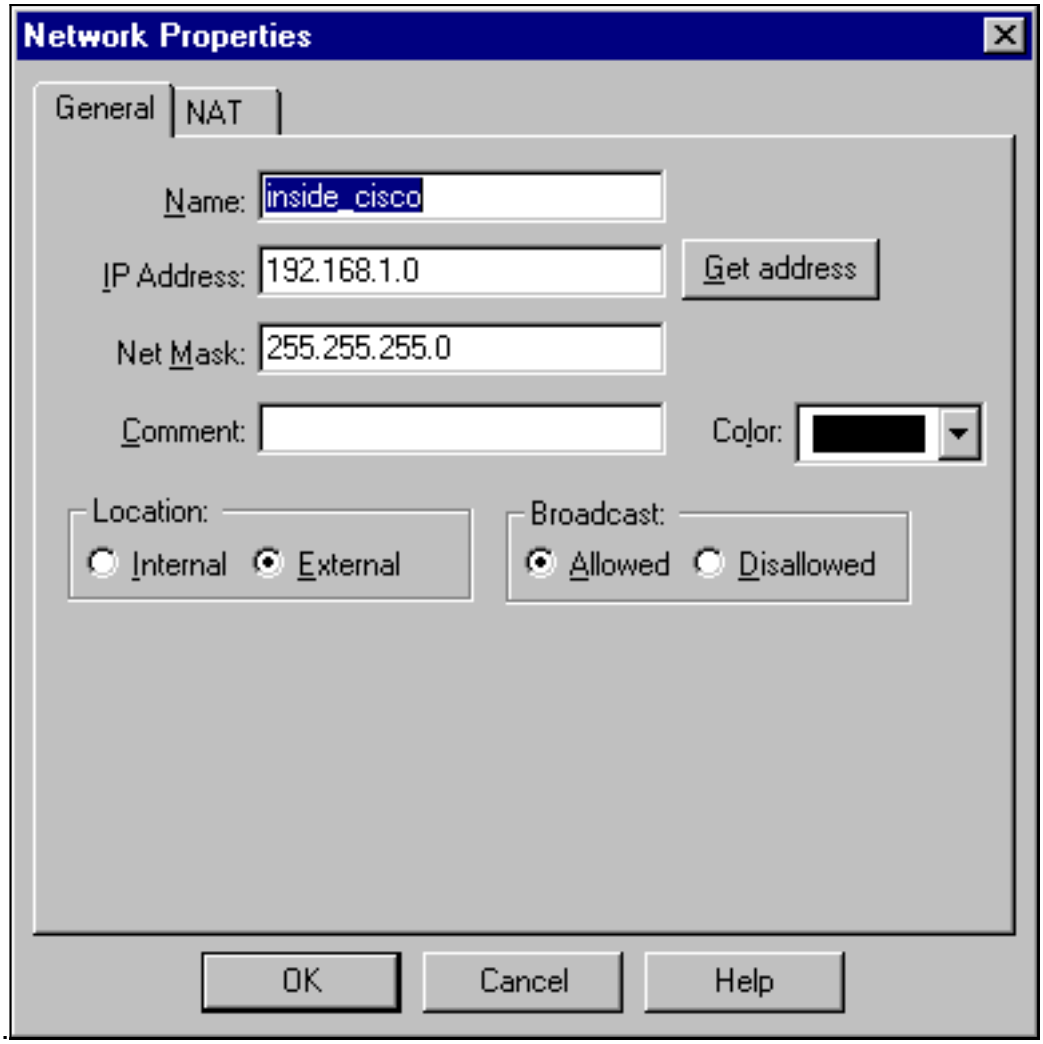
Locatie.

3. Selecteer **Manager > Netwerkobjecten > Bewerken** om het object te bewerken voor het opdracht RTPC VPN-checkpoint (gateway) waarnaar de Cisco-router **in** de **ingestelde** peer **172.18.124.157** wijst.Selecteer **Intern** onder Locatie. Selecteer voor type de optie **Gateway**. Selecteer onder Geïnstalleerde modules het vakje **VPN-1 en FireWall-1** en selecteer vervolgens het vakje **Management**



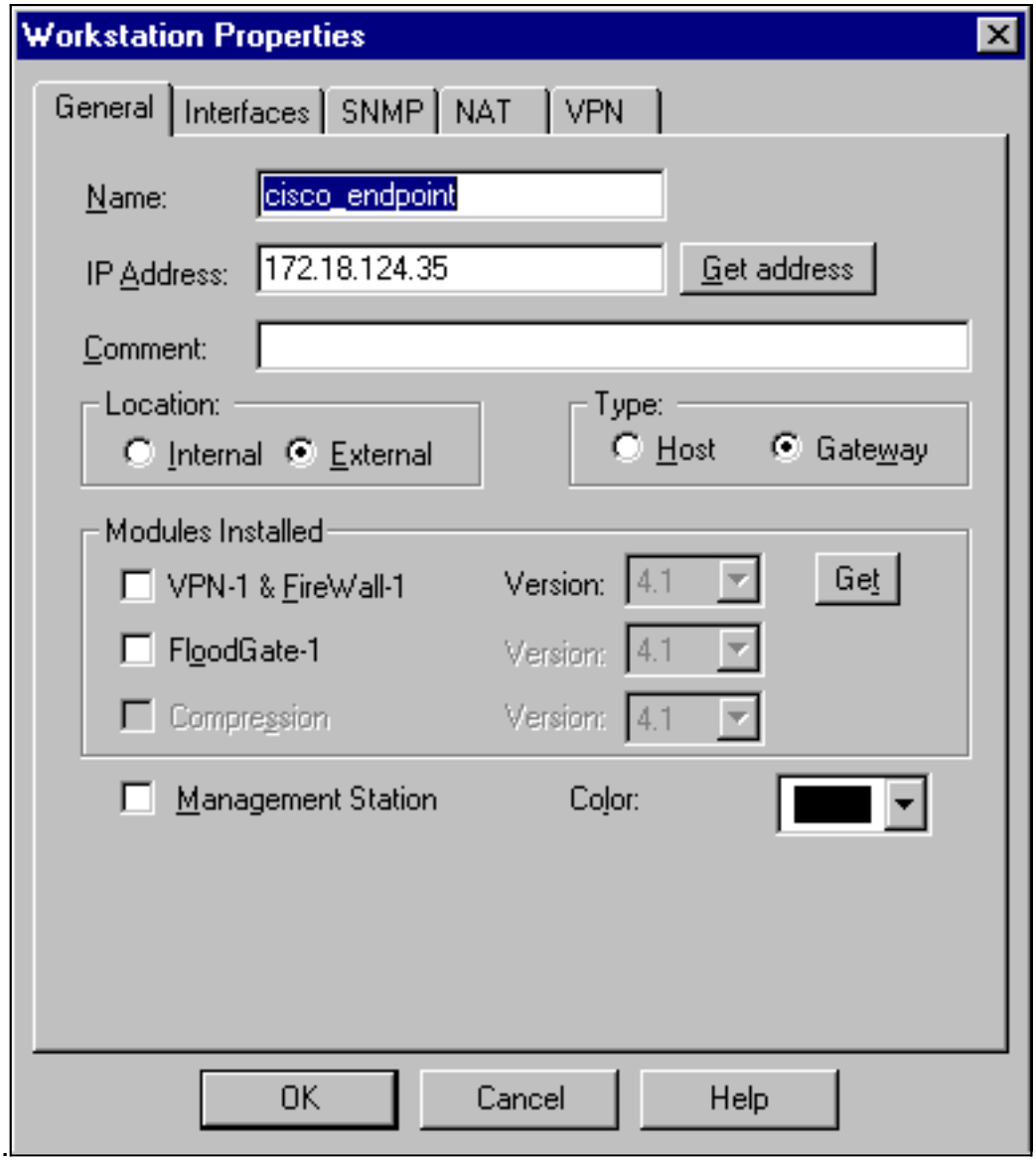
Station:

4. Selecteer **Bewerken > Netwerkobjecten > Nieuw > Netwerk** om het object voor het externe netwerk te configureren (aangeduid als "interne_cisco") achter de Cisco-router.Dit moet overeenkomen met het bron- (eerste) netwerk in de Cisco **Access-list 115** opdracht **voor ip 192.168.1.0 0.0.255 10.32.50.0.0.0.255**.Selecteer **Extern** onder



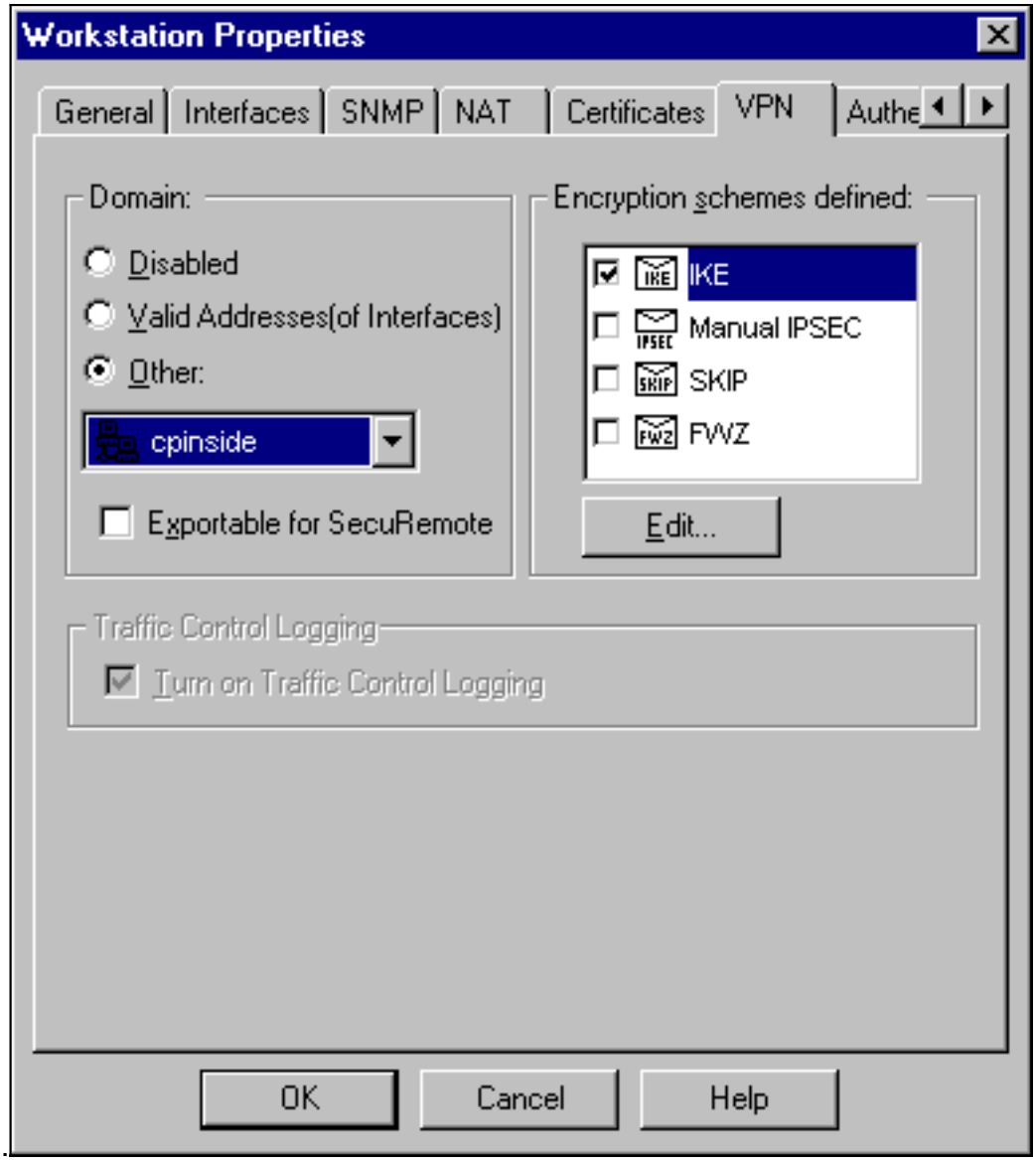
Locatie.

5. Selecteer **Manager > Netwerkobjecten > Nieuw > Workstation** om een object toe te voegen voor de externe Cisco-routergateway (genaamd "cisco_endpoints"). Dit is de interface van Cisco waarop de **opdracht *voor* crypto map** wordt toegepast.Selecteer **Extern** onder Locatie. Selecteer voor type de optie **Gateway**.**Opmerking:** selecteer niet het aankruisvakje VPN-



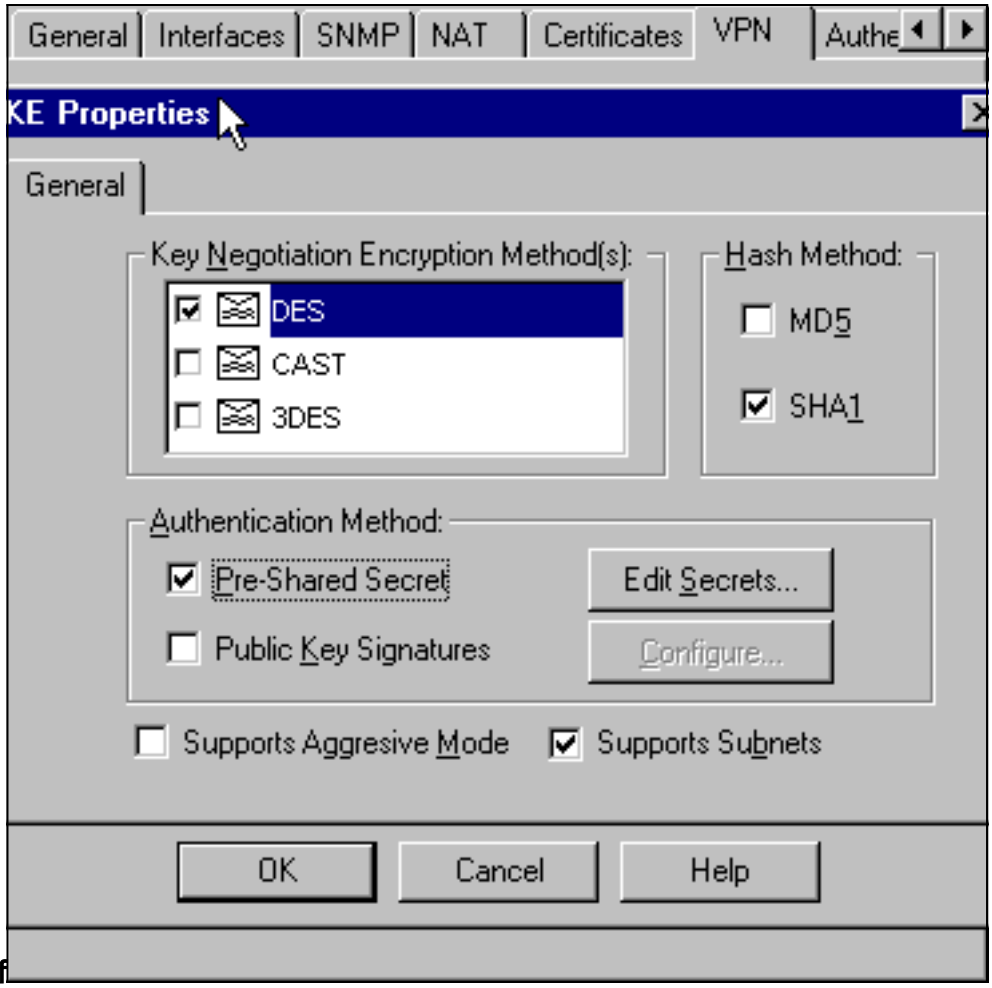
1/FireWall-1.

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



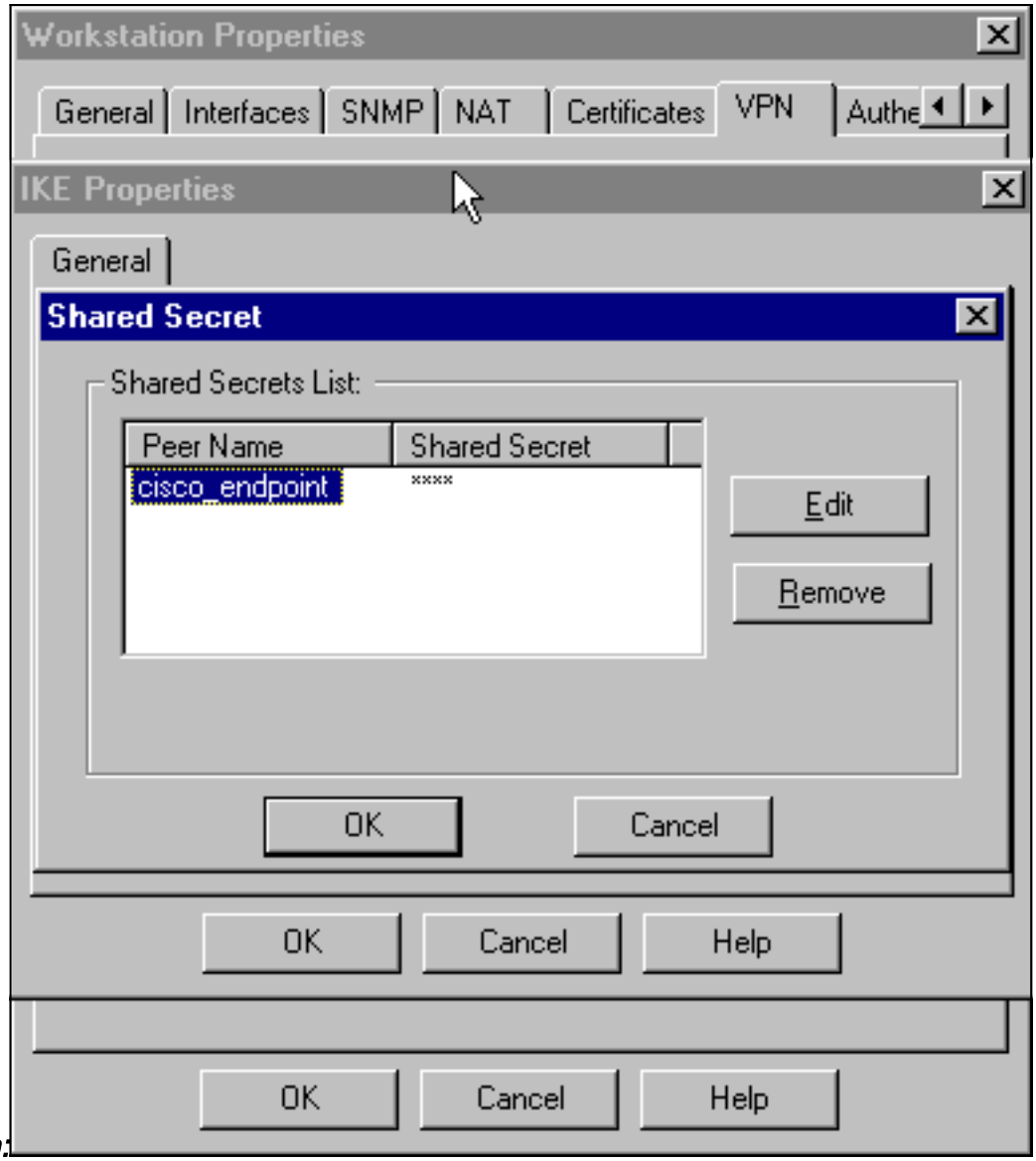
Bewerken.

7. Wijzig de IKE-eigenschappen voor DES-encryptie om met deze opdrachten akkoord te gaan:**beleid van crypto isakmp #encryptieOpmerking:** DES-encryptie is de standaardinstelling zodat het niet zichtbaar is in de Cisco-configuratie.
8. Wijzig de IKE-eigenschappen in SHA1-hashing om met deze opdrachten akkoord te gaan:**beleid van crypto isakmp #hash shaOpmerking:** Het SHA-hashing-algoritme is de standaardinstelling zodat het niet zichtbaar is in de Cisco-configuratie.Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder verificatiemethode. Dit stemt in met deze opdrachten:**beleid van crypto isakmp #controle**



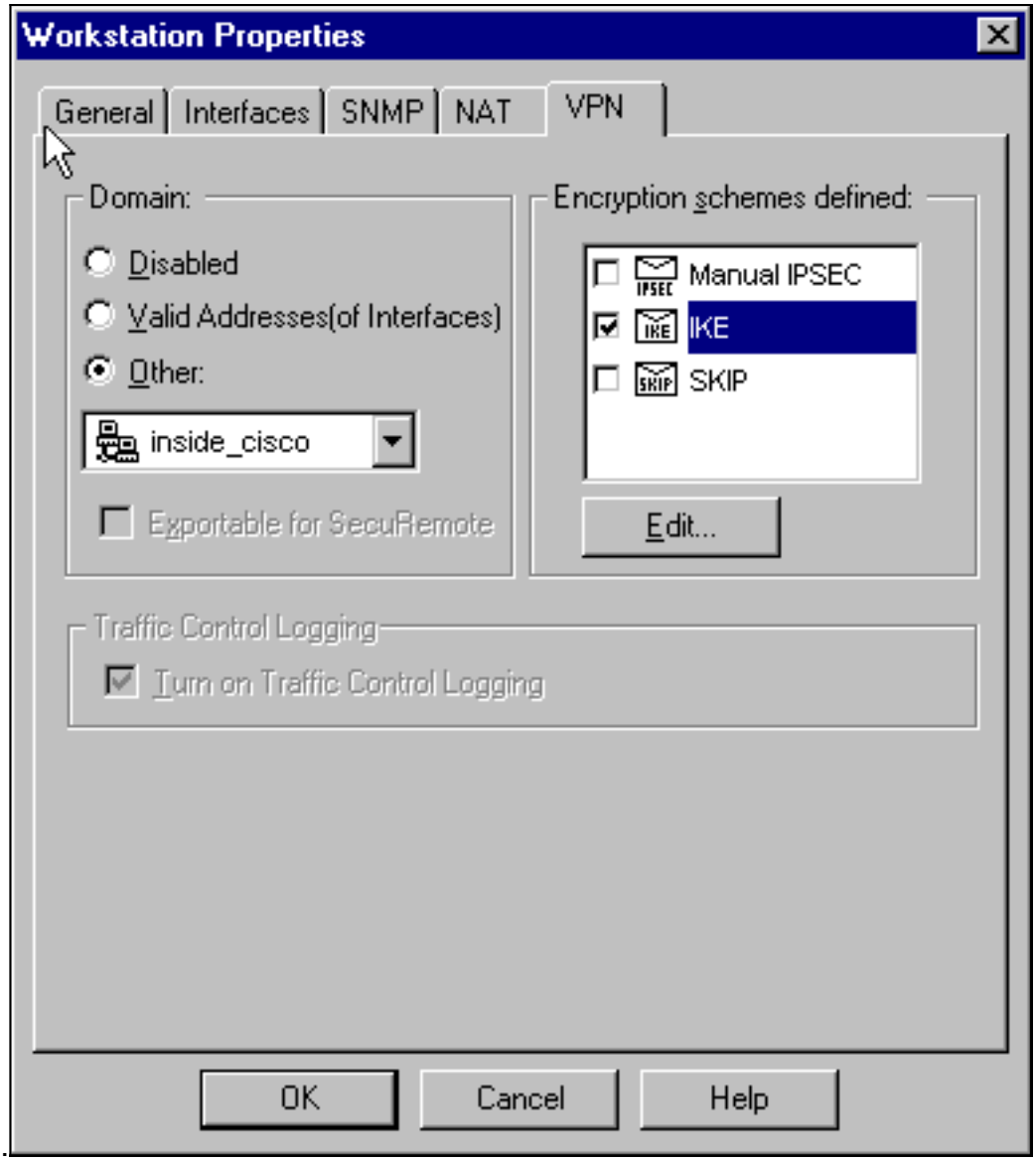
vooraf

9. Klik op **Geheimen bewerken** om de voorgedeelde sleutel in te stellen om met de *opdracht* ***Crypto*** Sakmp van de **sleutel adres van** Cisco *adres* ***te***



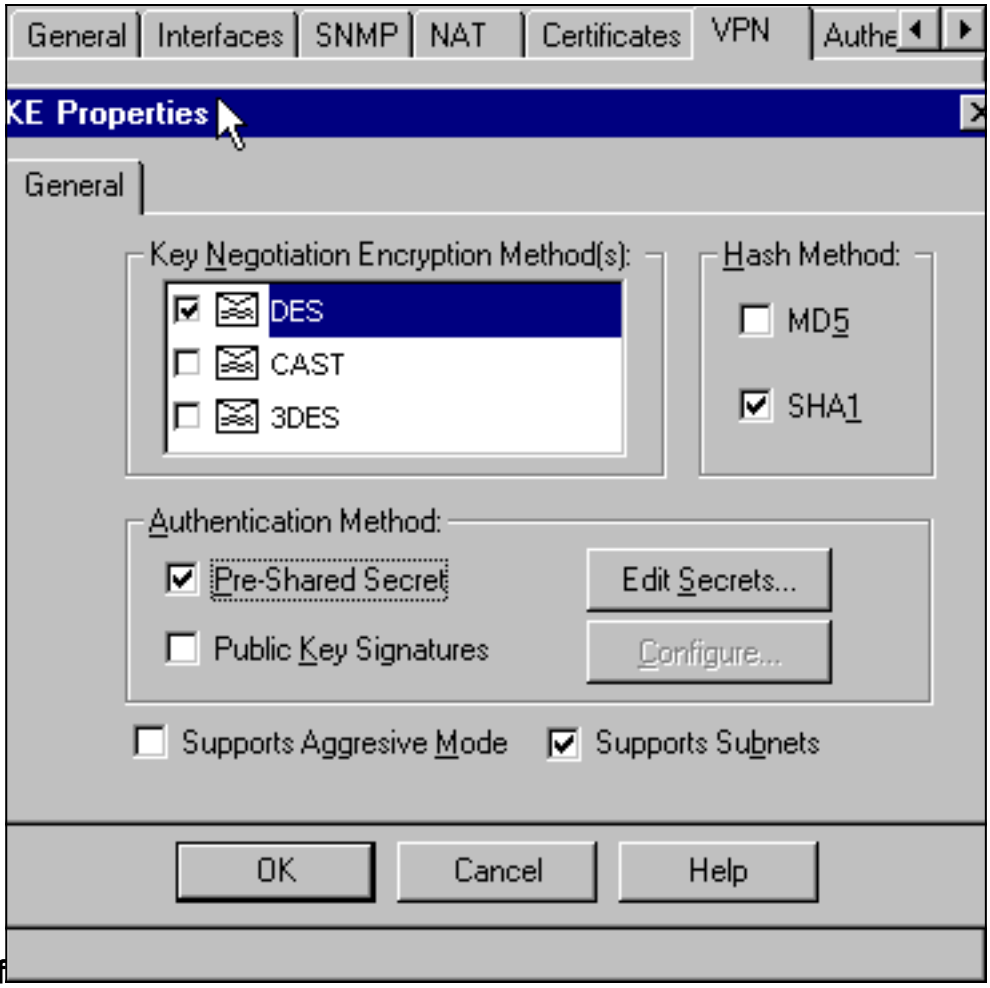
gaan:

10. 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 Cisco (genoemd "binnenkant_cisco"). Selecteer onder Encryption schemes die worden gedefinieerd **IKE** en klik vervolgens op



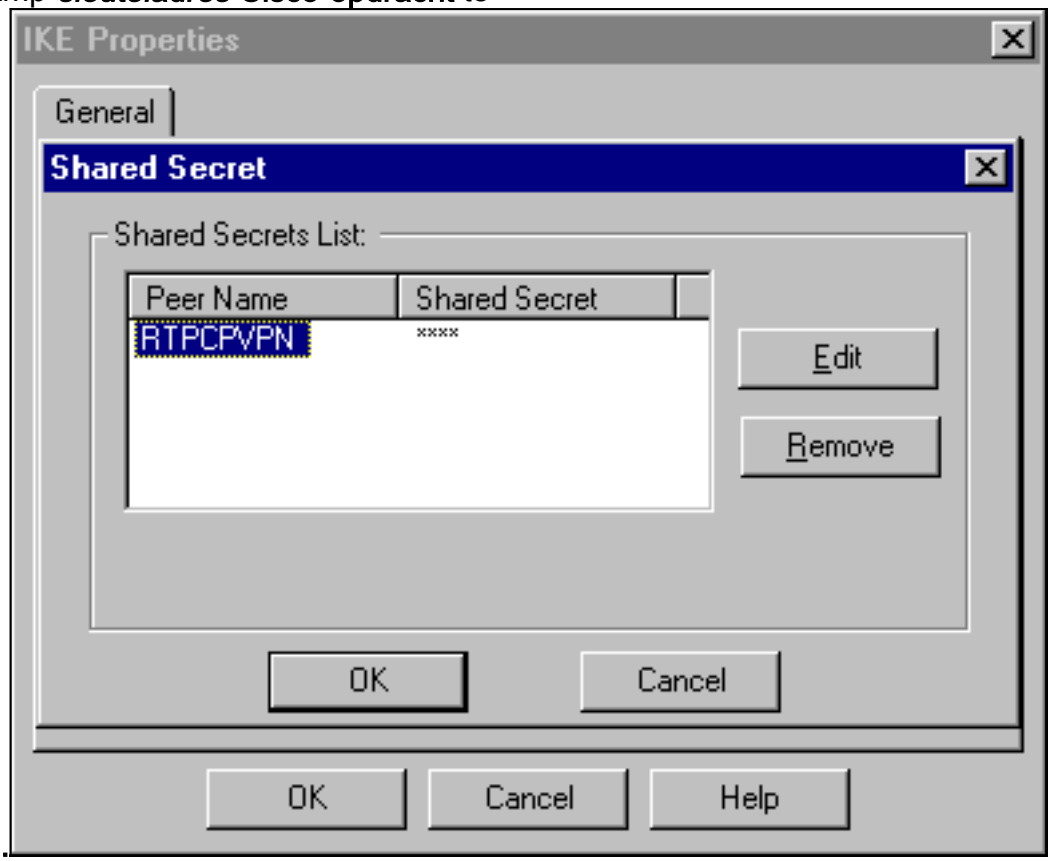
Bewerken.

11. Wijzig de IKE-eigenschappen DES-encryptie om met deze opdrachten akkoord te gaan:**beleid van crypto isakmp #encryptieOpmerking:** DES-encryptie is de standaardinstelling zodat het niet zichtbaar is in de Cisco-configuratie.
12. Wijzig de IKE-eigenschappen in SHA1-hashing om met deze opdrachten akkoord te gaan:**beleid van crypto isakmp #hash shaOpmerking:** Het SHA-hashing-algoritme is de standaardinstelling zodat het niet zichtbaar is in de Cisco-configuratie.Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Controleer **Ondersteunen subnetten**.Controleer **vooraf gedeeld geheim** onder verificatiemethode. Dit stemt in met deze opdrachten:**beleid van crypto isakmp #controle**



vooraf

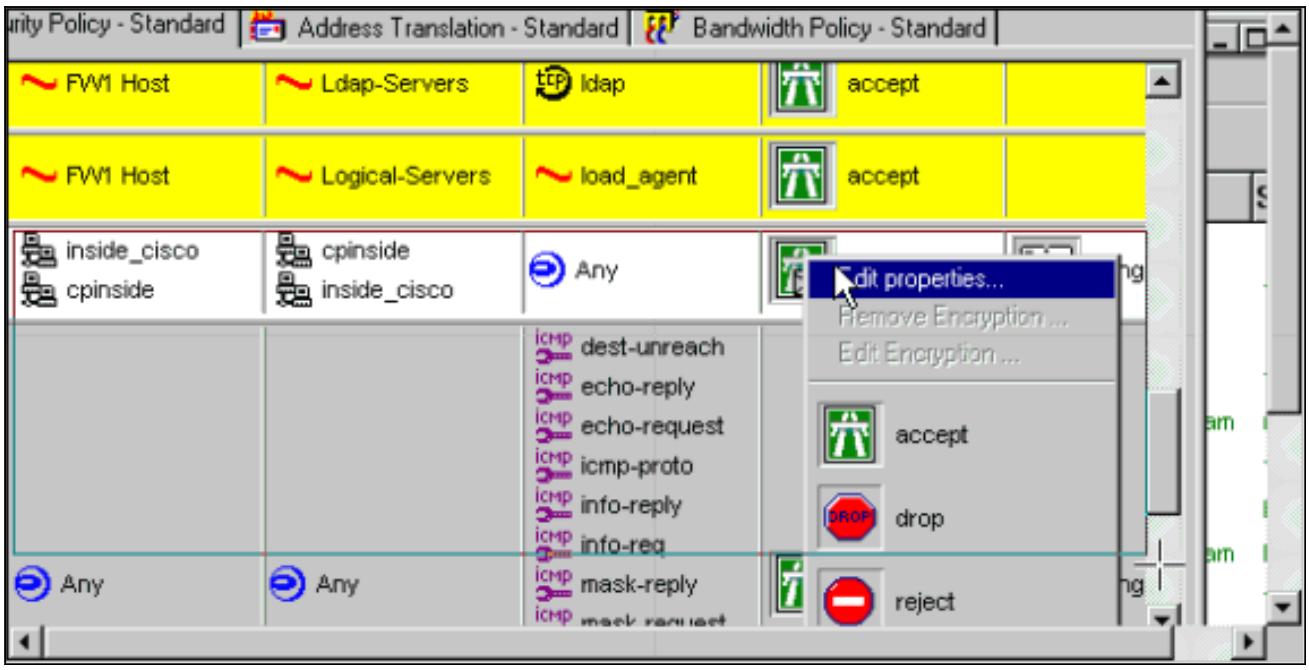
13. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de *opdracht* ***Crypto*** Sakmp-***sleuteladres*** **Cisco-opdracht** te



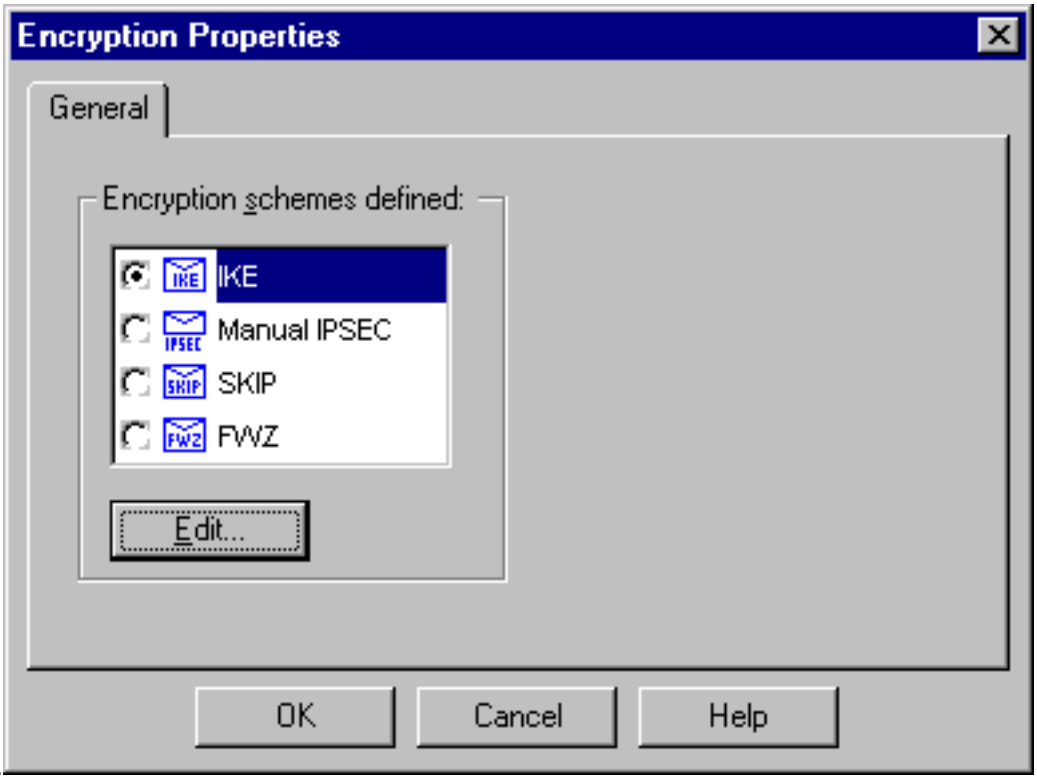
instemmen.

14. 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**.

15. Klik op het pictogram Green **Encrypt** en selecteer **Eigenschappen bewerken** om het coderingsbeleid te configureren onder het kopje Actie.

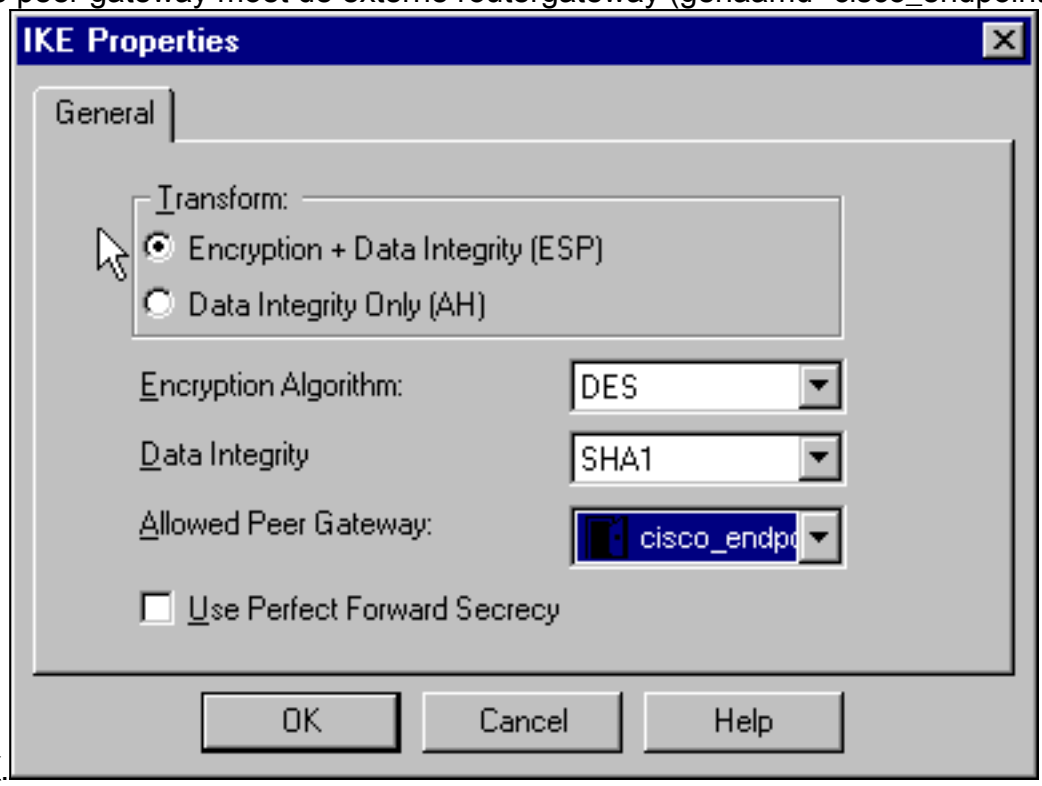


16. Selecteer **IKE** en klik vervolgens op



Bewerken.

17. Wijzig deze eigenschappen in het venster IKE Properties om met de Cisco IPsec transformaties in de **crypto ipsec transformatie-set rtpset esp-des esp-sha-hmac** opdracht overeen te komen: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 routergateway (genaamd "cisco_endpoints") zijn.



Klik op **OK**.

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

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw 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.

- **toon crypto isakmp sa**-Bekijk alle huidige IKE security associaties (SAs) bij een peer.
- **Laat crypto ipsec sa**-View de instellingen zien die door huidige SAs worden gebruikt.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

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

- **debug van crypto motor**-displays debug-berichten over crypto motoren, die encryptie en decryptie uitvoeren.
- **debug van crypto isakmp**-displays over IKE gebeurtenissen.
- **debug van crypto ipsec**-displays IPsec gebeurtenissen.
- **duidelijke crypto isakmp** - reinigt alle actieve IKE connecties.
- **duidelijke crypto sa**—hiermee worden alle IPsec SA's gereinigd.

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 router niet is geconfigureerd om aan te passen, 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.

Selectieteken

Omdat de tracering voor lang is ingesteld in het venster Policy Editor, moet het ontkende verkeer rood in het Log Viewer verschijnen. U kunt meer breedband debug gebruiken bij:

```
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
```

Opmerking: dit was een Microsoft Windows NT-installatie.

Geef deze opdrachten uit om de SA's te wissen op het checkpoint:

```
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 The Are you good? .

Voorbeeld van output van foutopsporing

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(sa_request): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
```

```
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
```

```
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

interface: Ethernet0/0
    Crypto map tag: rtp, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #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.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, media mtu 1500
     current outbound spi: 181C6E59

     inbound esp sas:
      spi: 0xA29984CA(2727969994)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--                 sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x181C6E59(404516441)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4607997/3447)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


cisco_endpoint#show crypto isakmp sa
    dst           src          state        conn-id   slot
172.18.124.157 172.18.124.35  QM_IDLE           1       0

cisco_endpoint#exit
```

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning en documentatie – Cisco Systems