Configuratie van een IPSec-tunnels - Cisco Secure PIX-firewall voor checkpoint 4.1-firewall

Inhoud

Inleiding

Deze steekproefconfiguratie toont hoe te om een IPSec-tunnel met pre-gedeelde sleutels te vormen om zich bij twee privé netwerken aan te sluiten. In ons voorbeeld, zijn de aangesloten netwerken het 192.168.1.X privé netwerk binnen de Cisco Secure Pix Firewall (PIX) en het 10.32.50.X privé netwerk binnen het Selectieteken. Aangenomen wordt dat het verkeer van binnen de PIX en binnen de Checkpoint 4.1 Firewall naar het internet (hier weergegeven door de 172.18.124.X netwerken) voorafgaand aan het begin van deze configuratie vloeit.

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:

- PIX-softwarerelease 5.3.1
- 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 de Cisco Technical Tips Convention voor meer informatie over documentconventies.

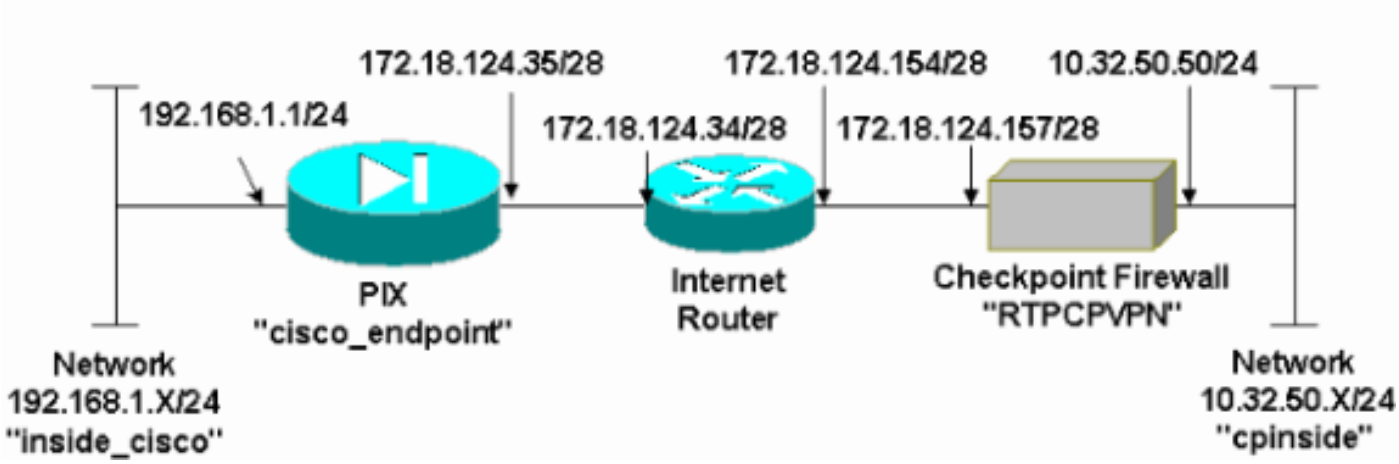
Configureren

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

N.B.: Als u aanvullende informatie wilt vinden over de opdrachten in dit document, gebruikt u het Opdrachtplanningprogramma (alleen geregistreerd klanten).

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven:



Configuraties

Dit document gebruikt de configuraties die in dit gedeelte worden weergegeven.

PIX-configuratie

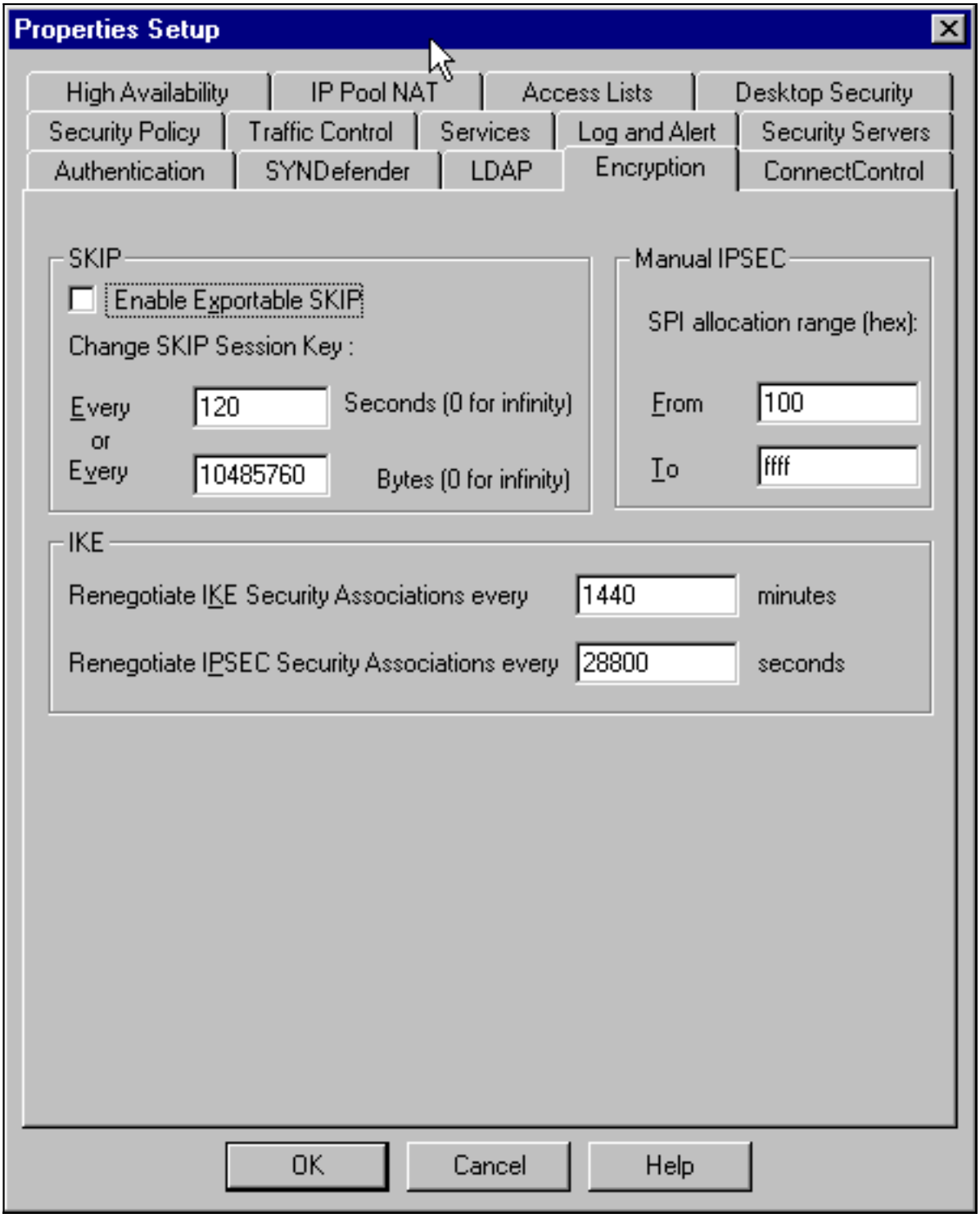
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
```

```
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
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
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
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
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
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
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
isakmp identity address
```

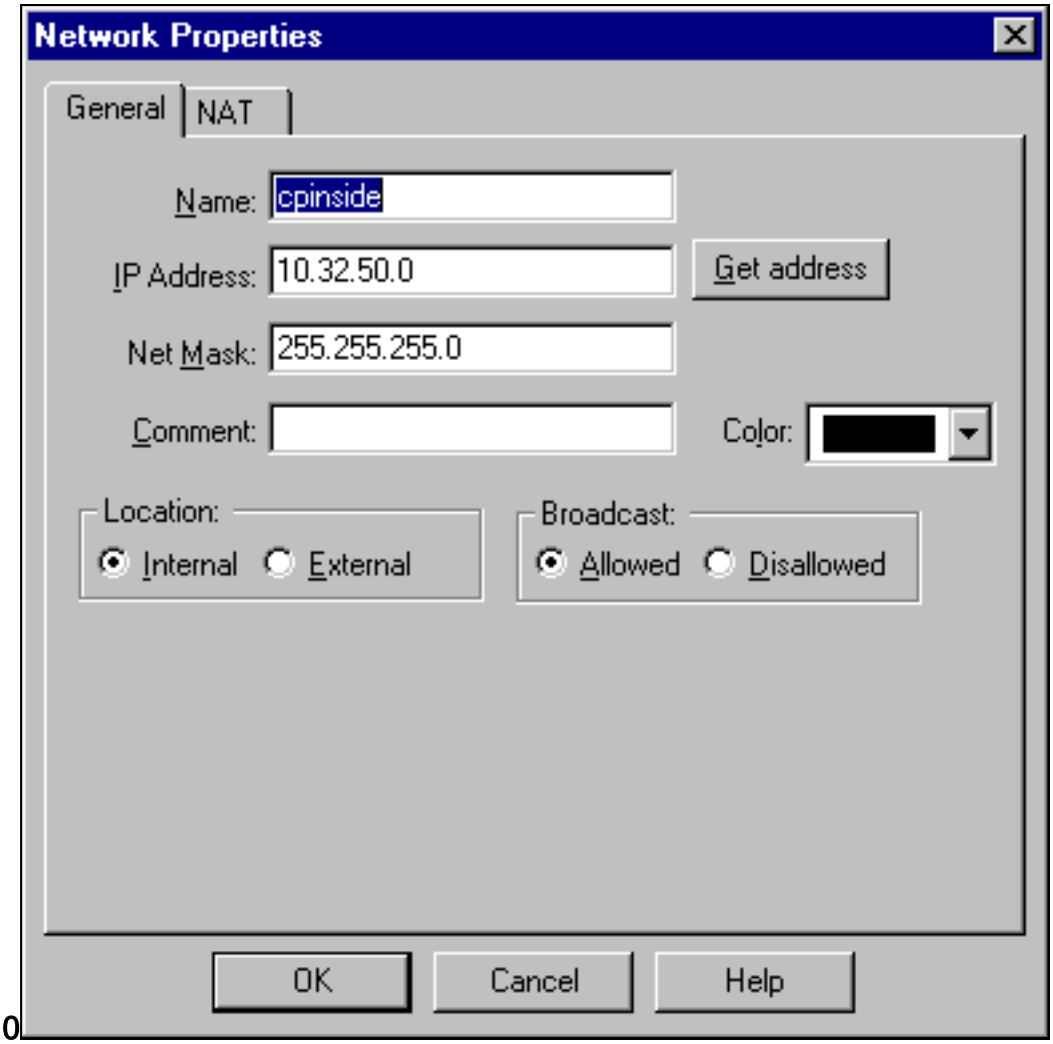
```
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

Selectietekenfirewall

1. Aangezien de standaard IKE- en IPSec-levens van verschillende verkopers verschillen, selecteert u **Eigenschappen > Encryption** om de leven van het checkpoint in te stellen om met de standaardinstellingen van PIX akkoord te gaan.De PIX standaard IKE levensduur is 86400 seconden (=1440 minuten), gewijzigd door deze opdracht: **isakmp-beleid # levensduur 86400**De PIX IKE-levensduur kan tussen 60 en 8640 seconden worden ingesteld.De standaard IPSec-levensduur van PIX is 28800 seconden, gewijzigd door deze opdracht: **geheimhoudingsduur van crypto ipsec (*)**U kunt een PIX IPSec-leven configureren tussen 120-8640
   seconden.

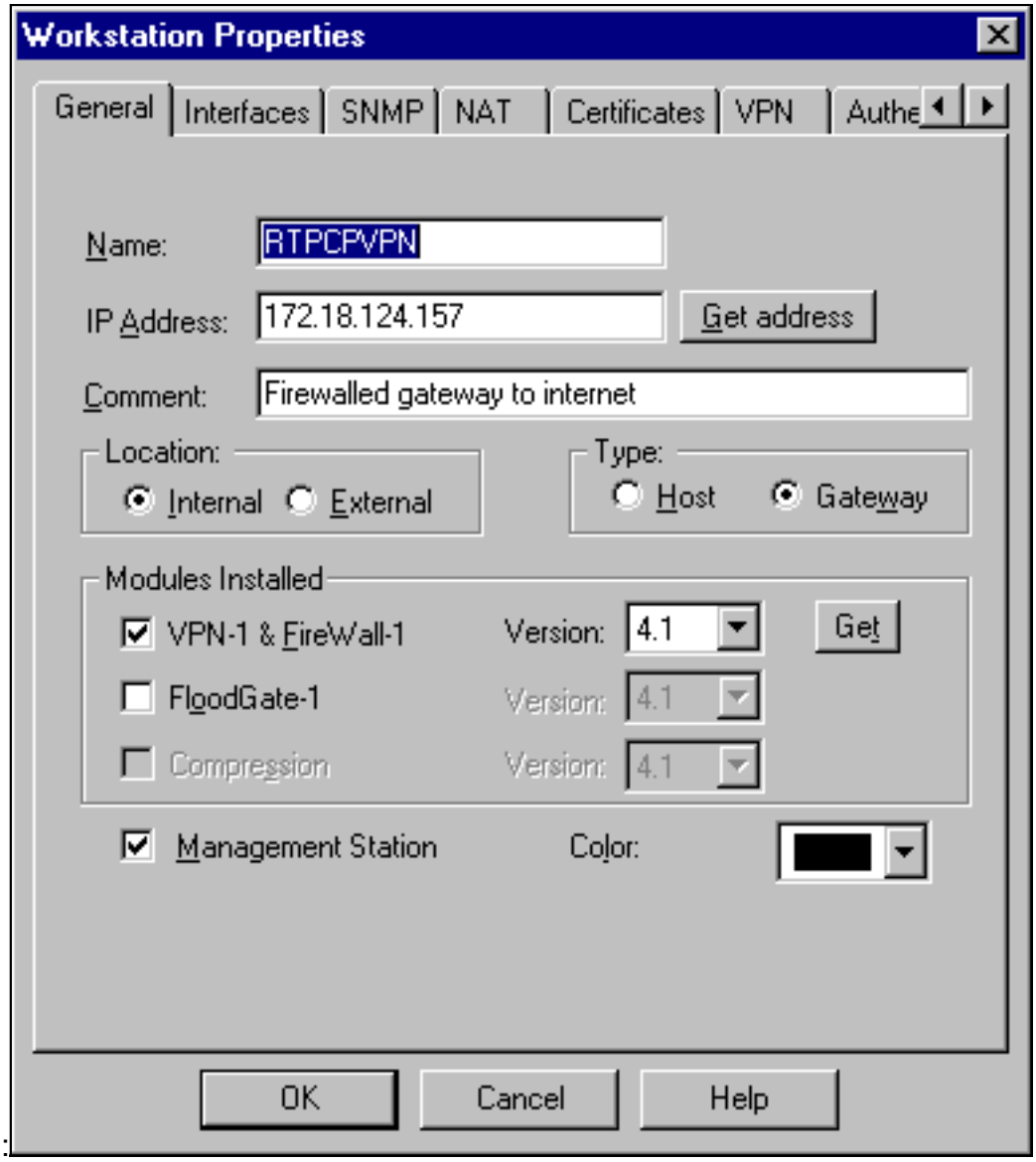


2. Selecteer **Manager > Netwerkobjecten > Nieuw (of Bewerken) > Netwerk** om het object voor het interne netwerk ("component") achter het checkpoint te configureren.Dit moet overeenkomen met het bestemming (tweede) netwerk in deze PIX-opdracht: **toegangslijst 115 vergunning ip 192.168.1.0 255.255.255.0 10.32.50.0**



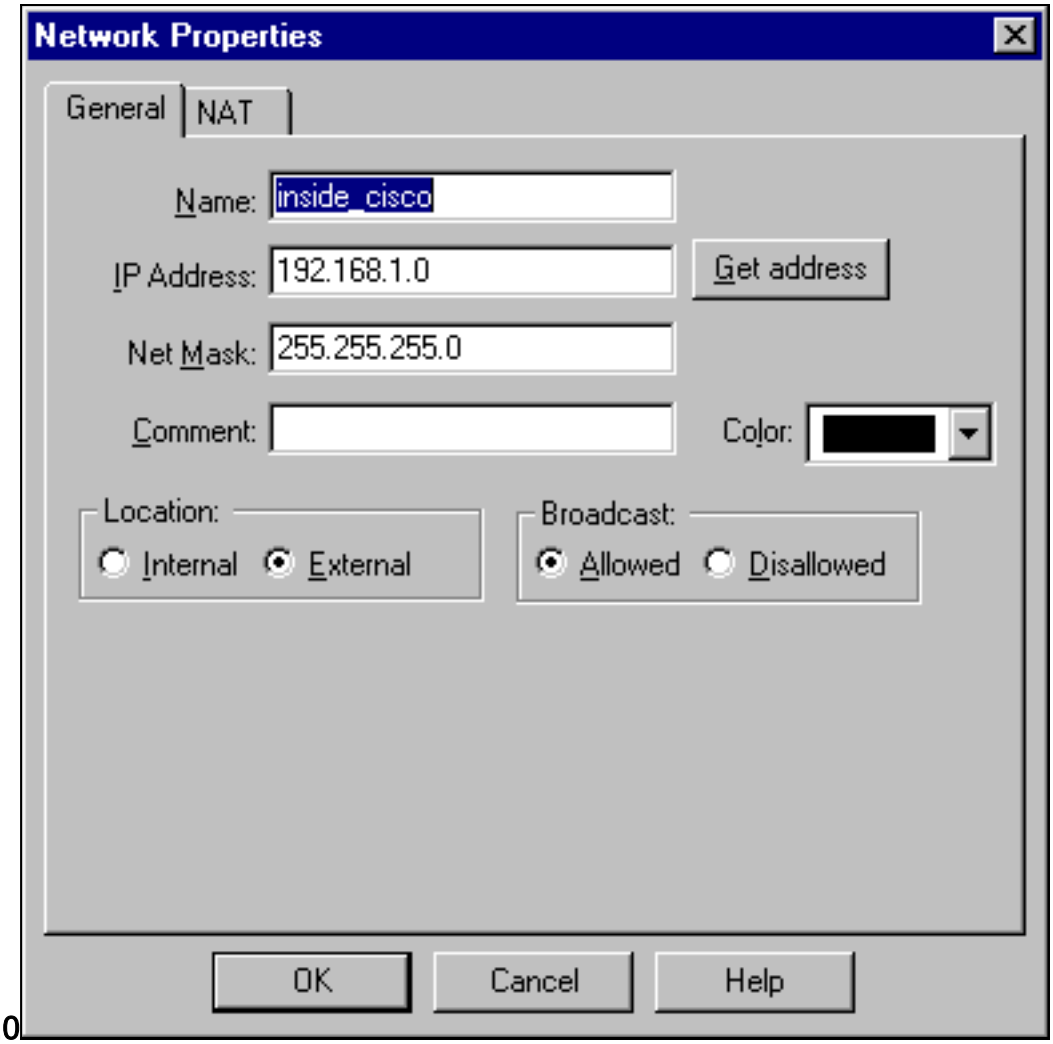
255.255.255.0

3. Selecteer **Manager > Netwerkobjecten > Bewerken** om het object voor het eindpunt van de gateway ("RTPC VPN"-controle) te bewerken waar PIX in deze opdracht naar wijst: **naam van crypto map # set peer ip_address**Selecteer onder Locatie de optie **Interne**. Selecteer voor type de optie **Gateway**. Selecteer onder Geïnstalleerde modules het vakje **VPN-1 en FireWall-1** en selecteer vervolgens het selectiekader **Management**



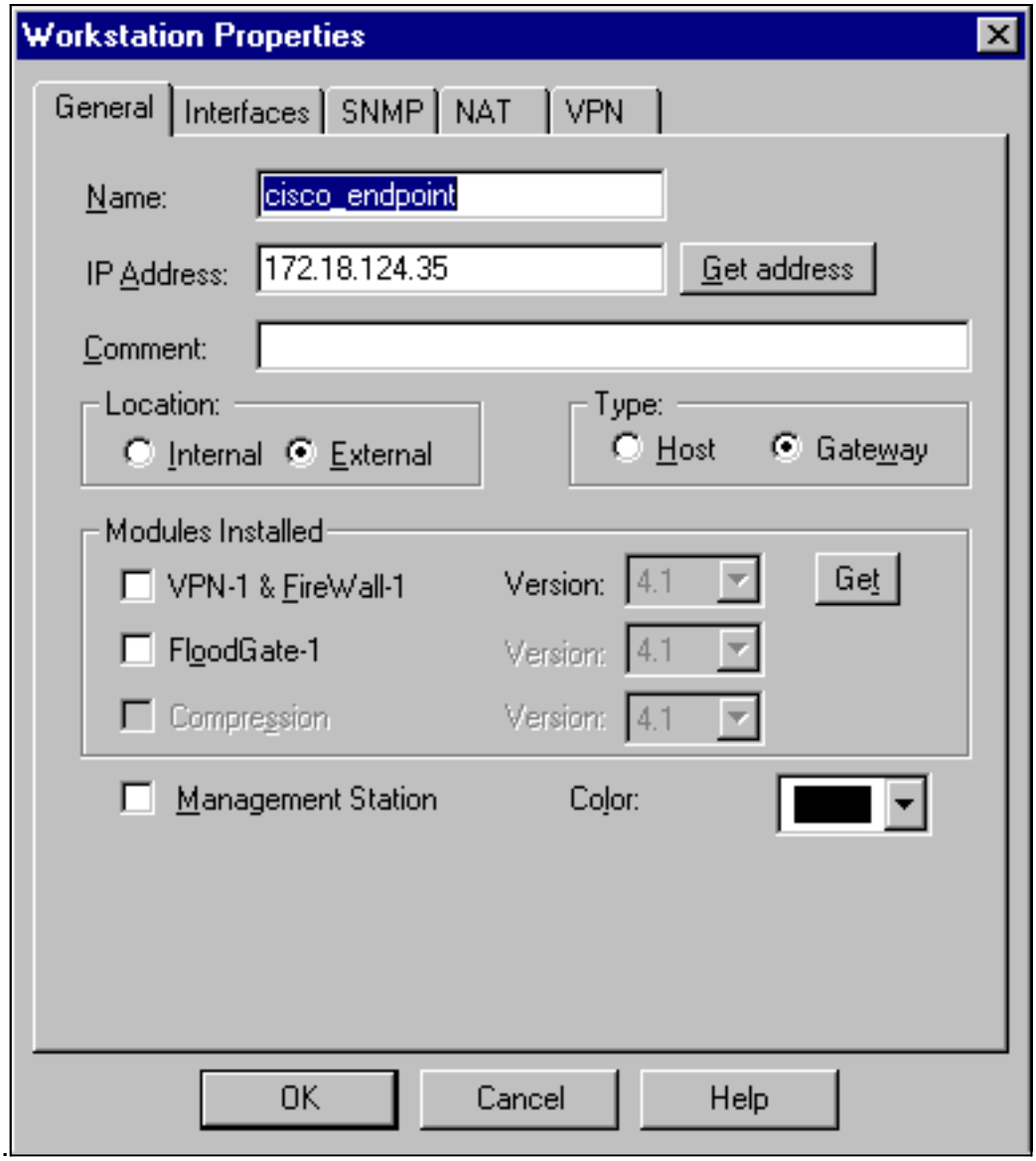
Station:

4. Selecteer **Manager > Netwerkobjecten > Nieuw > Netwerk** om het object voor het externe ("interne_cisco") netwerk achter de PIX te configureren.Dit moet overeenkomen met het bron- (eerste) netwerk in deze PIX-opdracht: **toegangslijst 115 vergunning ip 192.168.1.0 255.255.255.0 10.32.50.0**



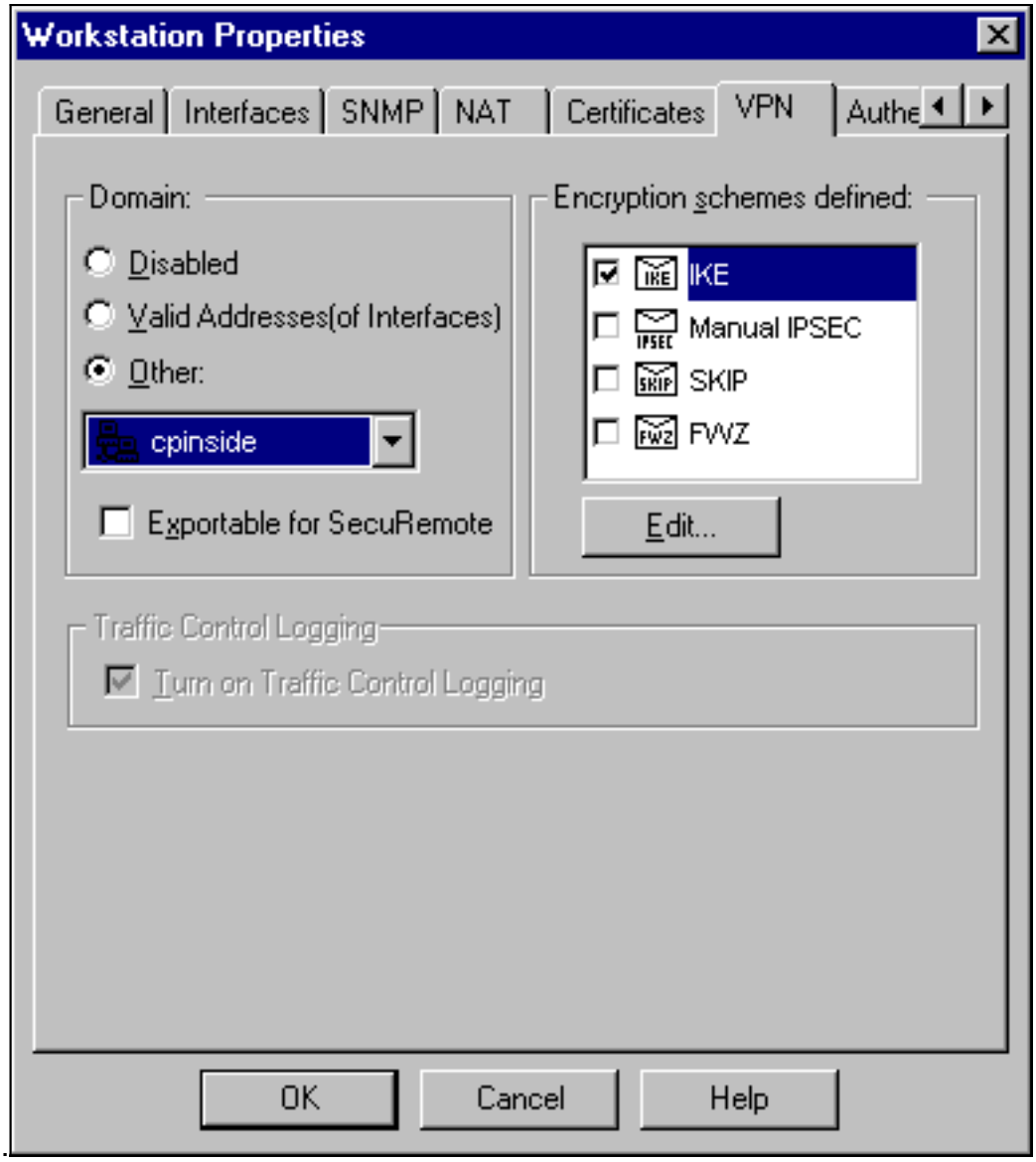
255.255.255.0

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



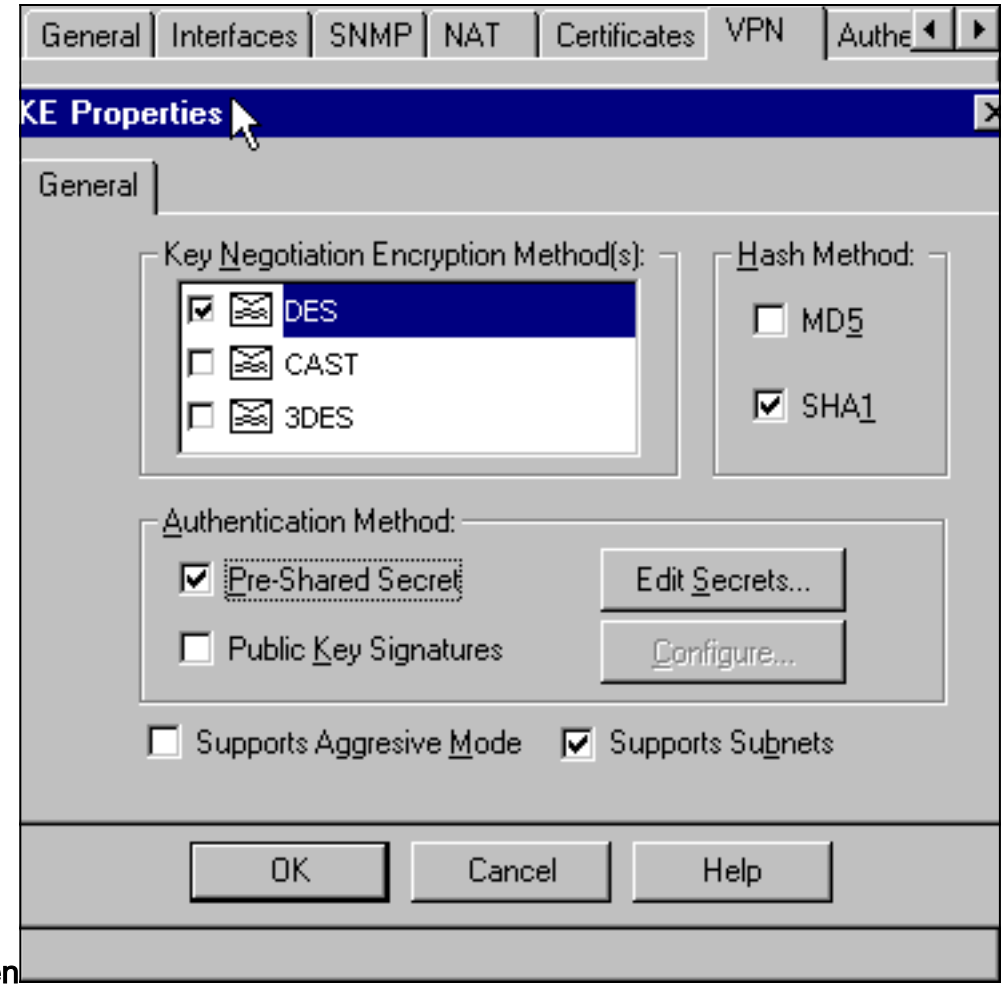
1/FireWall-1.

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



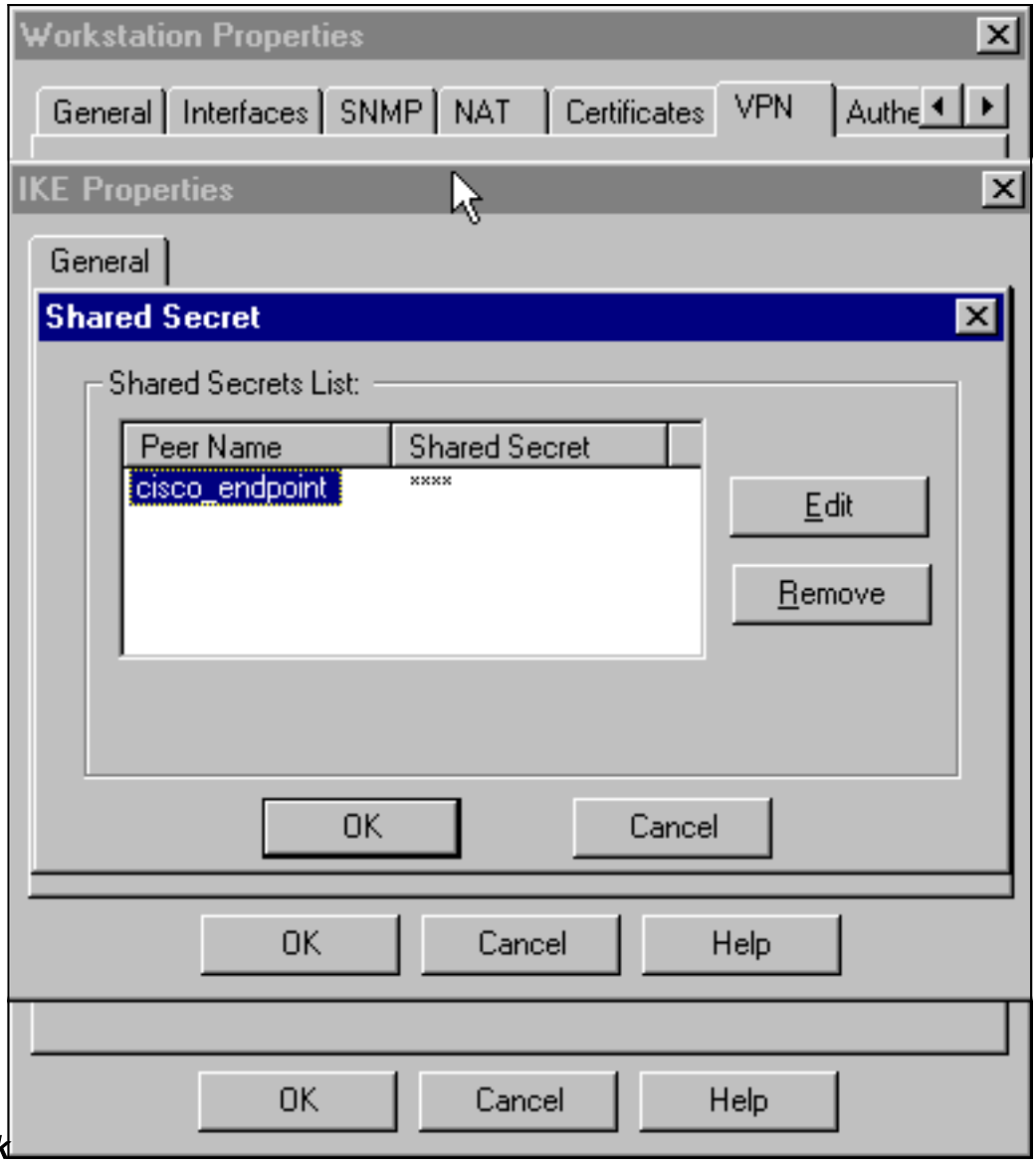
Bewerken.

7. Wijzig de IKE-eigenschappen voor DES-encryptie om met deze opdracht akkoord te gaan:**isakmp-beleid # encryptie**
8. Wijzig de IKE-eigenschappen in SHA1-hashing om met deze opdracht akkoord te gaan:**isakmp-beleid # hash sha**Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Selecteer het selectieteken **Ondersteunt**.Selecteer onder Verificatiemethode het **voorgedeelde** selectieteken. Dit is het eens met deze opdracht:**isakmp-beleid # authenticatie**



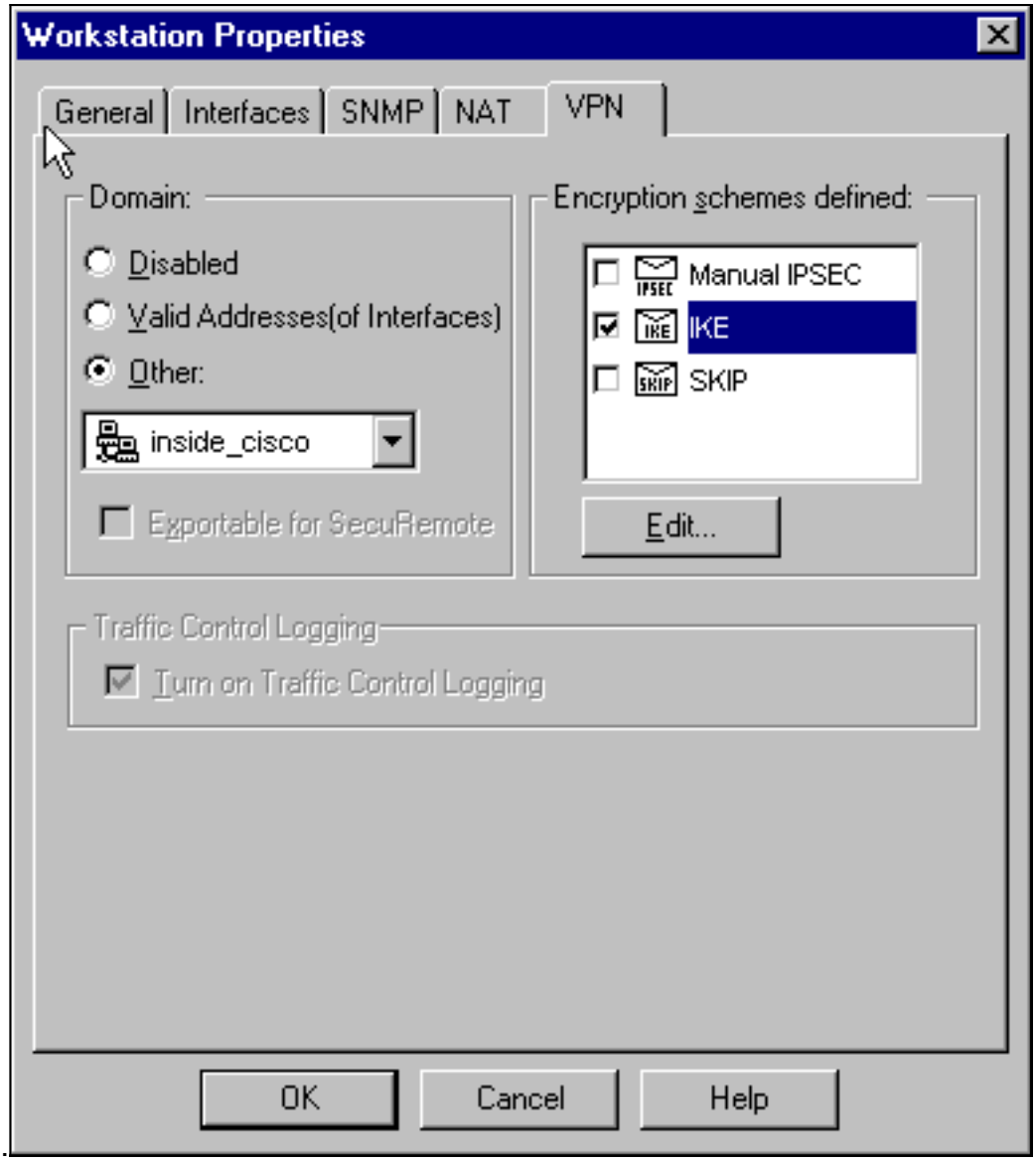
vóór aandelen

9. Klik op **Geheimen bewerken** om de voorgedeelde toets in te stellen om met de PIX-opdracht akkoord te gaan:**isakmp key *key* address netmask**



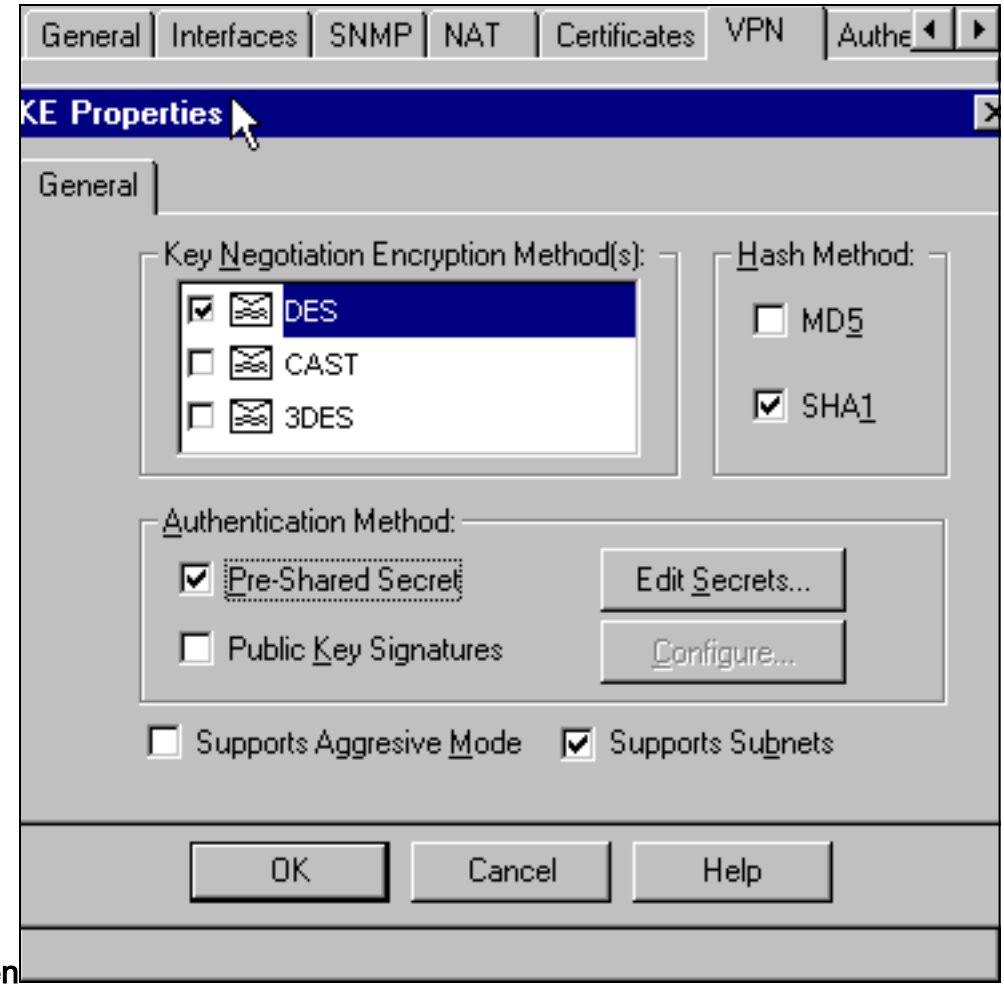
netmask

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



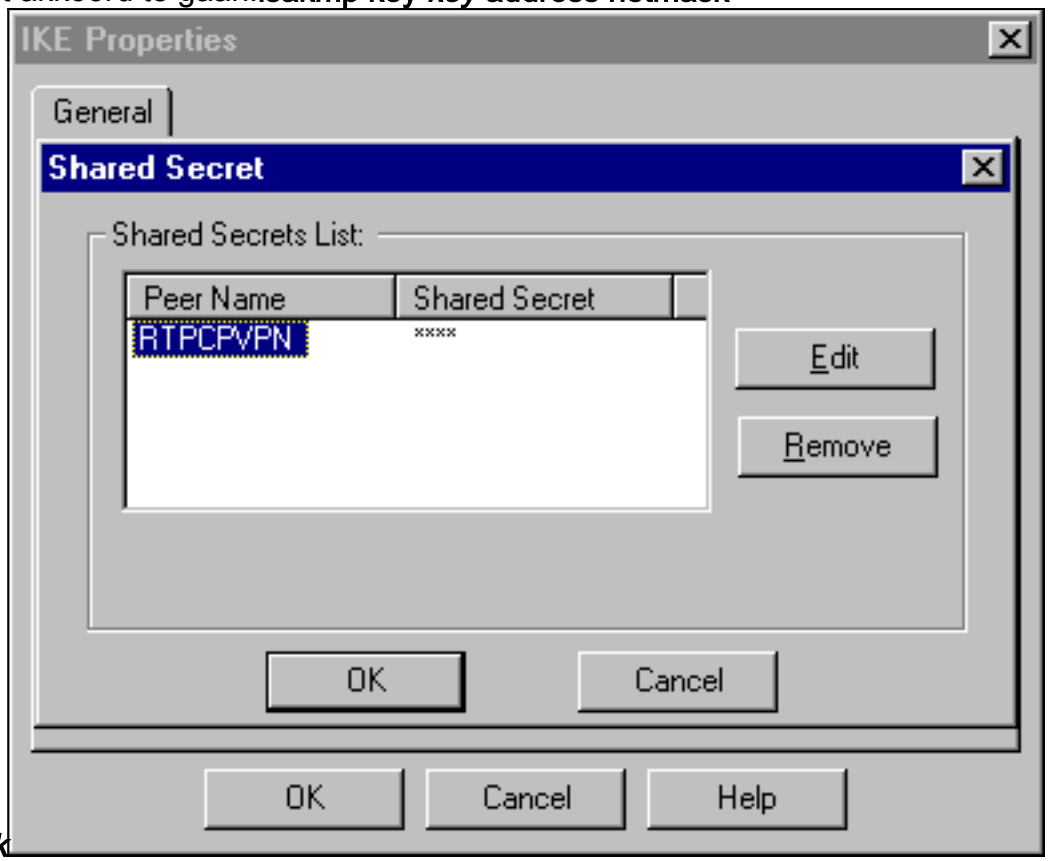
Bewerken.

11. Wijzig de IKE-eigenschappen DES-encryptie om met deze opdracht akkoord te gaan:**isakmp-beleid # encryptie**
12. Wijzig de IKE-eigenschappen in SHA1-hashing om met deze opdracht akkoord te gaan:**crypto isakmp-beleid #hash sha**Wijzig deze instellingen:De selectie van de **aggregatieroute** opheffen.Selecteer het selectieteken **Ondersteunt**.Selecteer onder Verificatiemethode het **voorgedeelde** vakje **Geheime**. Deze actie is met deze opdracht akkoord:**isakmp-beleid # authenticatie vóór**



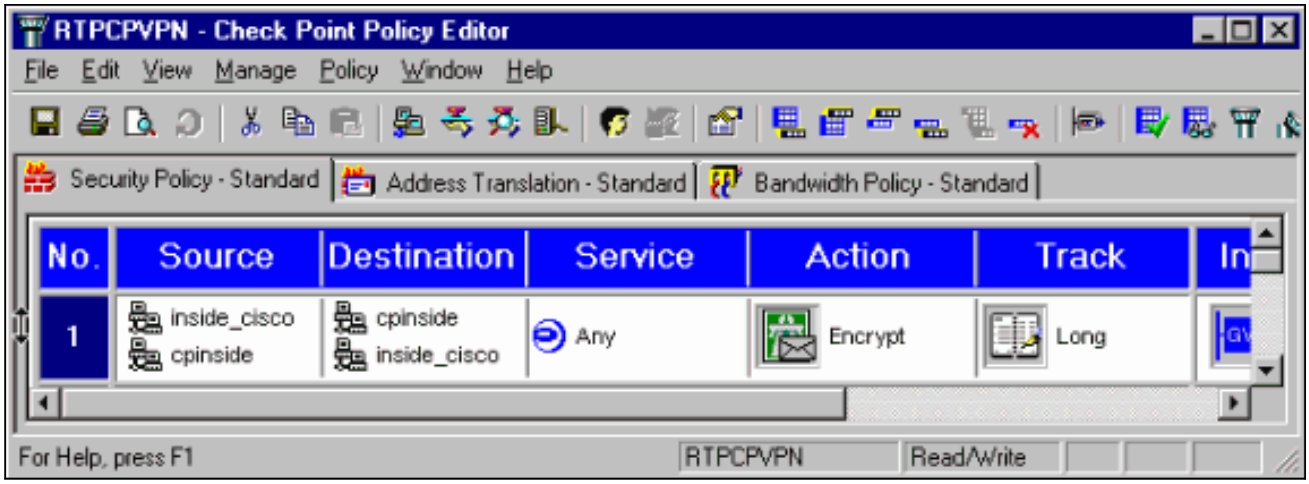
aandelen

13. Klik op **Bewerken geheimen** om de voorgedeelde toets in te stellen om met deze PIX-opdracht akkoord te gaan:**isakmp key *key* address netmask**

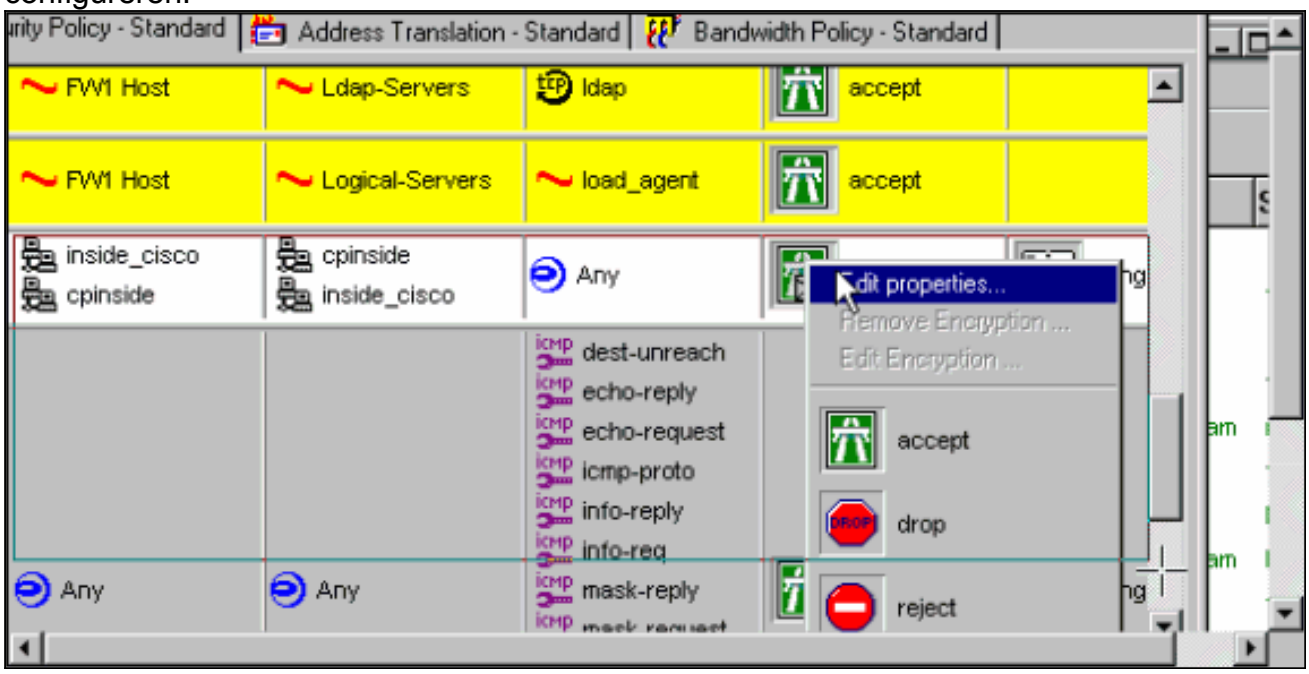


netmask

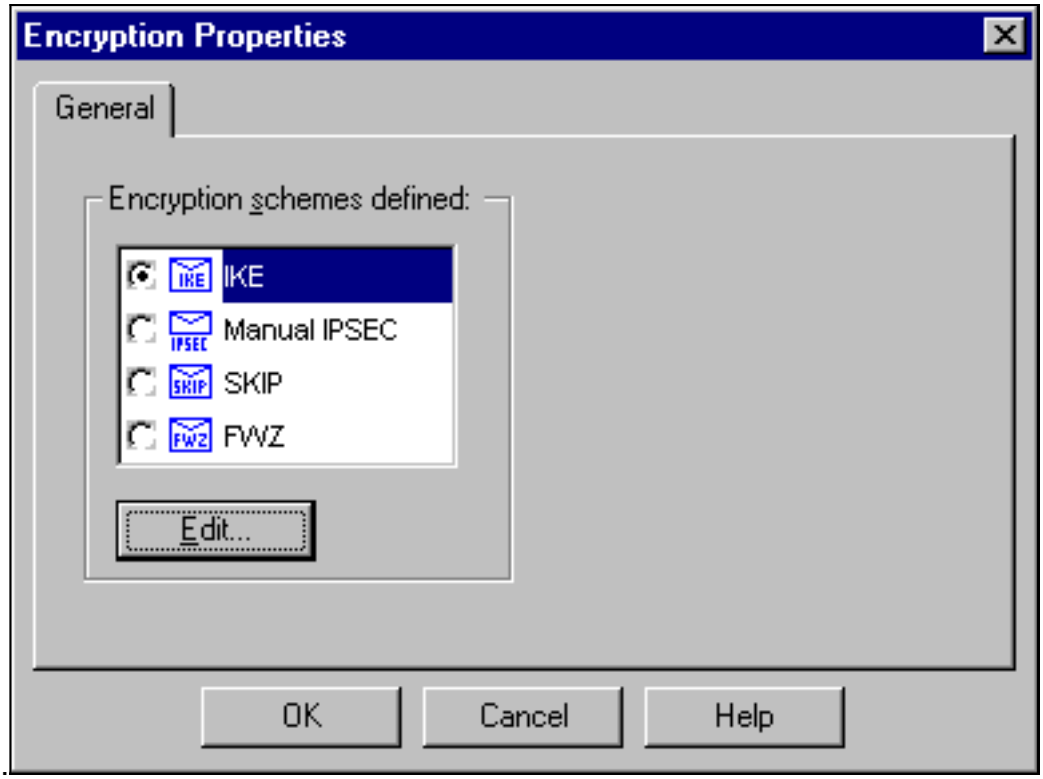
14. Typ in het venster Policy Editor een regel met zowel Bron als Destination als "interne_cisco" en "cpinto" (bidirectioneel). **Service=Any** instellen, **Action=Encrypt** en **Track=Long**.



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

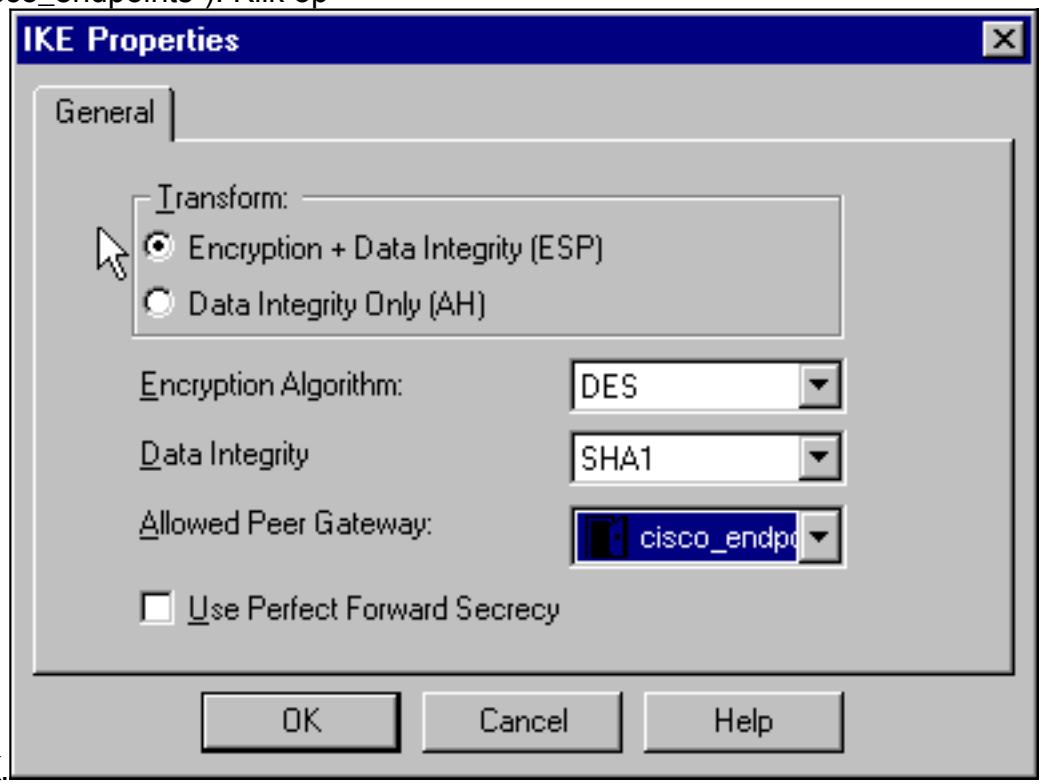


16. Selecteer **IKE** en klik vervolgens op



Bewerken.

17. Wijzig deze eigenschappen in het scherm IKE Properties om het eens te worden met de PIX IPSec transformaties in deze opdracht:**crypto ipsec transformatie myset esp-des esp-sha-hmac**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 PIX-poort zijn (aangeduid als "cisco_endpoints"). Klik op



OK.

18. Nadat het checkpoint is ingesteld, selecteert u **Policy** > **Install** in het menu Selectieteken zodat de wijzigingen van kracht kunnen worden.

Opdrachten zuiveren, weergeven en wissen

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

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.**

Voordat u **debug-**opdrachten geeft, raadpleegt u Belangrijke informatie over debug Commands.

Cisco PIX-firewall

- **debug van crypto motor**—Display debug-berichten over crypto motoren, die encryptie en decryptie uitvoeren.
- **debug crypto isakmp**-Display berichten over IKE gebeurtenissen.
- **debug van crypto ipsec**-weergave van IPSec-gebeurtenissen.
- **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 veiligheidsassociaties worden gebruikt.
- **duidelijke crypto isakmp sa** — (vanaf de configuratiemodus) wissen alle actieve IKE verbindingen.
- **duidelijke crypto ipsec sa**— (van configuratiewijze) Verwijdert alle IPSec security associaties.

Selectieteken:

Omdat de tracering voor lang is ingesteld in het venster Policy Editor dat in stap 14 is getoond, wordt het ontkende verkeer in het Log Viewer rood weergegeven. Een meer breedgedragen debug kan worden verkregen door in te voeren:

```
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.

U kunt SA's op Selectieteken met deze opdrachten 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
```

En **ja** antwoorden op The Are You Sure? .

Problemen oplossen

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

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 crypto ACL op de PIX niet wordt gevormd om te passen, zal de tunnel waarschijnlijk mislukken. 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.

Monster debug-uitvoer van PIX

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
cisco_endpoint# term mon
cisco_endpoint#
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
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-SHA
ISAKMP (0): atts are acceptable.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

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 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= 172.18.124.35, 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= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
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= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR2303: 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= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
    Crypto map tag: rtpmap, 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): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 172.18.124.157
  PERMIT, flags={origin_is_acl,}
 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0,
 #pkts decompress failed: 0 #send errors 0, #recv errors 0

  local crypto endpt.: 172.18.124.35,
  remote crypto endpt.: 172.18.124.157
  path mtu 1500, ipsec overhead 0, media mtu 1500
  current outbound spi: 0

  inbound esp sas:

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:

  outbound ah sas:

  outbound pcp sas:

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: 4, #pkts encrypt: 4, #pkts digest 4
 #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
 #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, ipsec overhead 56, media mtu 1500
  current outbound spi: ebc8c823

  inbound esp sas:
   spi: 0x9d71f29c(2641490588)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 3, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0xebc8c823(3955804195)
     transform: esp-des esp-sha-hmac ,
     in use settings ={Tunnel, }
     slot: 0, conn id: 4, crypto map: rtpmap
     sa timing: remaining key lifetime (k/sec): (4607999/28777)
     IV size: 8 bytes
     replay detection support: Y

  outbound ah sas:

  outbound pcp sas:
```

```
cisco_endpoint# sho cry is sa
        dst             src          state     pending    created
  172.18.124.157   172.18.124.35     QM_IDLE         0          2
```

Gerelateerde informatie

- PIX-ondersteuningspagina
- PIX-opdracht
- Verzoeken om opmerkingen (RFC's)
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- PIX 5.2: IPsec configureren
- PIX 5.3: IPsec configureren
- IPsec-ondersteuningspagina
- Technische ondersteuning - Cisco-systemen