

Configureer een IPSec-tunnels tussen een checkpoint-NG en een router

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[Cisco 1751 VPN-router configureren](#)

[Het selectieteken configureren](#)

[Verifiëren](#)

[Controleer de Cisco-router](#)

[Controleer controlepunt NG](#)

[Problemen oplossen](#)

[Cisco-router](#)

[Gerelateerde informatie](#)

Inleiding

Dit document toont aan hoe u een IPSec-tunnel met pre-gedeelde sleutels kunt vormen om zich aan twee privé netwerken aan te sluiten:

- Het privénetwerk 172.16.15.x binnen de router.
- Het privé-netwerk van 192.168.10.x binnen ^{Checkpoint™} Next Generation (NG).

Voorwaarden

Vereisten

De in dit document geschetste procedures zijn gebaseerd op deze veronderstellingen.

- Het basisbeleid voor ^{checkpoint™} wordt vastgesteld.
- Alle toegang, NAT-adresomzetting (Network Address Translation) en routinginstellingen worden geconfigureerd.
- Verkeer van binnen de router en binnen het ^{checkpoint™} naar het internet.

Gebruikte componenten

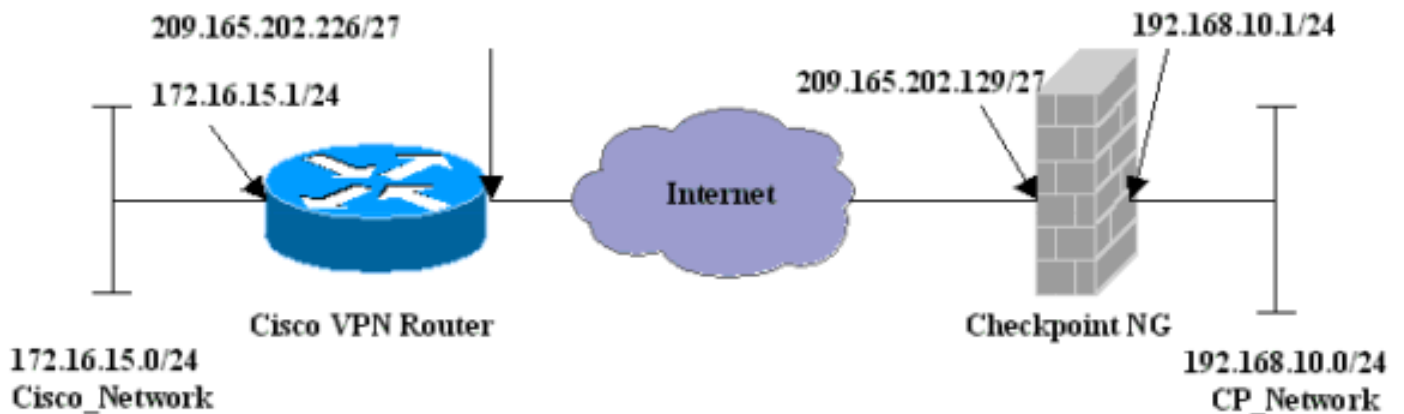
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 1751 router
- Cisco IOS®-software (C1700-K9O3SY7-M), versie 12.2(8)T4, RELEASE-SOFTWARE (FC1)
- Checkpoint™ NG-gebouw 50027

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.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

Raadpleeg voor meer informatie over documentconventies de [technische Tips](#) van [Cisco](#).

Cisco 1751 VPN-router configureren

Cisco VPN 1751 router

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
hostname sv1-6
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip domain-lookup
ip audit notify log
ip audit po max-events 100
!--- Internet Key Exchange (IKE) configuration. crypto
isakmp policy 1
    encr 3des
    hash md5
    authentication pre-share
```

```

group 2
lifetime 1800
!--- IPsec configuration. crypto isakmp key aptrules
address 209.165.202.129
!
crypto ipsec transform-set aptset esp-3des esp-md5-hmac
!
crypto map aptmap 1 ipsec-isakmp
set peer 209.165.202.129
set transform-set aptset
match address 110
!
interface Ethernet0/0
ip address 209.165.202.226 255.255.255.224
ip nat outside
half-duplex
crypto map aptmap
!
interface FastEthernet0/0
ip address 172.16.15.1 255.255.255.0
ip nat inside
speed auto
!--- NAT configuration. ip nat inside source route-map
nonat interface Ethernet0/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.225
no ip http server
ip pim bidir-enable
!--- Encryption match address access list. access-list
110 permit ip 172.16.15.0 0.0.0.255 192.168.10.0
0.0.0.255
!--- NAT access list. access-list 120 deny ip
172.16.15.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 120 permit ip 172.16.15.0 0.0.0.255 any
route-map nonat permit 10
match ip address 120
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
password cisco
login
end

```

[Het selectieteken configureren](#)

Checkpoint™ NG is een op het object gerichte configuratie. Netwerkojecten en -regels worden gedefinieerd om het beleid op te stellen dat betrekking heeft op de VPN-configuratie. Dit beleid wordt vervolgens geïnstalleerd met behulp van de Checkpoint™ NG Policy Editor om de Checkpoint™ NG-kant van de VPN-configuratie te voltooien.

1. Maak Cisco network subtype en Checkpoint™ NG network subtype als netwerkojecten. Dit is wat versleuteld is. Als u de objecten wilt maken, selecteert u **Bewerken > Netwerkojecten** en vervolgens selecteert u **Nieuw > Netwerk**. Voer de juiste netwerkinformatie in en klik vervolgens op **OK**. Deze voorbeelden tonen een set van objecten die CP_Network en Cisco_Network worden

Network Properties - CP_Network

General NAT

Name: CP_Network

IP Address: 192.168.10.0

Net Mask: 255.255.255.0

Comment:

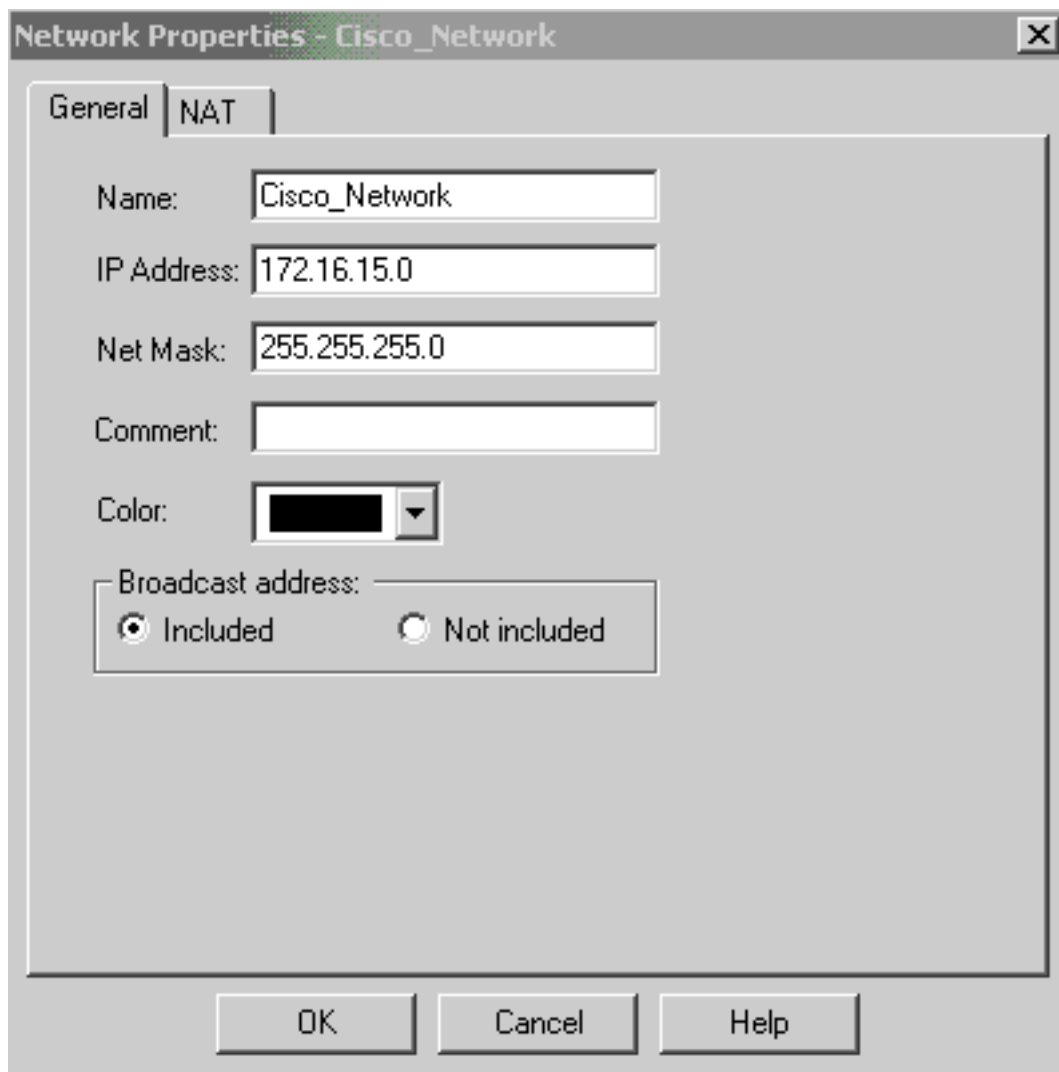
Color:

Broadcast address:

Included Not included

OK Cancel Help

genoemd.



2. Maak de objecten Cisco_Router en Checkpoint_NG als werkstation objecten. Dit zijn de VPN-apparaten. Als u de objecten wilt maken, selecteert u **Bewerken > Netwerkobjecten** en vervolgens selecteert u **Nieuw > Werkstation**. Let op dat u het object ^{Checkpoint™} NG-werkstation kunt gebruiken dat is gemaakt tijdens de eerste ^{checkpoint™}-instelling. Selecteer de opties om het werkstation in te stellen als **Gateway** en **Interoperable VPN-apparaat**. Deze voorbeelden tonen een set van objecten die chef en Cisco_Router worden genoemd.

General

Topology

NAT

VPN

Authentication

Management

+ Advanced

General

Name: chef

IP Address: 209.165.202.129

Get address

Comment: CP_Server

Color: Type: Host Gateway

Check Point Products

 Check Point products installed: Version NG

- 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

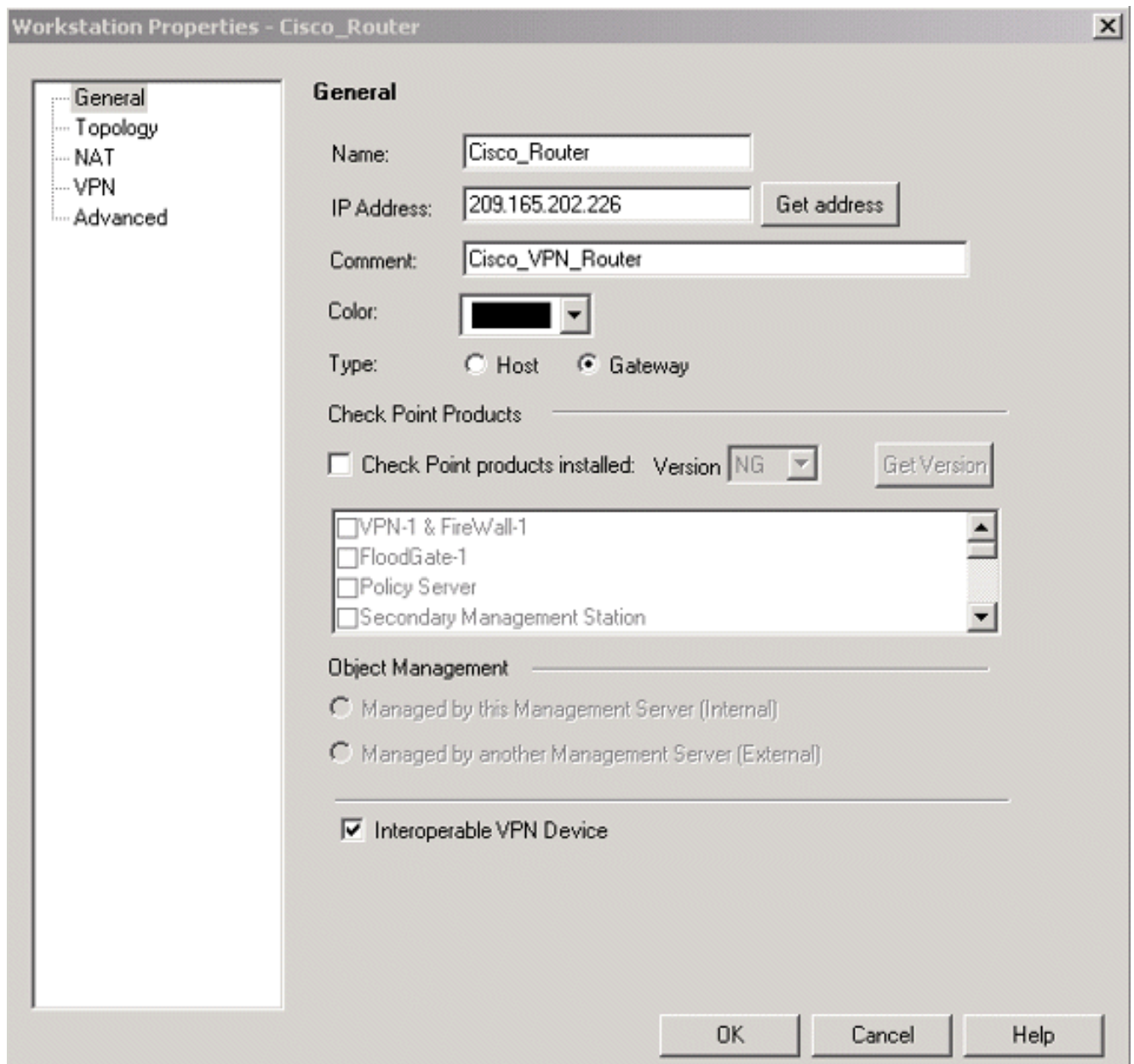
DN: cn=cp_mgmt,o=chef.6h9tua

 Interoperable VPN Device

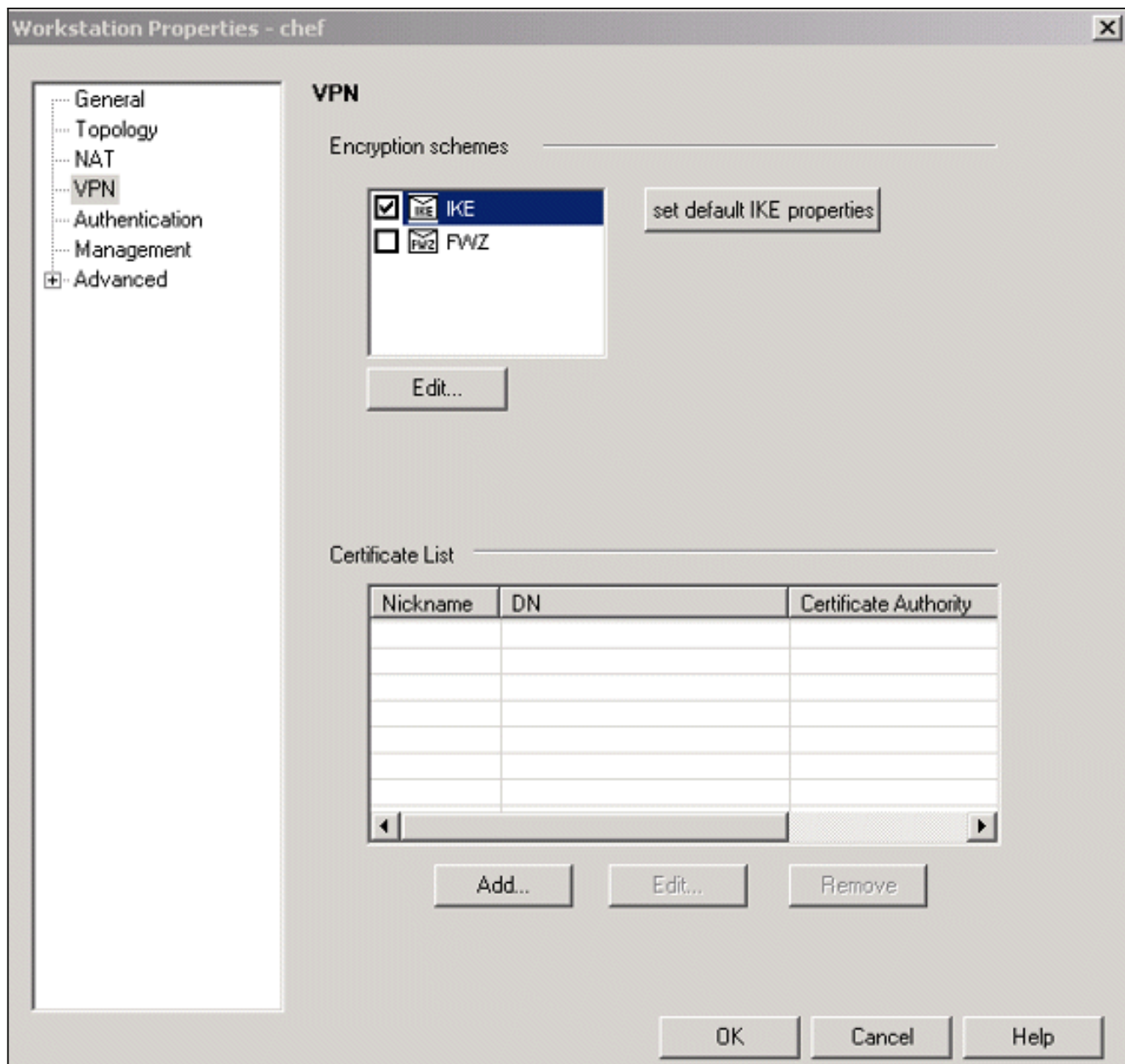
OK

Cancel

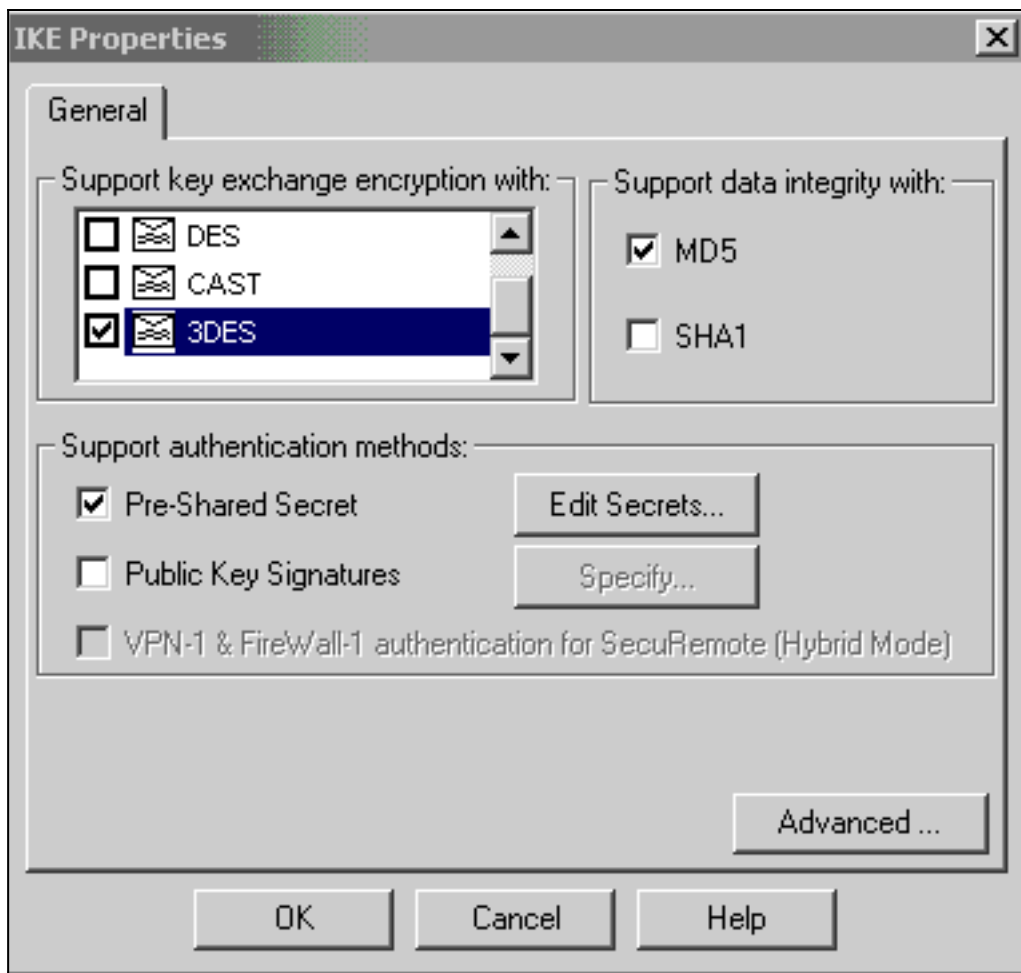
Help



3. Configureer de IKE in het tabblad VPN en klik vervolgens op **Bewerken**.

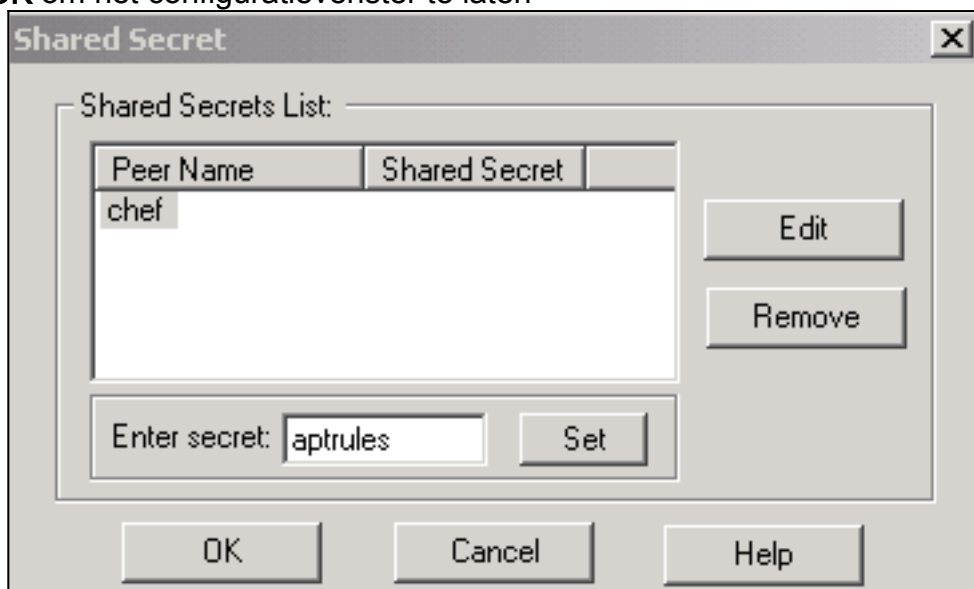


4. Configureer het uitwisselingsbeleid en klik op **Geheimen**



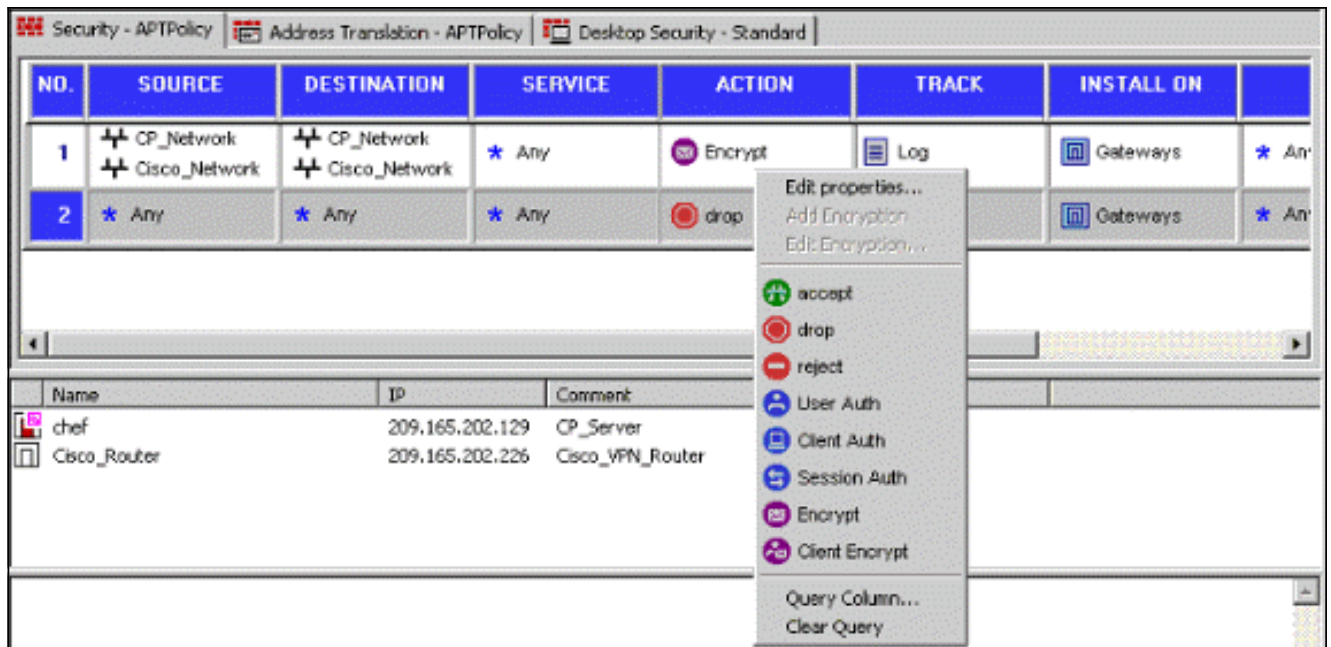
bewerken.

5. Stel de vooraf gedeelde toetsen in die gebruikt moeten worden en klik vervolgens meerdere malen op **OK** om het configuratievenster te laten

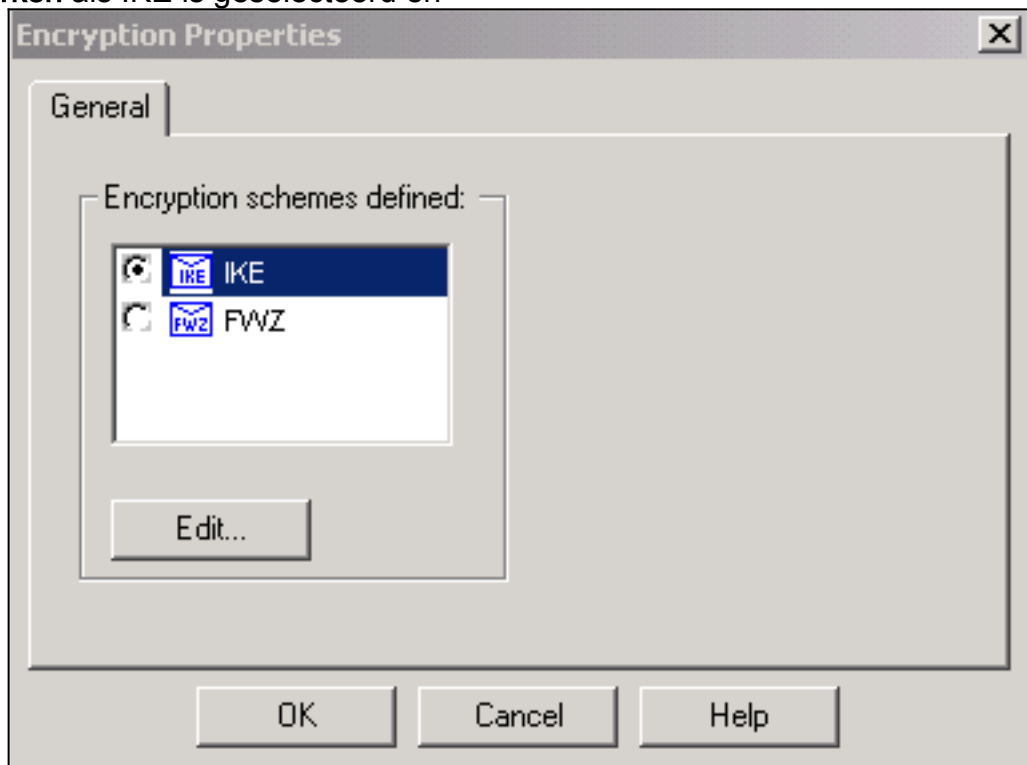


verdwijnen.

6. Selecteer **Regels > Toevoegen Regels > Boven** om de coderingsregels voor het beleid te configureren. De regel bovenaan is de eerste regel die vóór een andere regel wordt uitgevoerd die encryptie kan omzeilen. Configureer de bron en de bestemming om de CP_Network en de Cisco_Network in te sluiten, zoals hier wordt getoond. Nadat u het gedeelte Encrypt Action van de regel hebt toegevoegd, klikt u met de rechtermuisknop op **Actie** en vervolgens selecteert u **Eigenschappen bewerken**.

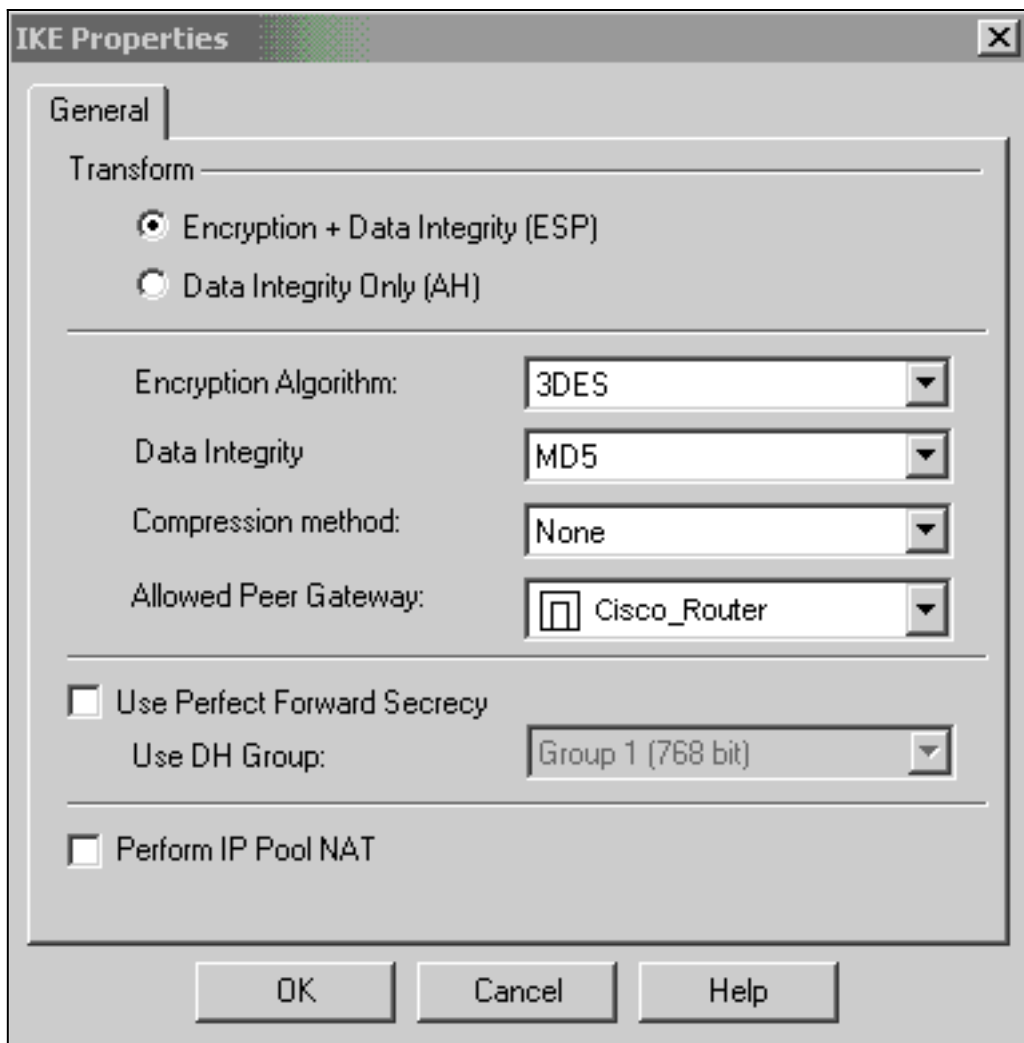


7. Klik op **Bewerken** als IKE is geselecteerd en



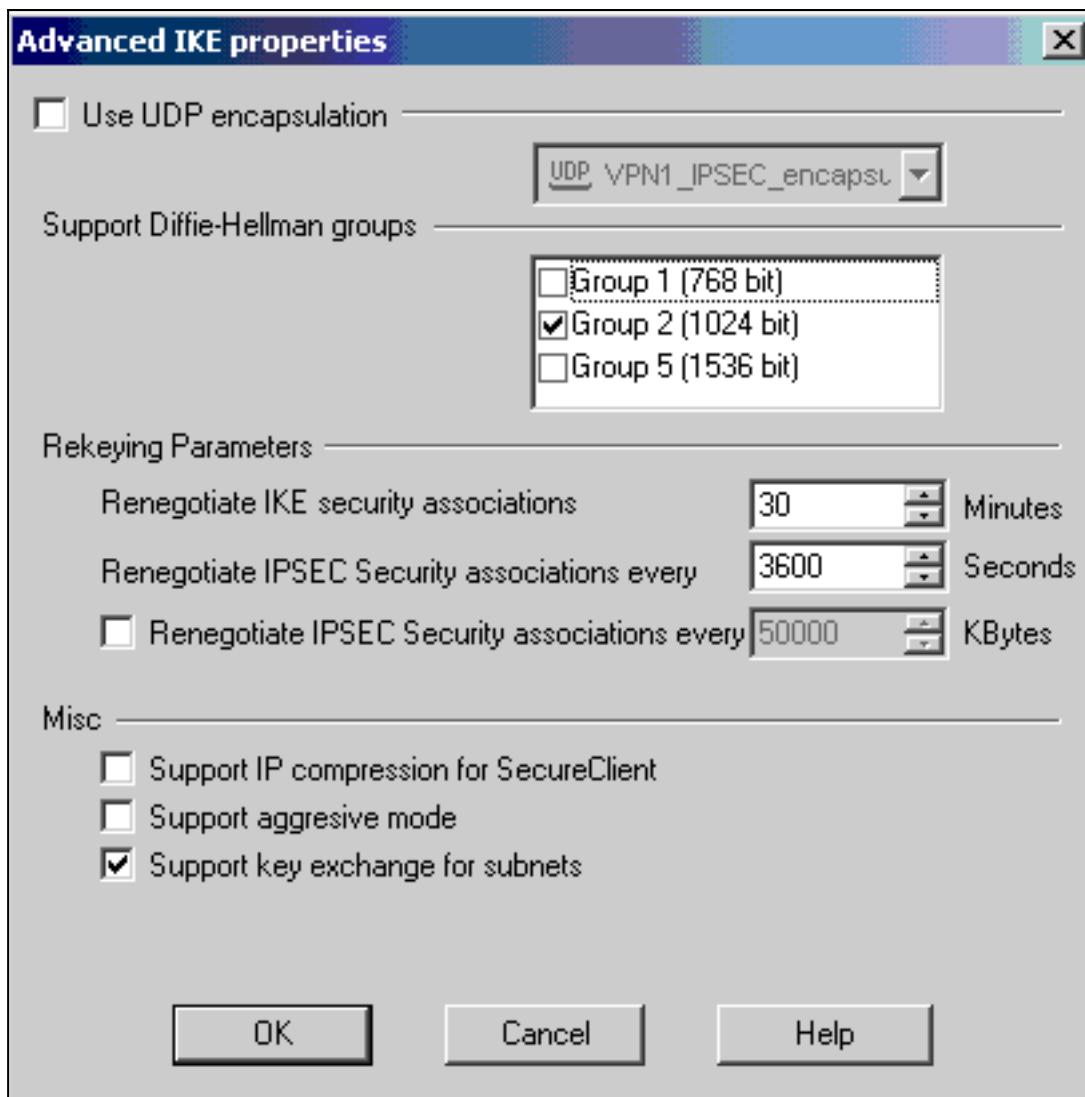
geselecteerd.

8. Bevestig de IKE-



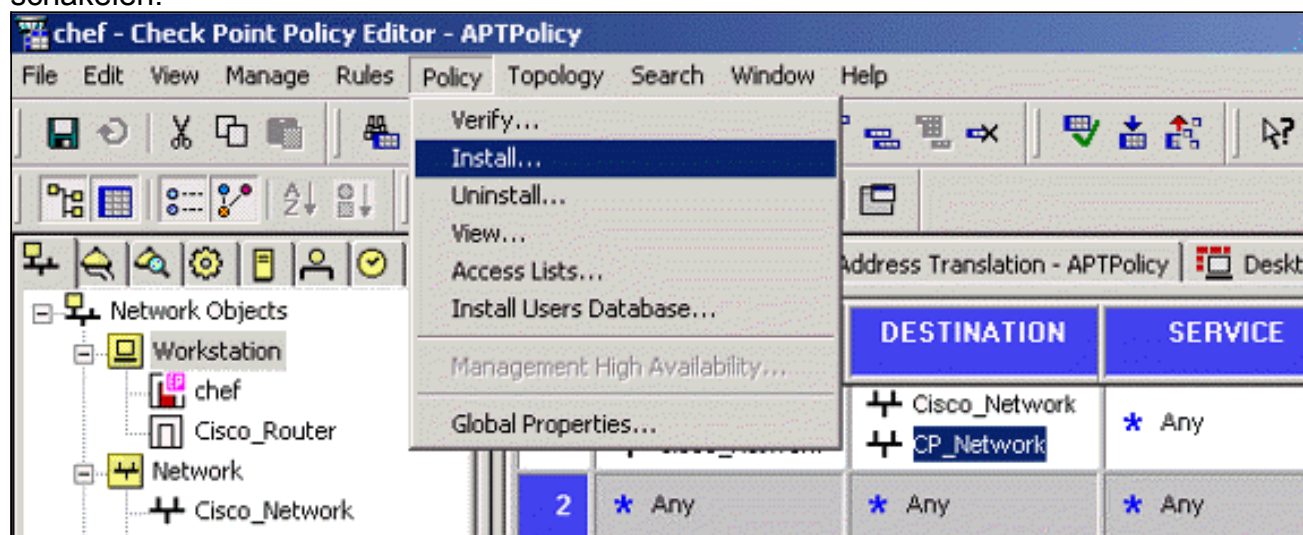
configuratie.

9. Een van de belangrijkste kwesties met het runnen van VPN tussen Cisco apparaten en andere IPSec apparaten is de zeer belangrijke heronderhandeling van de Uitwisseling. Zorg ervoor dat de instelling voor de IKE-uitwisseling op de Cisco-router precies hetzelfde is als de instelling die is ingesteld op ^{Checkpoint™} NG. **Toelichting:** De werkelijke waarde van deze parameter is afhankelijk van uw specifieke zakelijke beveiligingsbeleid. In dit voorbeeld, is de [IKE configuratie op de router](#) ingesteld op 30 minuten met het **leven 1800** bevel. Dezelfde waarde moet op ^{checkpoint™} NG worden ingesteld. Als u deze waarde op ^{Checkpoint™} op NG wilt instellen, selecteert u **Netwerkwobject beheren**, selecteert u het object ^{Checkpoint™} en klikt u op **Bewerken**. Selecteer vervolgens **VPN** en bewerk de IKE. Selecteer **Advance** en stel de rekenparameters in. Nadat u de sleuteluitwisseling voor het netwerkwobject ^{Checkpoint™} NG vormt, voert u dezelfde configuratie uit van de Key Exchange-onderhandeling voor het netwerkwobject Cisco_Router. **Opmerking:** Zorg ervoor dat u de juiste Diffie-Hellman groep hebt geselecteerd om die op de router te

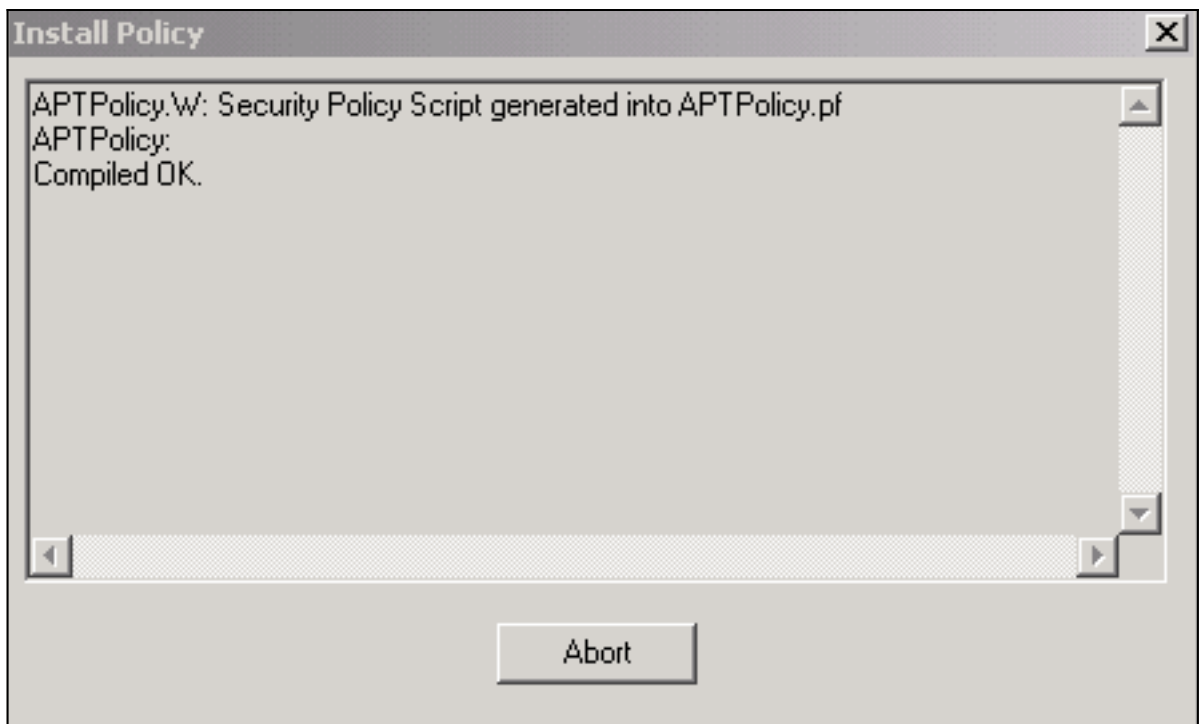


matchen.

10. De beleidsconfiguratie is voltooid. Sla het beleid op en selecteer **Policy > Install** om dit in te schakelen.

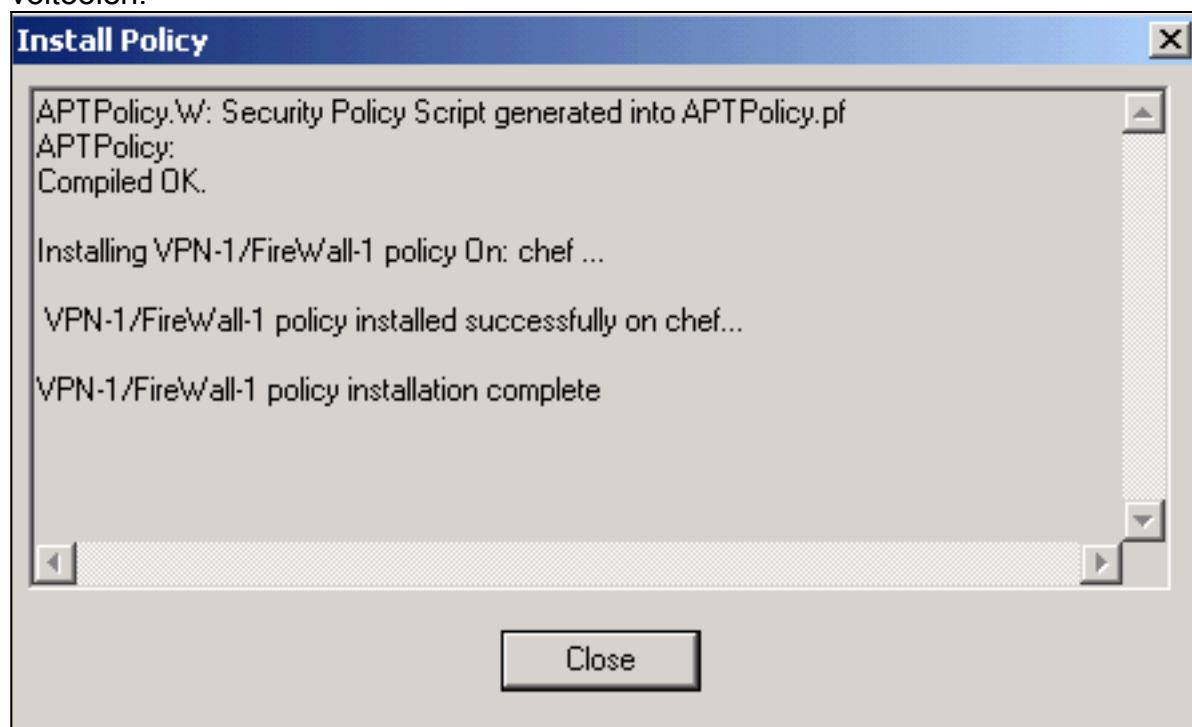


Het installatievenster toont voortgangsnoden bij het samenstellen van het



beleid.

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



[Verifiëren](#)

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

[Controleer de Cisco-router](#)

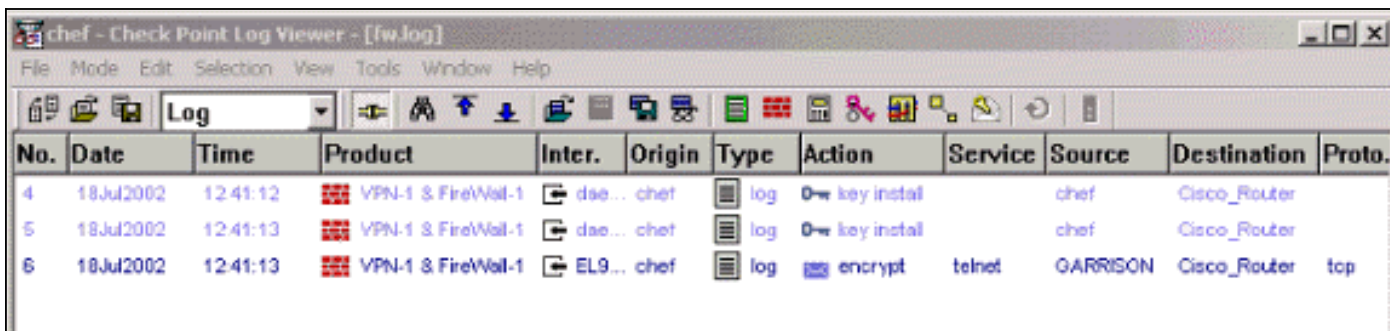
Bepaalde opdrachten met **show** worden ondersteund door de tool [Output Interpreter \(alleen voor geregistreerde klanten\)](#). Hiermee kunt u een analyse van de output van opdrachten met **show**

genereren.

- toon `crypto isakmp sa`-Toont alle huidige IKE security associaties (SAs) bij een peer.
- Laat `crypto ipsec sa`-displays de instellingen die worden gebruikt door de huidige SAs.

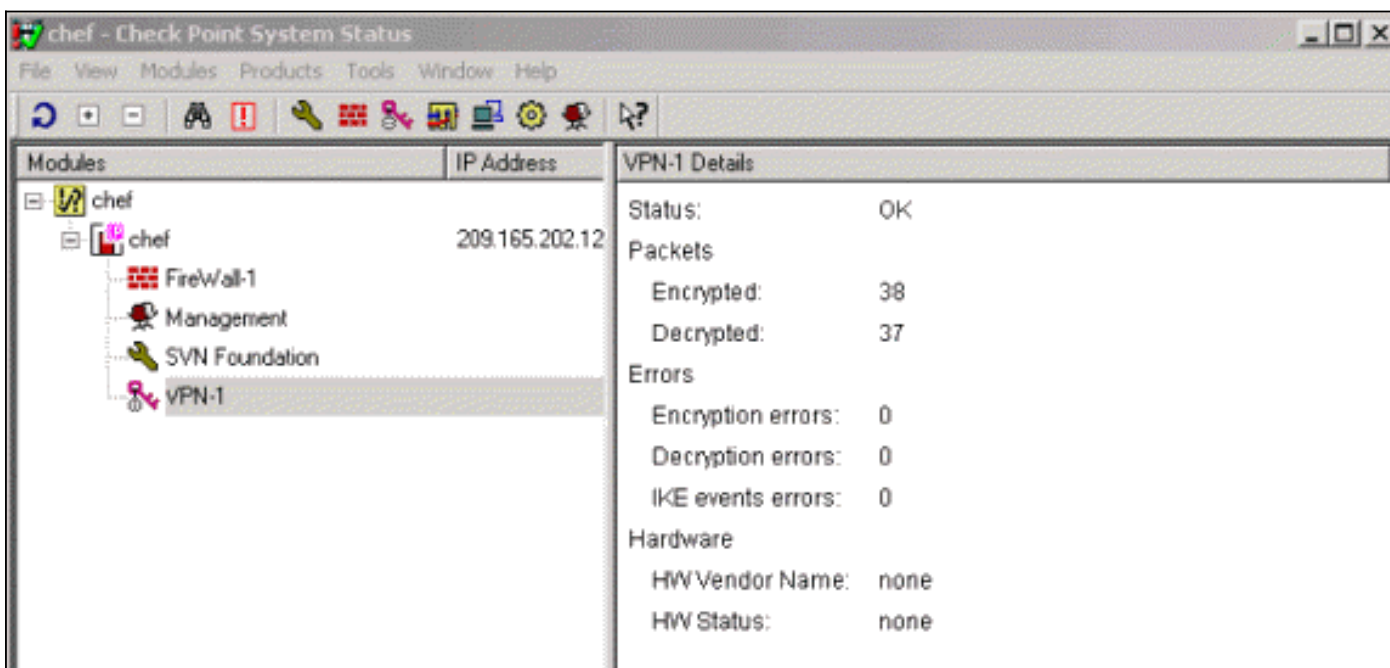
Controleer controlepunt NG

Als u de logbestanden wilt weergeven, selecteert u **Windows > Log Viewer**.



No.	Date	Time	Product	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
4	18Jul2002	12:41:12	VPN-1 & FireWall-1	dse...	chef	log	key instal		chef	Cisco_Router	
5	18Jul2002	12:41:13	VPN-1 & FireWall-1	dae...	chef	log	key instal		chef	Cisco_Router	
6	18Jul2002	12:41:13	VPN-1 & FireWall-1	EL9...	chef	log	encrypt	telnet	GARRISON	Cisco_Router	tcp

Als u de systeemstatus wilt weergeven, selecteert u **Venster > Systeemstatus**.



Modules	IP Address	VPN-1 Details
chef		Status: OK
chef	209.165.202.12	Packets
FireWall-1		Encrypted: 38
Management		Decrypted: 37
SVN Foundation		Errors
VPN-1		Encryption errors: 0
		Decryption errors: 0
		IKE events errors: 0
		Hardware
		HW Vendor Name: none
		HW Status: none

Problemen oplossen

Cisco-router

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

Raadpleeg voor meer informatie over probleemoplossing de [IP-beveiligingsprobleemoplossing - Opdrachten begrijpen en gebruiken](#).

Opmerking: Voordat u `debug`-opdrachten afgeeft, raadpleegt u [Belangrijke informatie over Debug Commands](#).

- **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** — ontruimt alle IPSec SAs.

Succesvol debug Log in

```

18:05:32: ISAKMP (0:0): received packet from
      209.165.202.129 (N) NEW SA
18:05:32: ISAKMP: local port 500, remote port 500
18:05:32: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_READY New State = IKE_R_MM1
18:05:32: ISAKMP (0:1): processing SA payload. message ID = 0
18:05:32: ISAKMP (0:1): processing vendor id payload
18:05:32: ISAKMP (0:1): vendor ID seems Unity/DPD
      but bad major
18:05:32: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:32: ISAKMP (0:1): Checking ISAKMP transform 1
      against priority 1 policy
18:05:32: ISAKMP: encryption 3DES-CBC
18:05:32: ISAKMP: hash MD5
18:05:32: ISAKMP: auth pre-share
18:05:32: ISAKMP: default group 2
18:05:32: ISAKMP: life type in seconds
18:05:32: ISAKMP: life duration (VPI) of 0x0 0x0 0x7 0x8
18:05:32: ISAKMP (0:1): atts are acceptable. Next payload is 0
18:05:33: ISAKMP (0:1): processing vendor id payload
18:05:33: ISAKMP (0:1): vendor ID seems Unity/DPD but bad major
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM1 New State = IKE_R_MM1
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM1 New State = IKE_R_MM2
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
      MM_SA_SETUP
18:05:33: ISAKMP (0:1): Input = IKE_MSG_FROM_PEER,
      IKE_MM_EXCH
Old State = IKE_R_MM2 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): processing KE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): processing NONCE payload.
      message ID = 0
18:05:33: ISAKMP (0:1): found peer pre-shared key
      matching 209.165.202.129
18:05:33: ISAKMP (0:1): SKEYID state generated
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM3 New State = IKE_R_MM3
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129 (R)
      MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MSG_INTERNAL,
      IKE_PROCESS_COMPLETE
Old State = IKE_R_MM3 New State = IKE_R_MM4
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)

```

MM_KEY_EXCH
18:05:33: ISAKMP (0:1): Input = IKE_MESG_FROM_PEER,
IKE_MM_EXCH
Old State = IKE_R_MM4 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = 0
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = 0
18:05:33: ISAKMP (0:1): SA has been authenticated
with 209.165.202.129
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_MAIN_MODE
Old State = IKE_R_MM5 New State = IKE_R_MM5
18:05:33: ISAKMP (0:1): SA is doing pre-shared key authentication
using id type ID_IPV4_ADDR
18:05:33: ISAKMP (1): ID payload
next-payload : 8
type : 1
protocol : 17
port : 500
length : 8
18:05:33: ISAKMP (1): Total payload length: 12
18:05:33: ISAKMP (0:1): sending packet to 209.165.202.129
(R) QM_IDLE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PROCESS_COMPLETE
Old State = IKE_R_MM5 New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): Input = IKE_MESG_INTERNAL,
IKE_PHASE1_COMPLETE
Old State = IKE_P1_COMPLETE
New State = IKE_P1_COMPLETE
18:05:33: ISAKMP (0:1): received packet from 209.165.202.129 (R)
QM_IDLE
18:05:33: ISAKMP (0:1): processing HASH payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing SA payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): Checking IPSec proposal 1
18:05:33: ISAKMP: transform 1, ESP_3DES
18:05:33: ISAKMP: attributes in transform:
18:05:33: ISAKMP: SA life type in seconds
18:05:33: ISAKMP: SA life duration (VPI) of 0x0 0x0 0xE 0x10
18:05:33: ISAKMP: authenticator is HMAC-MD5
18:05:33: ISAKMP: encaps is 1
18:05:33: ISAKMP (0:1): atts are acceptable.
18:05:33: IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) INBOUND local= 209.165.202.226, remote= 209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_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
18:05:33: ISAKMP (0:1): processing NONCE payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): processing ID payload.
message ID = -1335371103
18:05:33: ISAKMP (0:1): asking for 1 spis from ipsec
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_PEER, IKE_QM_EXCH
Old State = IKE_QM_READY New State = IKE_QM_SPI_STARVE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(spi_response): getting spi 2147492563 for SA

from 209.165.202.226 to 209.165.202.129 for prot 3
18:05:33: ISAKMP: received ke message (2/1)
18:05:33: ISAKMP (0:1): sending packet to
209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Node -1335371103,
Input = IKE_MESG_FROM_IPSEC, IKE_SPI_REPLY
Old State = IKE_QM_SPI_STARVE New State = IKE_QM_R_QM2
18:05:33: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:33: ISAKMP (0:1): Creating IPsec SAs
18:05:33: inbound SA from 209.165.202.129 to 209.165.202.226
(proxy 192.168.10.0 to 172.16.15.0)
18:05:33: has spi 0x800022D3 and conn_id 200 and flags 4
18:05:33: lifetime of 3600 seconds
18:05:33: outbound SA from 209.165.202.226 to 209.165.202.129
(proxy 172.16.15.0 to 192.168.10.0)
18:05:33: has spi -2006413528 and conn_id 201 and flags C
18:05:33: lifetime of 3600 seconds
18:05:33: ISAKMP (0:1): deleting node -1335371103 error
FALSE reason "quick mode done (await())"
18:05:33: ISAKMP (0:1): Node -1335371103, Input = IKE_MESG_FROM_PEER,
IKE_QM_EXCH
Old State = IKE_QM_R_QM2 New State = IKE_QM_PHASE2_COMPLETE
18:05:33: IPSEC(key_engine): got a queue event...
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) INBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,
spi= 0x800022D3(2147492563), conn_id= 200, keysize= 0,
flags= 0x4
18:05:33: IPSEC(initialize_sas): ,
(key eng. msg.) OUTBOUND local= 209.165.202.226,
remote=209.165.202.129,
local_proxy= 172.16.15.0/255.255.255.0/0/0 (type=4),
remote_proxy= 192.168.10.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-md5-hmac ,
lifedur= 3600s and 0kb,

spi= 0x88688F28(2288553768), conn_id= 201, keysize= 0,
flags= 0xC
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.226, sa_prot= 50,
sa_spi= 0x800022D3(2147492563),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 200
18:05:33: IPSEC(create_sa): sa created,
(sa) sa_dest= 209.165.202.129, sa_prot= 50,
sa_spi= 0x88688F28(2288553768),
sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 201
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
18:05:34: ISAKMP (0:1): received packet
from 209.165.202.129 (R) QM_IDLE
18:05:34: ISAKMP (0:1): phase 2 packet is a duplicate
of a previous packet.

```
18:05:34: ISAKMP (0:1): retransmitting due to retransmit phase 2
18:05:34: ISAKMP (0:1): ignoring retransmission, because phase2
node marked dead -1335371103
```

```
sv1-6#show crypto isakmp sa
```

```
dst src state conn-id slot
209.165.202.226 209.165.202.129 QM_IDLE 1 0
```

```
sv1-6#show crypto ipsec sa
```

```
interface: Ethernet0/0
Crypto map tag: aptmap, local addr. 209.165.202.226
local ident (addr/mask/prot/port): (172.16.15.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
current_peer: 209.165.202.129
PERMIT, flags={origin_is_acl,}
#pkts encaps: 21, #pkts encrypt: 21, #pkts digest 21
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify 24
#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.: 209.165.202.226, remote crypto endpt.: 209.165.202.129
path mtu 1500, media mtu 1500
current outbound spi: 88688F28
inbound esp sas:
spi: 0x800022D3(2147492563)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 200, flow_id: 1, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3559)
IV size: 8 bytes
replay detection support: Y
inbound ah sas:
inbound pcp sas:
outbound esp sas:
spi: 0x88688F28(2288553768)
transform: esp-3des esp-md5-hmac ,
in use settings ={Tunnel, }
slot: 0, conn id: 201, flow_id: 2, crypto map: aptmap
sa timing: remaining key lifetime (k/sec): (4607997/3550)
IV size: 8 bytes
replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

```
sv1-6#show crypto engine conn act
```

ID	Interface	IP-	Address	State	Algorithm	Encrypt	Decrypt
1	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	0	0	
200	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	0	24	
201	Ethernet0/0	209.165.202.226	set	HMAC_MD5+3DES_56_C	21	0	

[Gerelateerde informatie](#)

- [IPsec-ondersteuningspagina](#)
- [Technische ondersteuning - Cisco-systemen](#)