IPsec tussen twee IOS-routers met configuratievoorbeeld voor Private Networks

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco IOS router in een site-to-site IPsec VPN met overlappende privé netwerkadressen achter VPN-gateways kunt configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS 3640 routers die softwareversie 12.4 uitvoeren.

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.

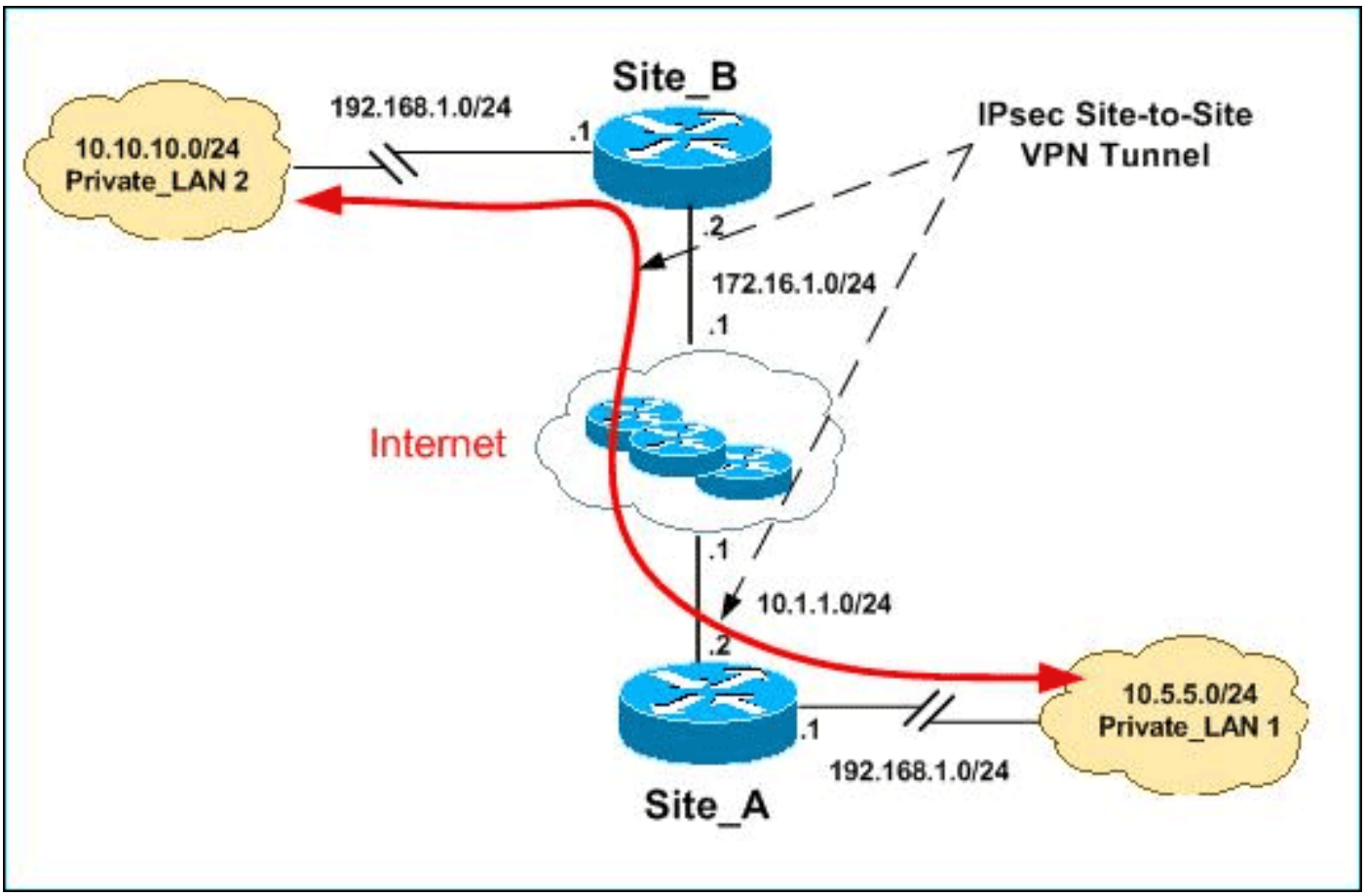
Configureren

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

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Zowel Private_LAN1 als Private_LAN2 hebben een IP-subtype van 192.168.1.0/24. Dit simuleert de overlappende adresruimte achter elke kant van de IPsec-tunnel.

In dit voorbeeld voert de Site_A router een tweerichtingsvertaling uit zodat de twee particuliere LAN's kunnen communiceren via de IPsec-tunnel. De vertaling betekent dat Private_LAN1 "ziet" Private_LAN2 als 10.10.10.0/24 door de IPsec-tunnel en Private_LAN2 "ziet" Private_LAN1 als 10.5.5.0/24 door de IPSec-tunnel.

Configuraties

Dit document gebruikt deze configuraties:

- Configuratie van Site_A router
- Configuratie van Site_A router CLI
- Configuratie van Site_B-router

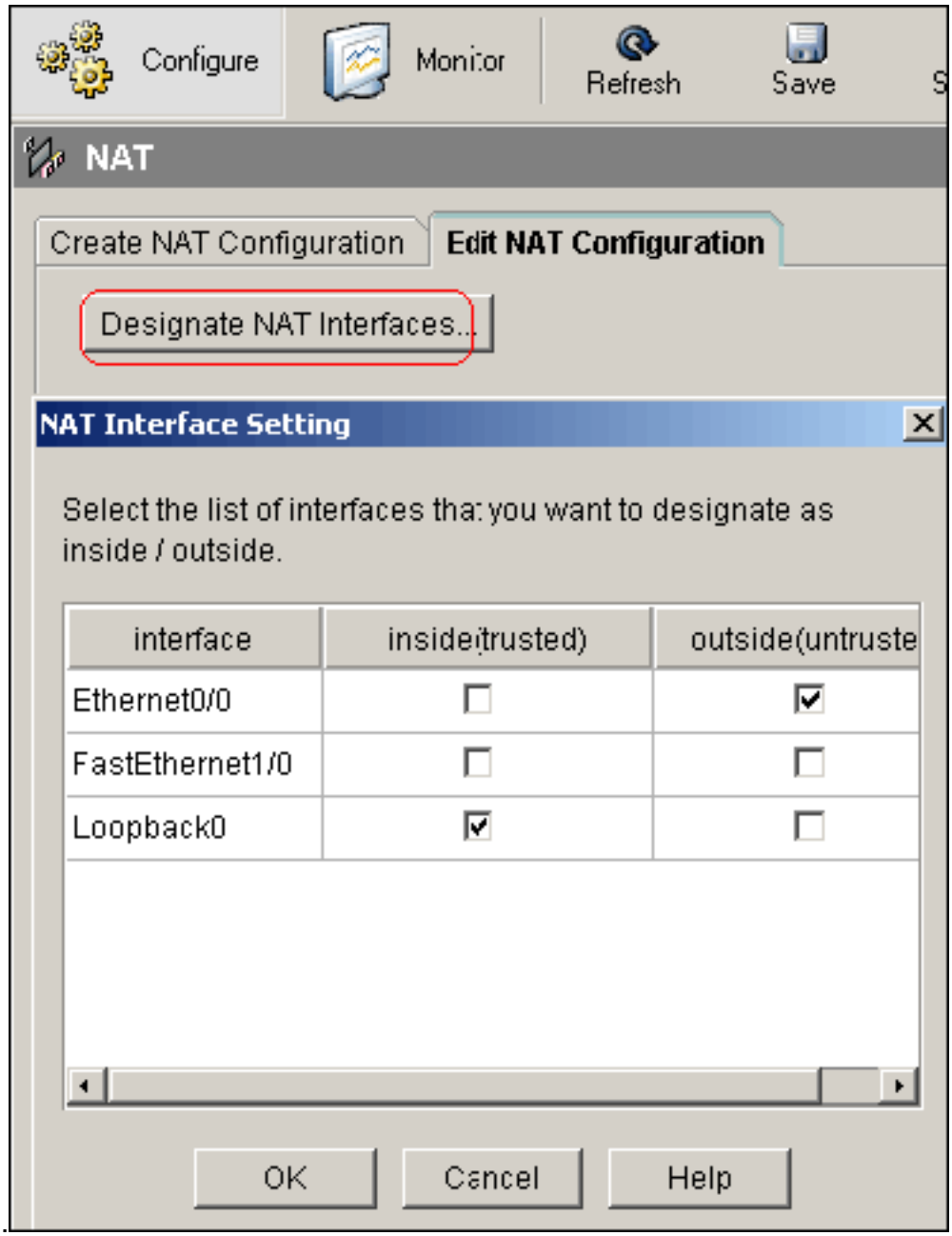
Configuratie van Site_A router

N.B.: Dit document gaat ervan uit dat de router is ingesteld met basisinstellingen zoals de interfaceconfiguratie, enz. Raadpleeg de basisrouterconfiguratie met behulp van een dm voor meer informatie.

NAT-configuratie

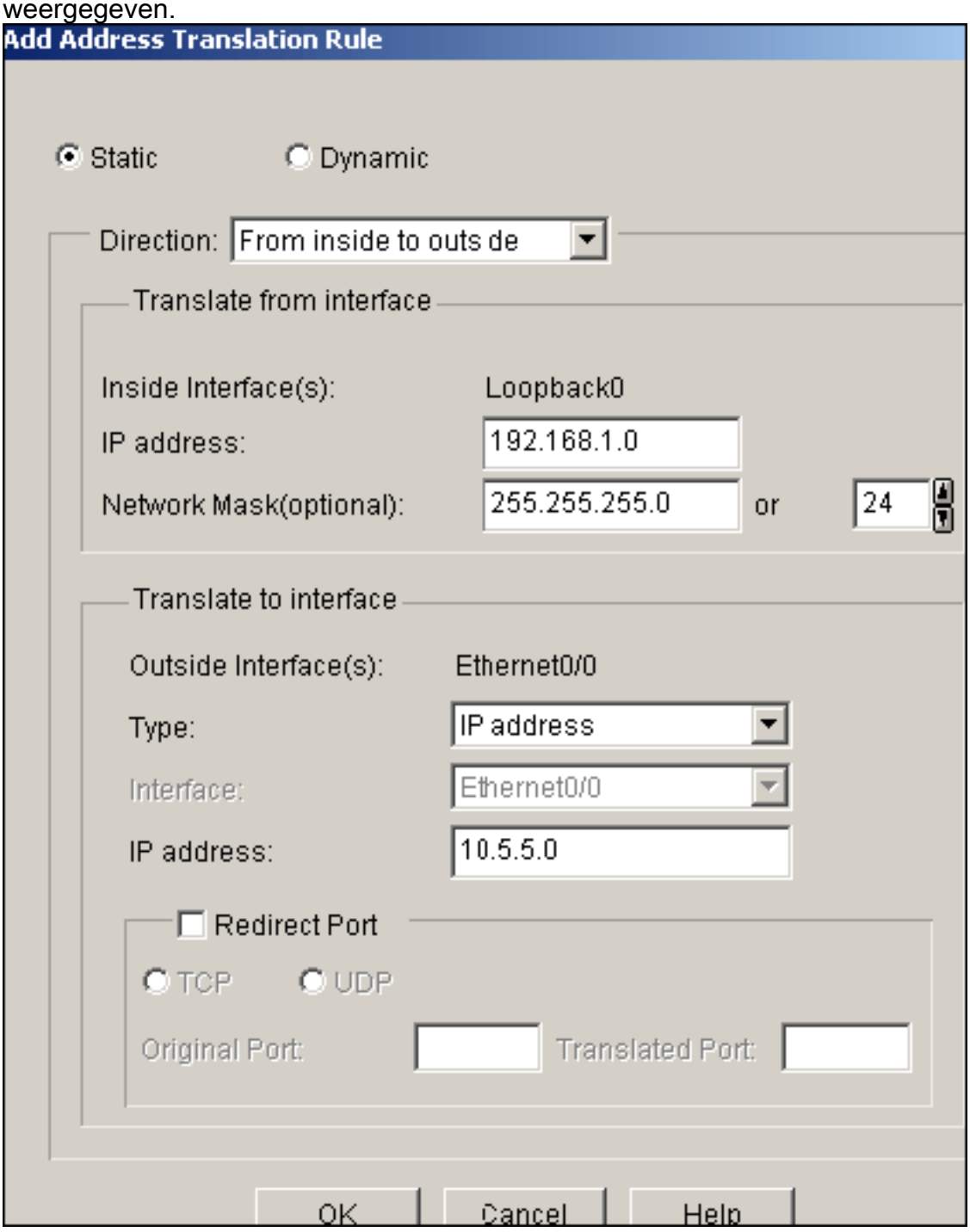
Voltooi deze stappen om NAT te gebruiken om PDN op de Site_A router te configureren:

1. Kies **Configureren > NAT > NAT-configuratie bewerken** en klik op **NAT-interfaces** toewijzen om vertrouwde en onvertrouwde interfaces te definiëren zoals weergegeven.

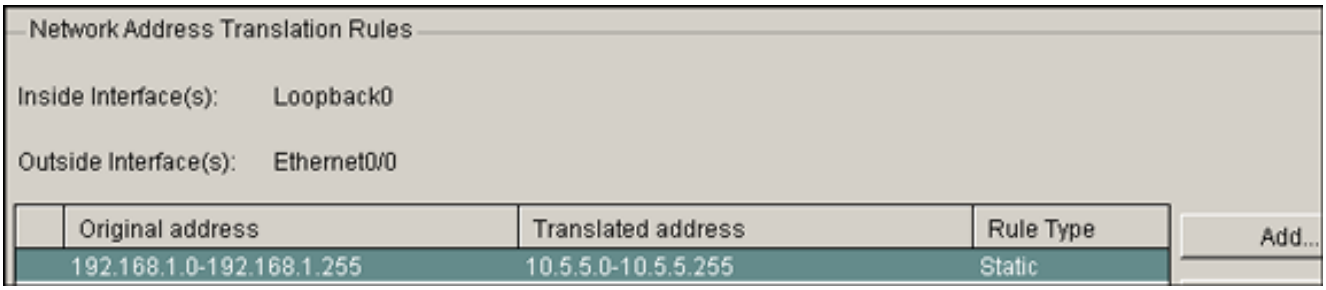


2. Klik op **OK**.
3. Klik op **Add** om de NAT-vertaling van binnen naar buiten te configureren zoals wordt

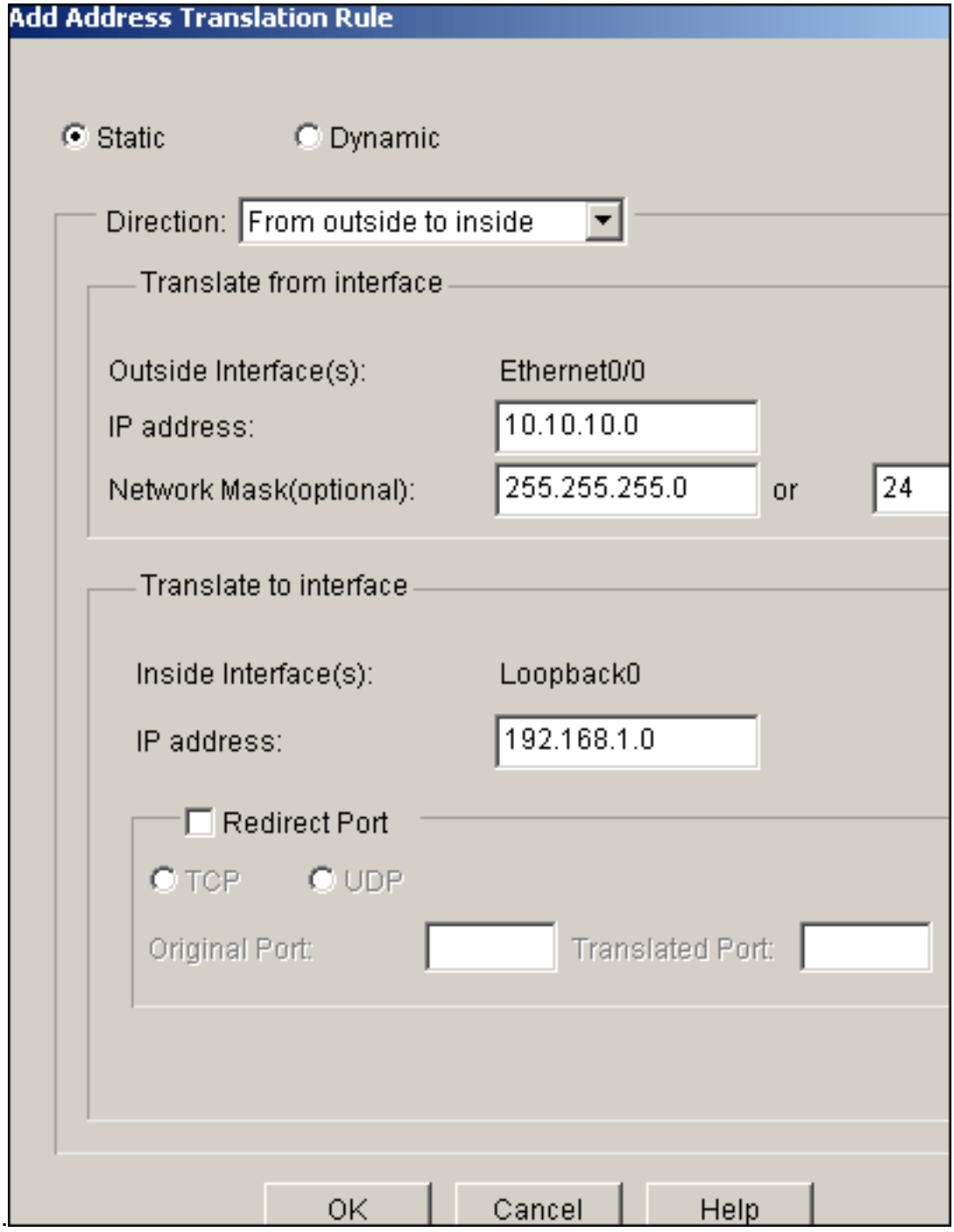
weergegeven.



4. Klik op
OK.

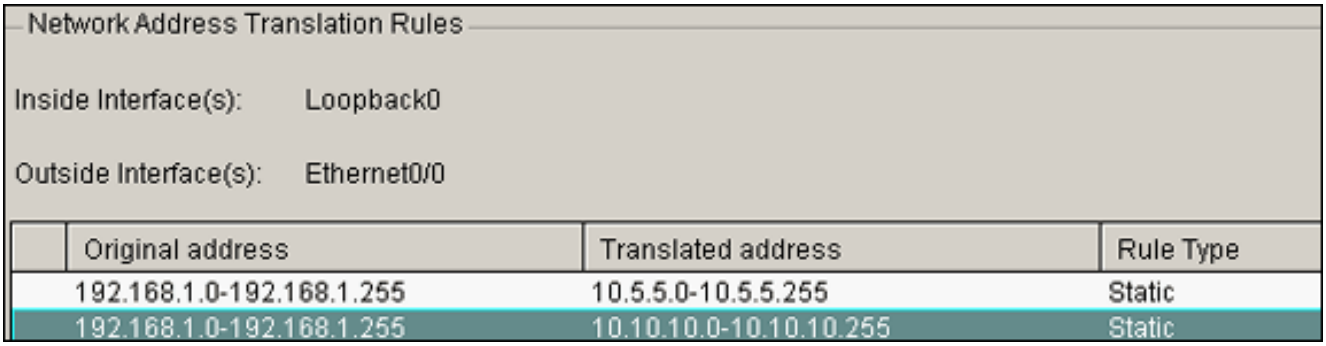


5. Klik nogmaals op **Add** om de NAT-vertaling van buiten naar binnen te configureren zoals wordt



weergegeven.

6. Klik op **OK**.

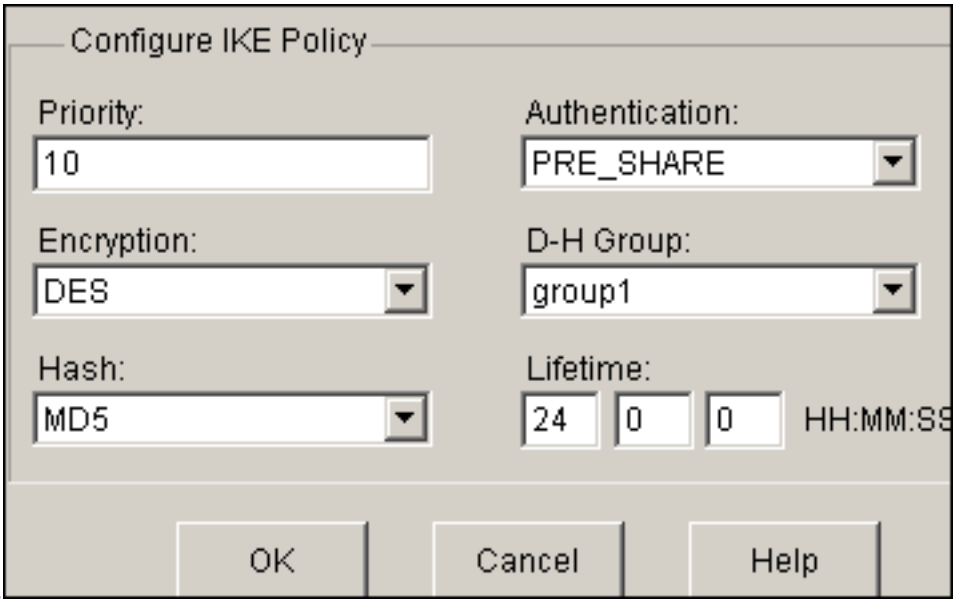


Opmerking: Hier is de equivalente CLI-configuratie:

VPN-configuratie

Voltooi deze stappen om VPN te gebruiken om PDM op de Site_A router te configureren:

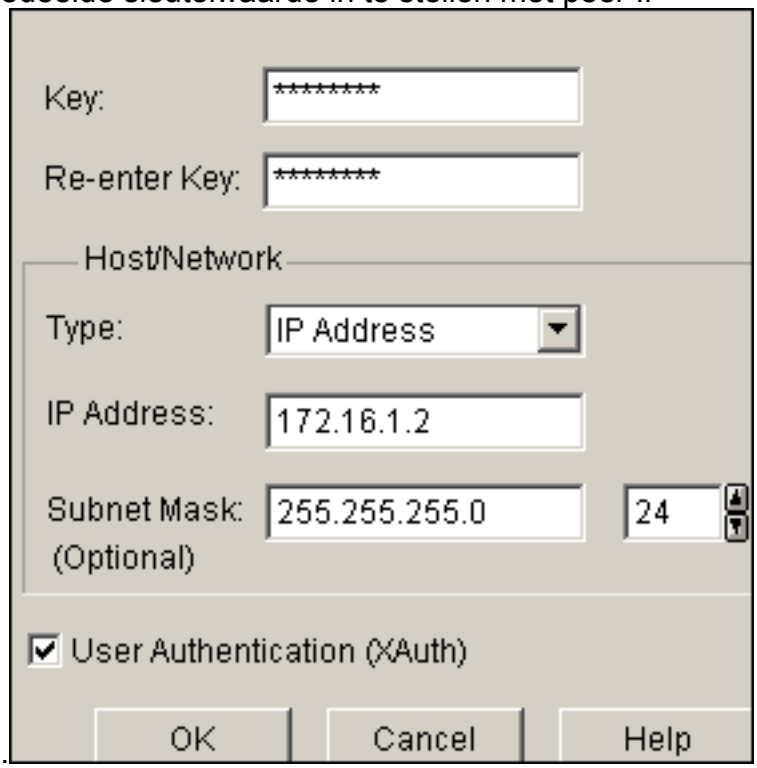
1. Kies **Configureren > VPN > VPN-componenten >IKE > IKE-beleid > Toevoegen** om het IKE-beleid te definiëren zoals in deze afbeelding.



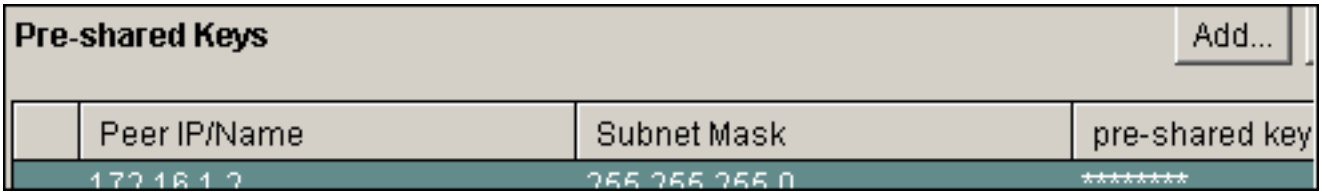
2. Klik op **OK**.

Opmerking: Hier is de equivalente CLI-configuratie:

3. Kies **Configureren > VPN > VPN-componenten >IKE > Voorgedeelde toetsen > Add** om de voorgedeelde sleutelwaarde in te stellen met peer IP-adres.

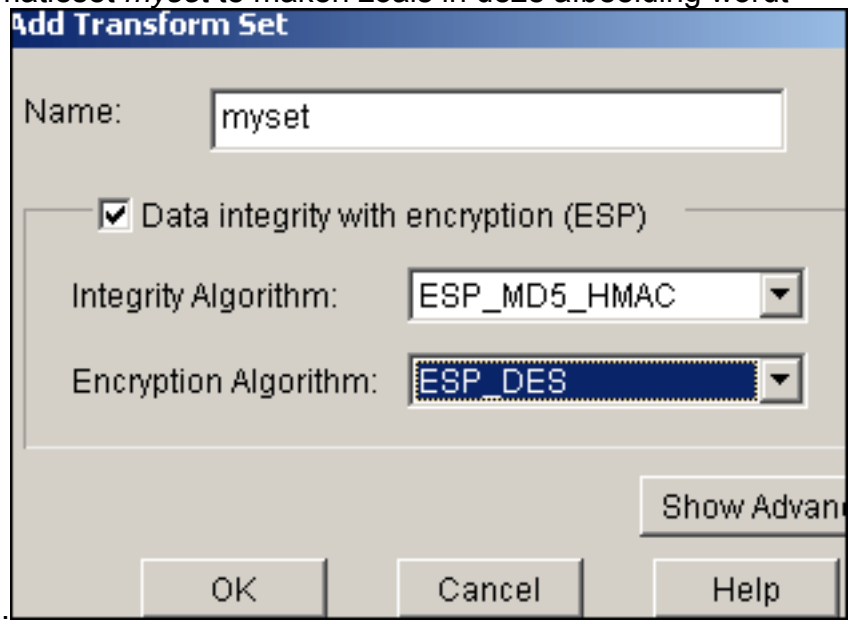


4. Klik op **OK**.



Opmerking: Hier is de equivalente CLI-configuratie:

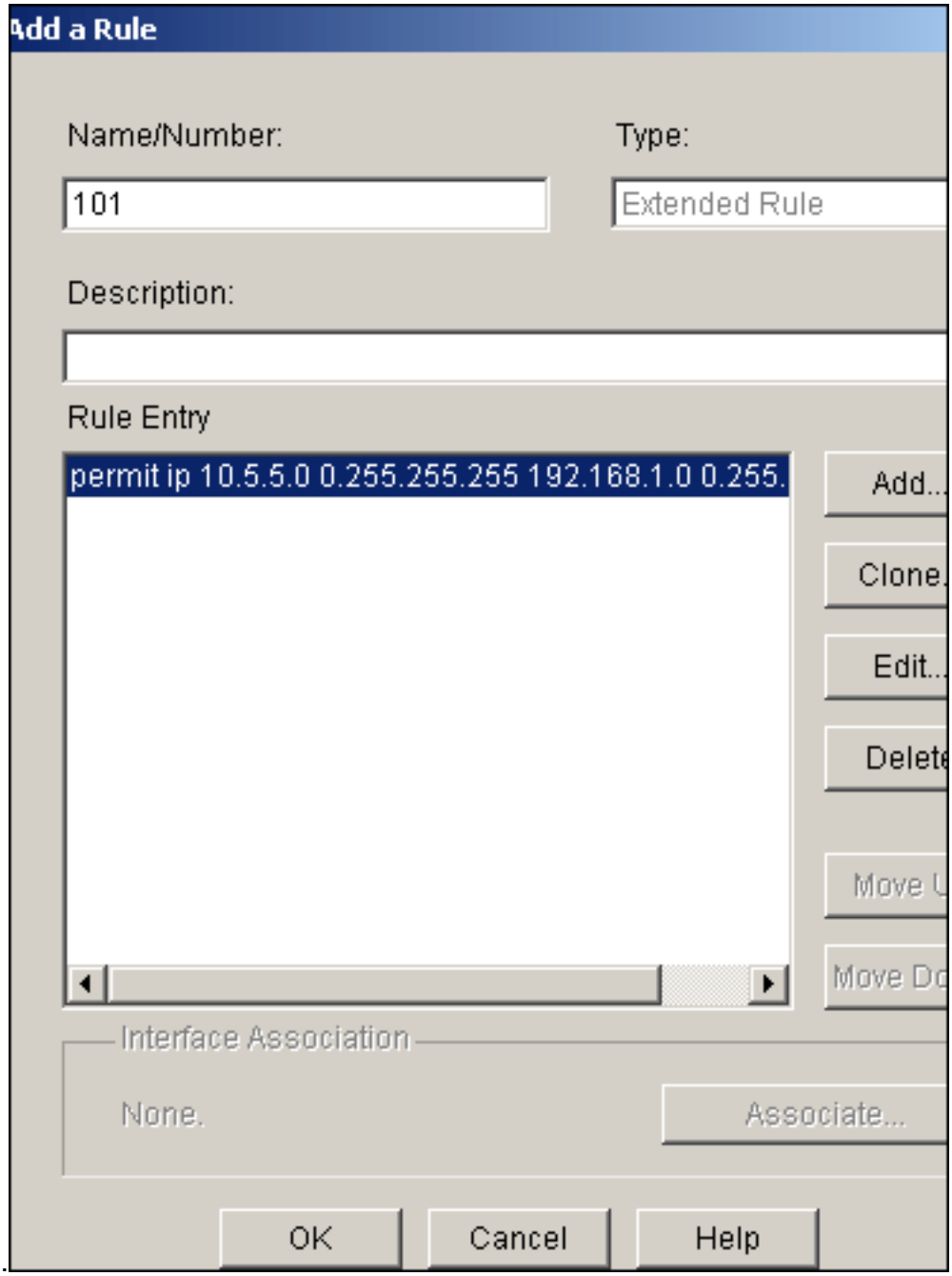
5. Kies **Configureren > VPN-componenten > IPSec > Transformatiesets > Toevoegen** om een transformatieset *myset* te maken zoals in deze afbeelding wordt getoond.



6. Klik op **OK**.

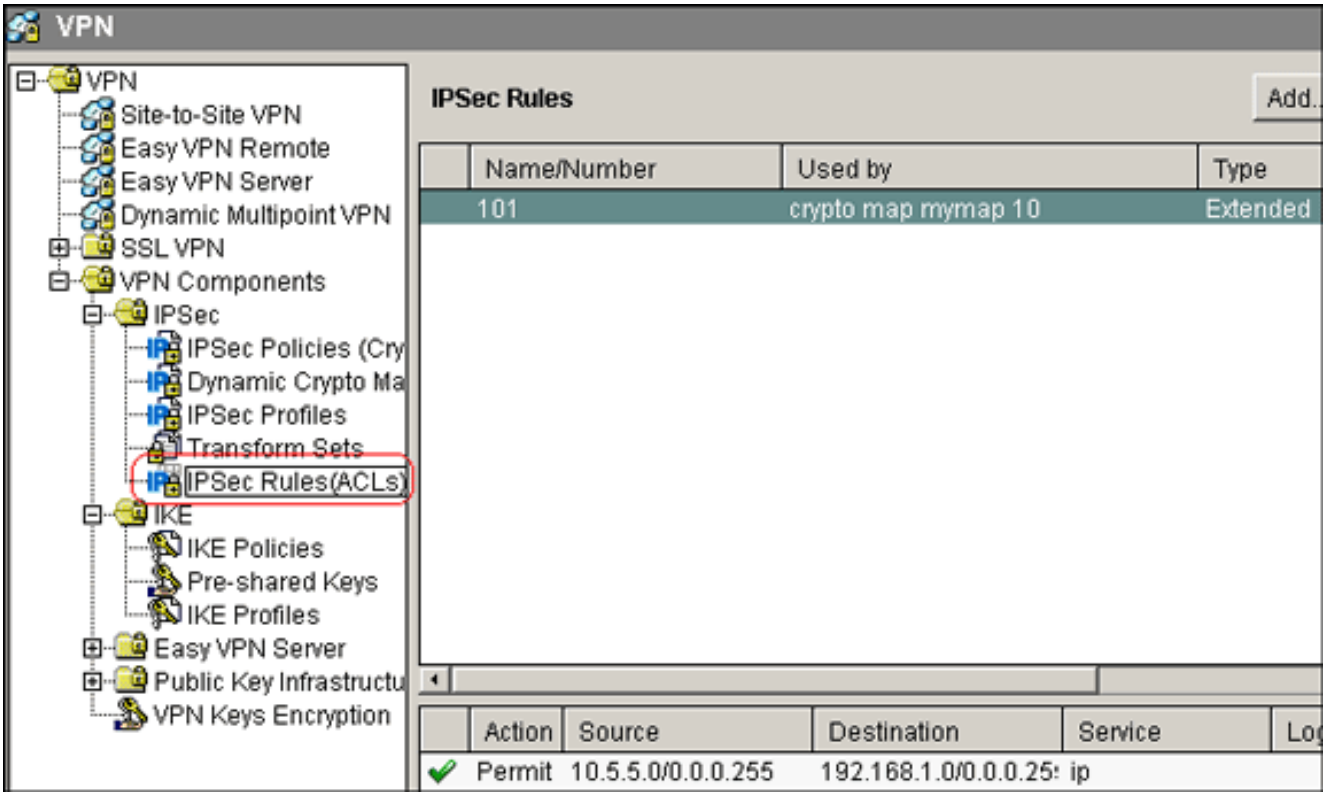
Opmerking: Hier is de equivalente CLI-configuratie:

7. Kies **Configureren > VPN-componenten > IPSec > IPSec-regels (ACL's) > Add** om een crypto toegangscontrolelijst (ACL's) *101* te



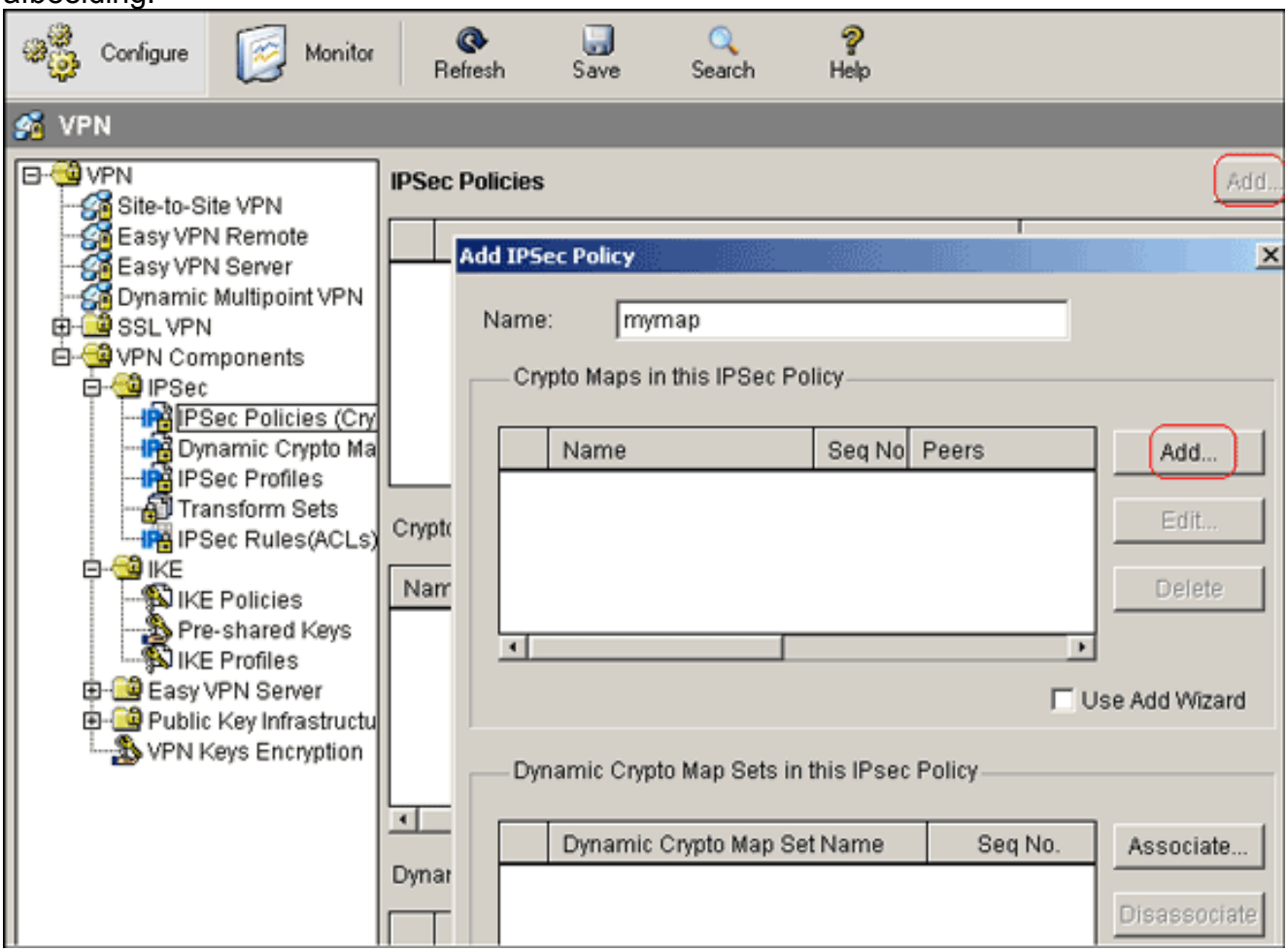
maken.

8. Klik op **OK**.

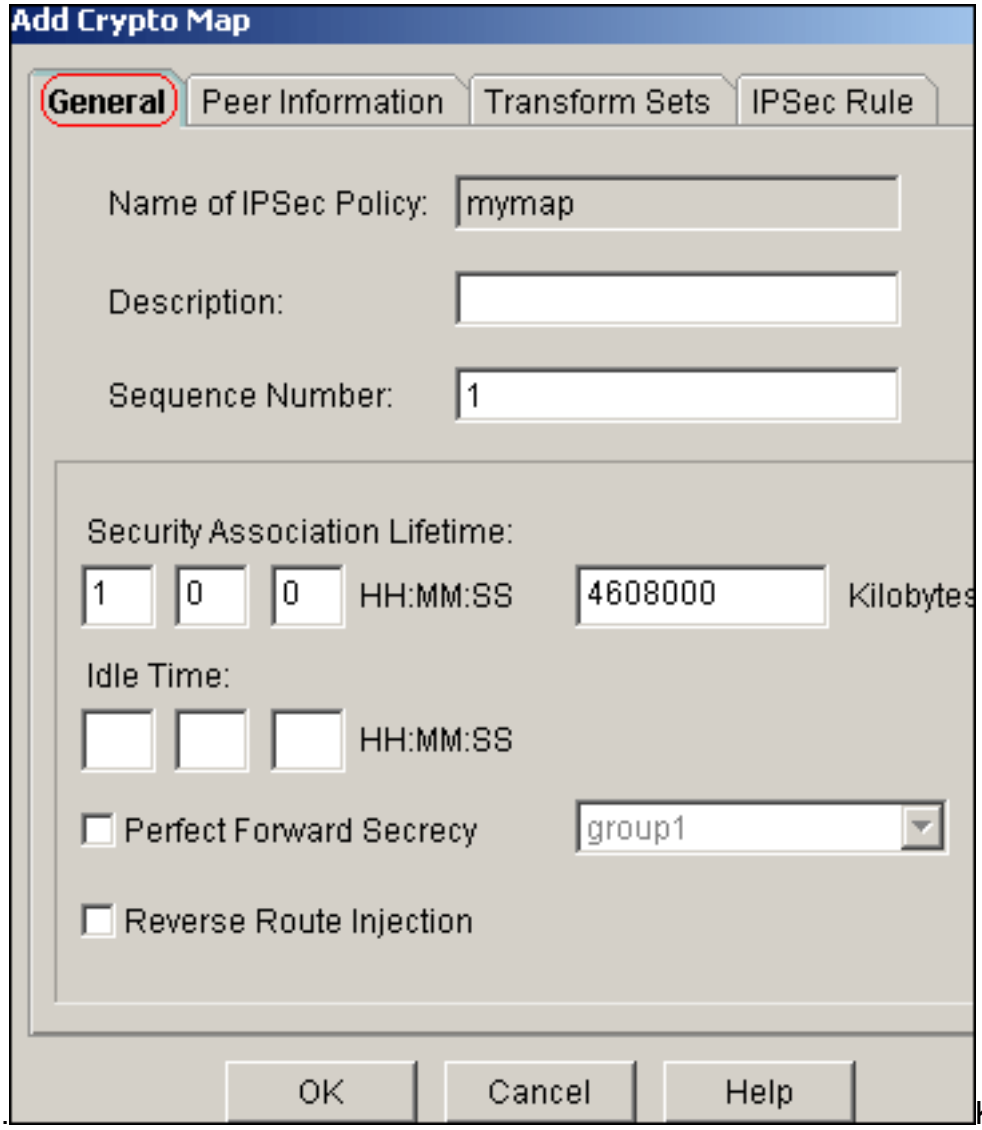


Opmerking: Hier is de equivalente CLI-configuratie:

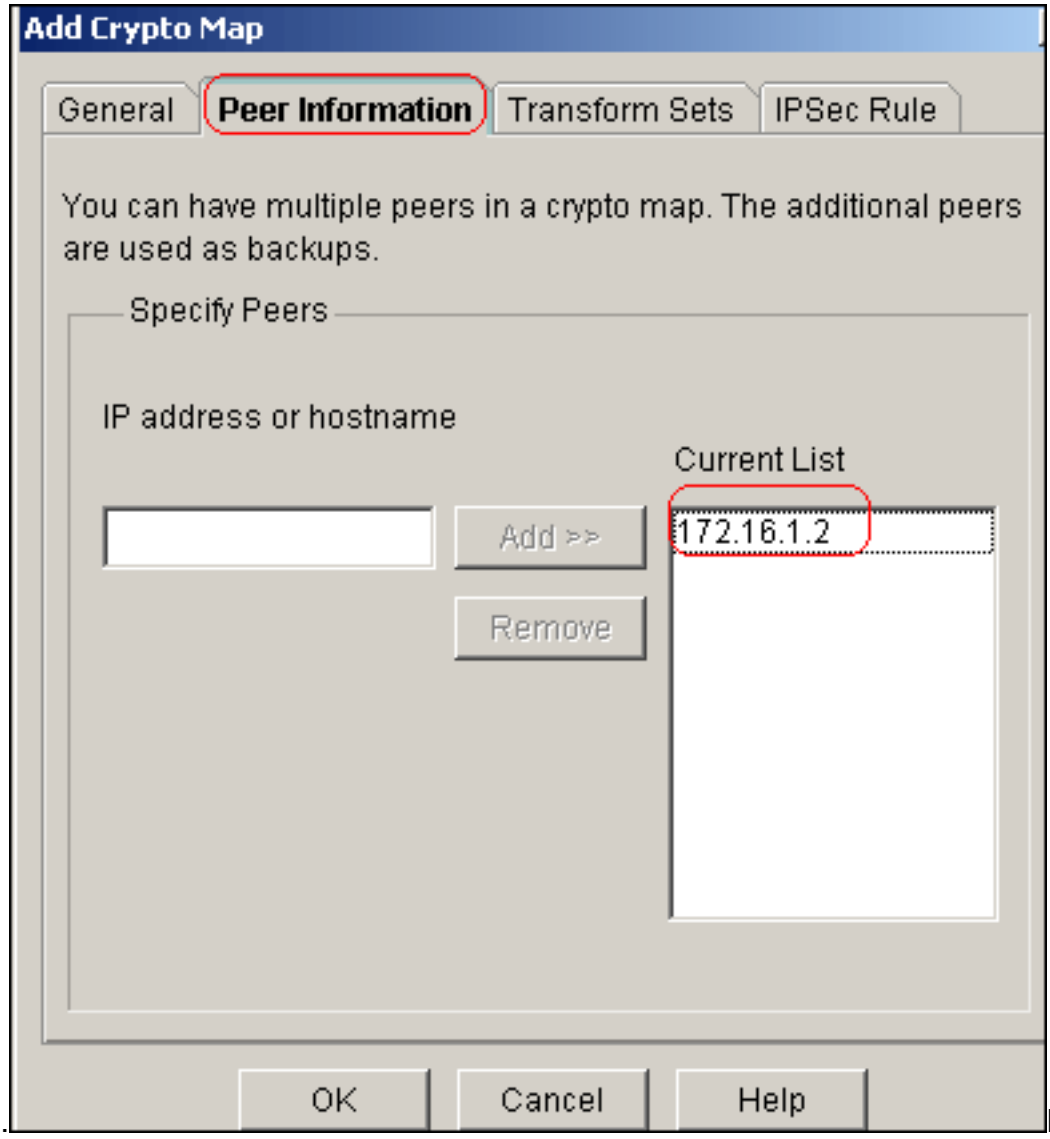
9. Kies **Configureren > VPN-componenten > IPSec > IPSec-beleid > Add** in om cryto map *mymap* te maken zoals in deze afbeelding.



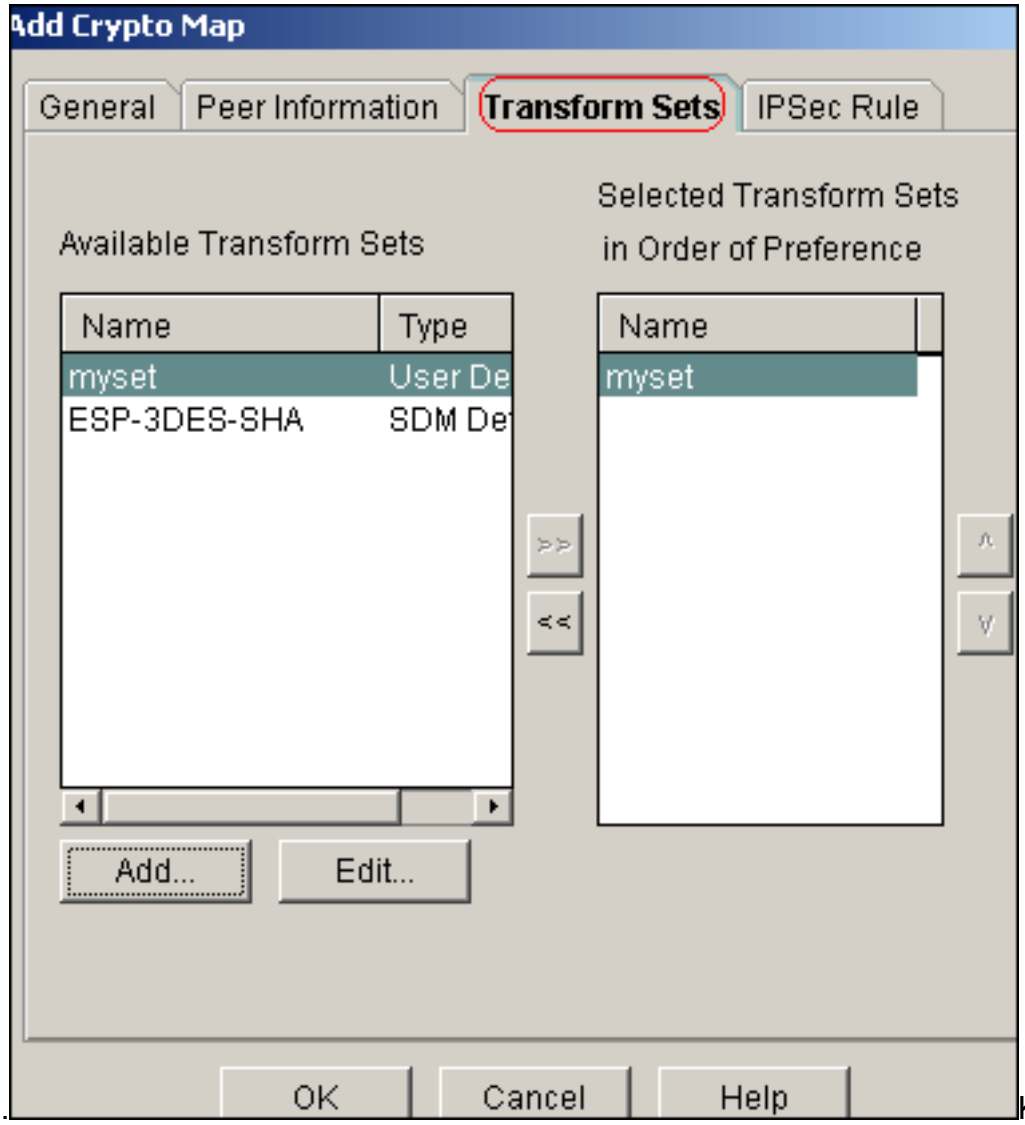
10. Klik op **Toevoegen**.Klik op het **tabblad Algemeen** en bewaar de



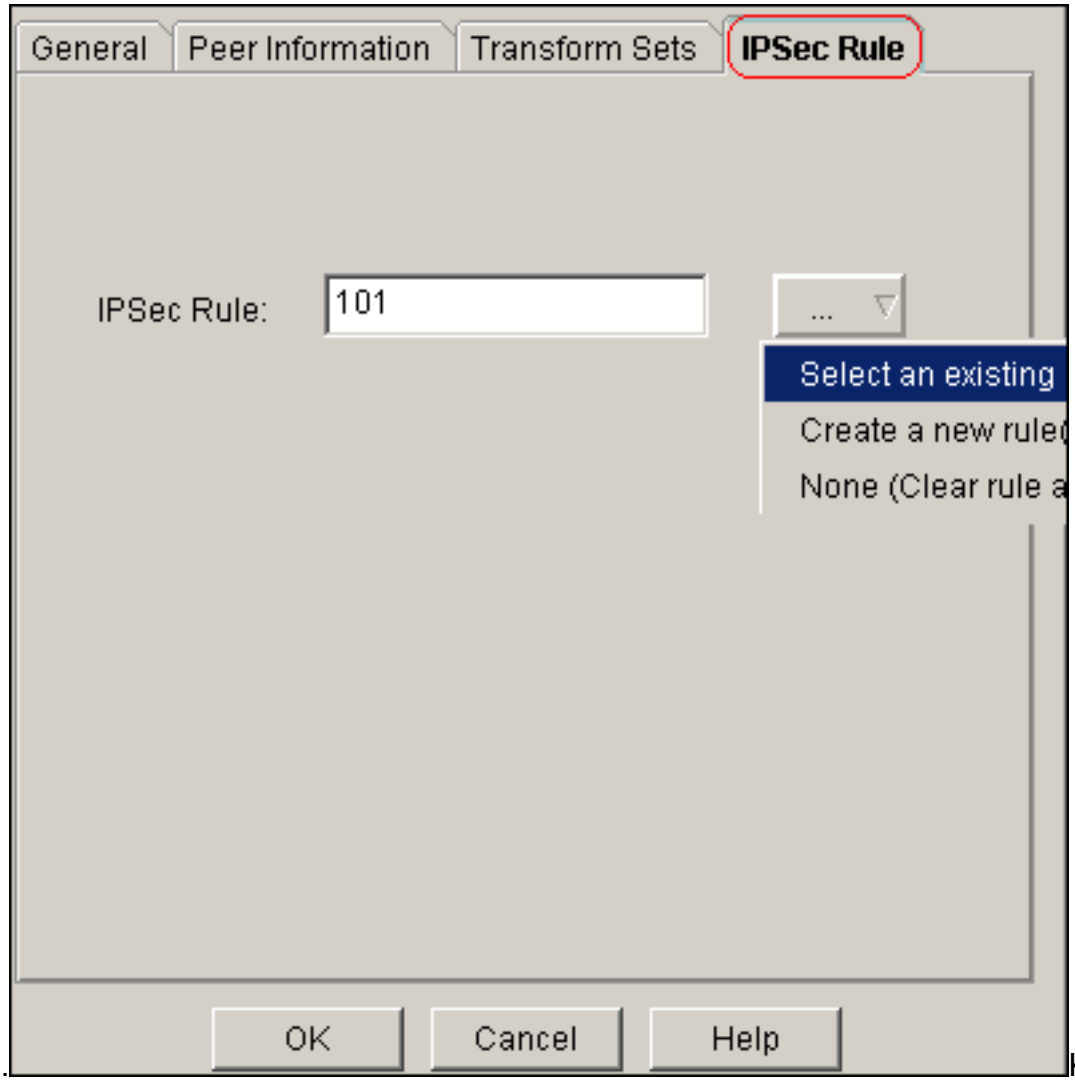
standaardinstellingen. Klik op het tabblad **Peer Informatie** om het IP-adres van een peer toe te voegen



172.16.1.2. Klik op het tabblad **Omzetten** om de gewenste *myset* voor transformatie te

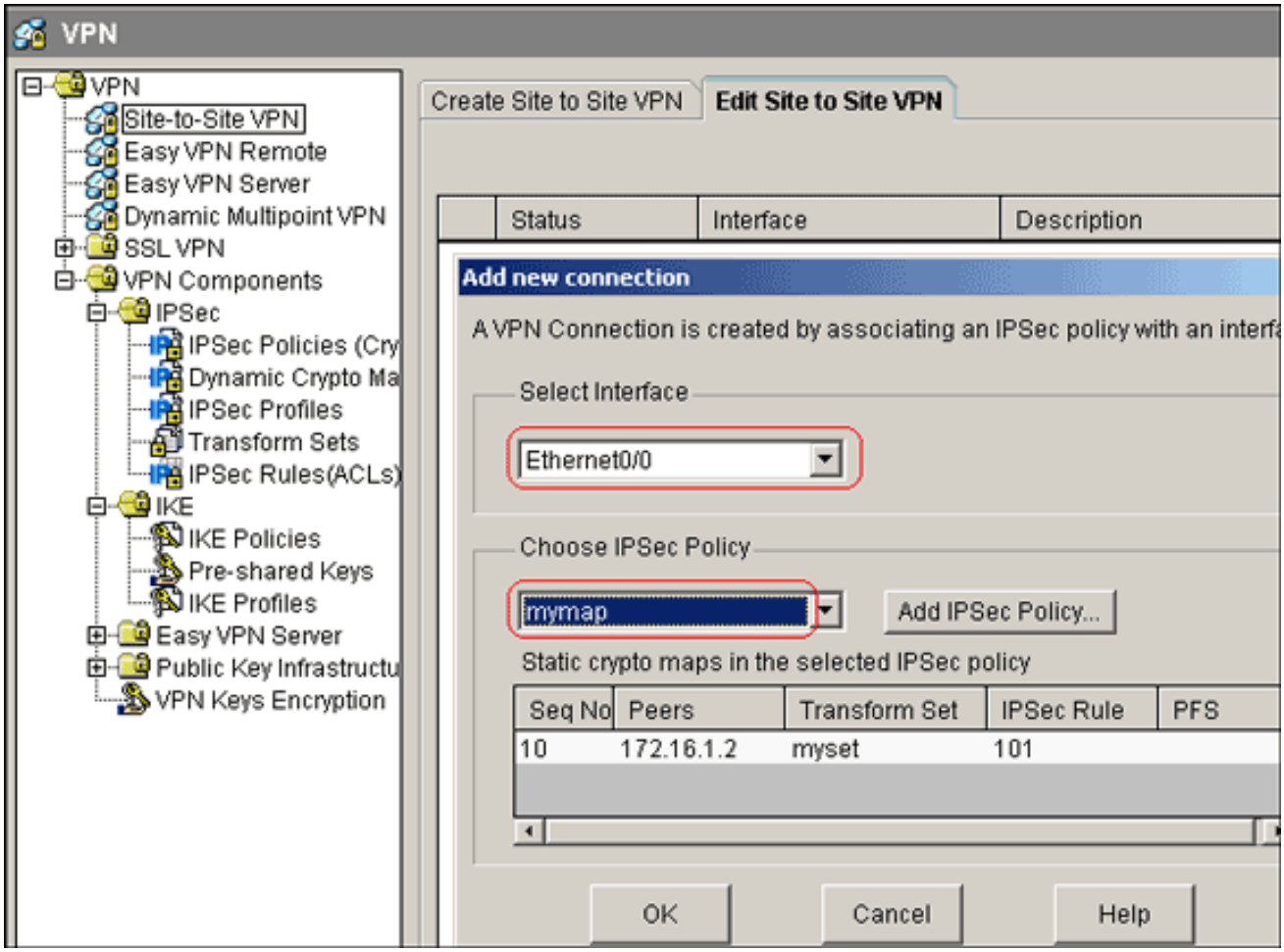


selecteren. Klik op het tabblad **IPSec-regel** om de bestaande crypto ACL 101 te



selecteren. Klik op **OK**.**Opmerking:** Hier is de equivalente CLI-configuratie:

11. Kies **Configureer > VPN > Site-to-Site VPN > Site-to-Site VPN bewerken > Add** om crypto kaart van de interface met Ethernet0/0 toe te passen.



12. Klik op **OK**.**Opmerking:** Hier is de equivalente CLI-configuratie:

Configuratie van Site_A router CLI

Site_A router

```
Site_A#show running-config
*Sep 25 21:15:58.954: %SYS-5-CONFIG_I: Configured from
console by console
Building configuration...

Current configuration : 1545 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Site_A
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
```

```
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
!--- Defines ISAKMP policy. crypto isakmp key 6 L2L12345
address 172.16.1.2 255.255.255.0

!--- Defines pre-shared secret used for IKE
authentication ! ! crypto ipsec transform-set myset esp-
des esp-md5-hmac
!--- Defines IPSec encryption and authentication
algorithms. ! crypto map mymap 10 ipsec-isakmp
 set peer 172.16.1.2
 set transform-set myset
 match address 101
!--- Defines crypto map. ! ! ! ! interface Loopback0 ip
address 192.168.1.1 255.255.255.0 ip nat inside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.1.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 half-duplex
 crypto map mymap
!--- Apply crypto map on the outside interface. ! ! !---
Output Suppressed ! ip http server no ip http secure-
server ! ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
ip nat inside source static network 192.168.1.0 10.5.5.0
/24

!--- Static translation defined to translate
Private_LAN1 !--- from 192.168.1.0/24 to 10.5.5.0/24. !-
-- Note that this translation is used for both !--- VPN
and Internet traffic from Private_LAN1. !--- A routable
global IP address range, or an extra NAT !--- at the ISP
router (in front of Site_A router), is !--- required if
Private_LAN1 also needs internal access. ip nat outside
source static network 192.168.1.0 10.10.10.0 /24

!--- Static translation defined to translate
Private_LAN2 !--- from 192.168.1.0/24 to 10.10.10.0/24.
! access-list 101 permit ip 10.5.5.0 0.0.0.255
192.168.1.0 0.0.0.255

!--- Defines IPSec interesting traffic. !--- Note that
the host behind Site_A router communicates !--- to
Private_LAN2 using 10.10.10.0/24. !--- When the packets
arrive at the Site_A router, they are first !---
translated to 192.168.1.0/24 and then encrypted by
IPSec. ! ! control-plane ! ! line con 0 line aux 0 line
vty 0 4 ! ! end Site_A#
```

Configuratie van Site_B router CLI

Site_B router
Site_B#**show running_config** Building configuration...

```
Current configuration : 939 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Site_B
!
!
ip subnet-zero
!
!
crypto isakmp policy 10
 hash md5
 authentication pre-share
crypto isakmp key L2L12345 address 10.1.1.2
255.255.255.0
!
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap 10 ipsec-isakmp
 set peer 10.1.1.2
 set transform-set myset
 match address 101
!
!
!
!
interface Ethernet0
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1
 ip address 172.16.1.2 255.255.255.0
 crypto map mymap
!
!--- Output Suppressed ! ip classless ip route 0.0.0.0
0.0.0.0 172.16.1.1
ip http server
!
access-list 101 permit ip 192.168.1.0 0.0.0.255 10.5.5.0
0.0.0.255
!
line con 0
line aux 0
line vty 0 4
!
end

Site_B#
```

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**-Toont alle huidige IKE (Internet Key Exchange) veiligheidsassociaties (SAs) bij een peer.

```
Site_A#show crypto isakmp sa
dst             src             state          conn-id slot status
172.16.1.2      10.1.1.2        QM_IDLE              1    0 ACTIVE
```

- **toon crypto isakmp als detail**-Toont de details van alle huidige IKE SAs bij een peer.

```
Site_A#show cryto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH Lifetime
 Cap.
1     10.1.1.2        172.16.1.2               ACTIVE des  md5  psk  1  23:59:42

       Connection-id:Engine-id =  1:1(software)
```

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

```
Site_A#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: mymap, local addr 10.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 172.16.1.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
    #pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 3, #recv errors 0

     local crypto endpt.: 10.1.1.2, remote crypto endpt.: 172.16.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x1A9CDC0A(446487562)

     inbound esp sas:
      spi: 0x99C7BA58(2580003416)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: SW:2, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3336)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x1A9CDC0A(446487562)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: SW:1, crypto map: mymap
        sa timing: remaining key lifetime (k/sec): (4478520/3335)
        IV size: 8 bytes
```

```
        replay detection support: Y
        Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Site_A#
```

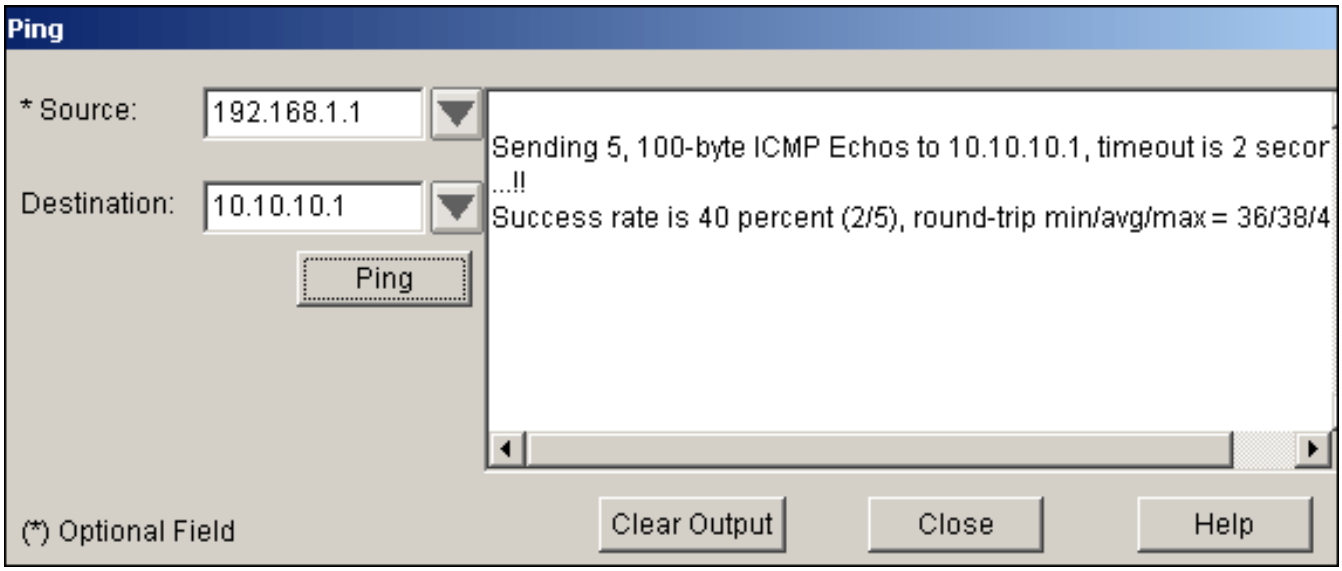
- **informatie over de ip** nat **vertalingen**-displays met de vertaalsleuf.

```
Site_A#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                10.10.10.1         192.168.1.1
--- ---                ---                10.10.10.0         192.168.1.0
--- 10.5.5.1           192.168.1.1        ---                ---
--- 10.5.5.0           192.168.1.0        ---                ---
```

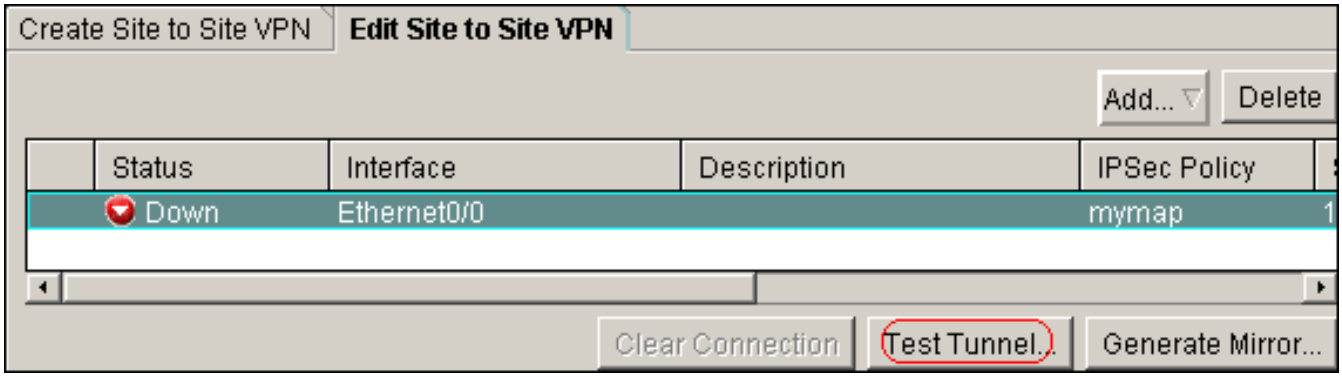
- **ip nat statistics**-displays statistische informatie over de vertaling tonen.

```
Site_A#show ip nat statistics
Total active translations: 4 (2 static, 2 dynamic; 0 extended)
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Loopback0
Hits: 42  Misses: 2
CEF Translated packets: 13, CEF Punted packets: 0
Expired translations: 7
Dynamic mappings:
Queued Packets: 0
Site_A#
```

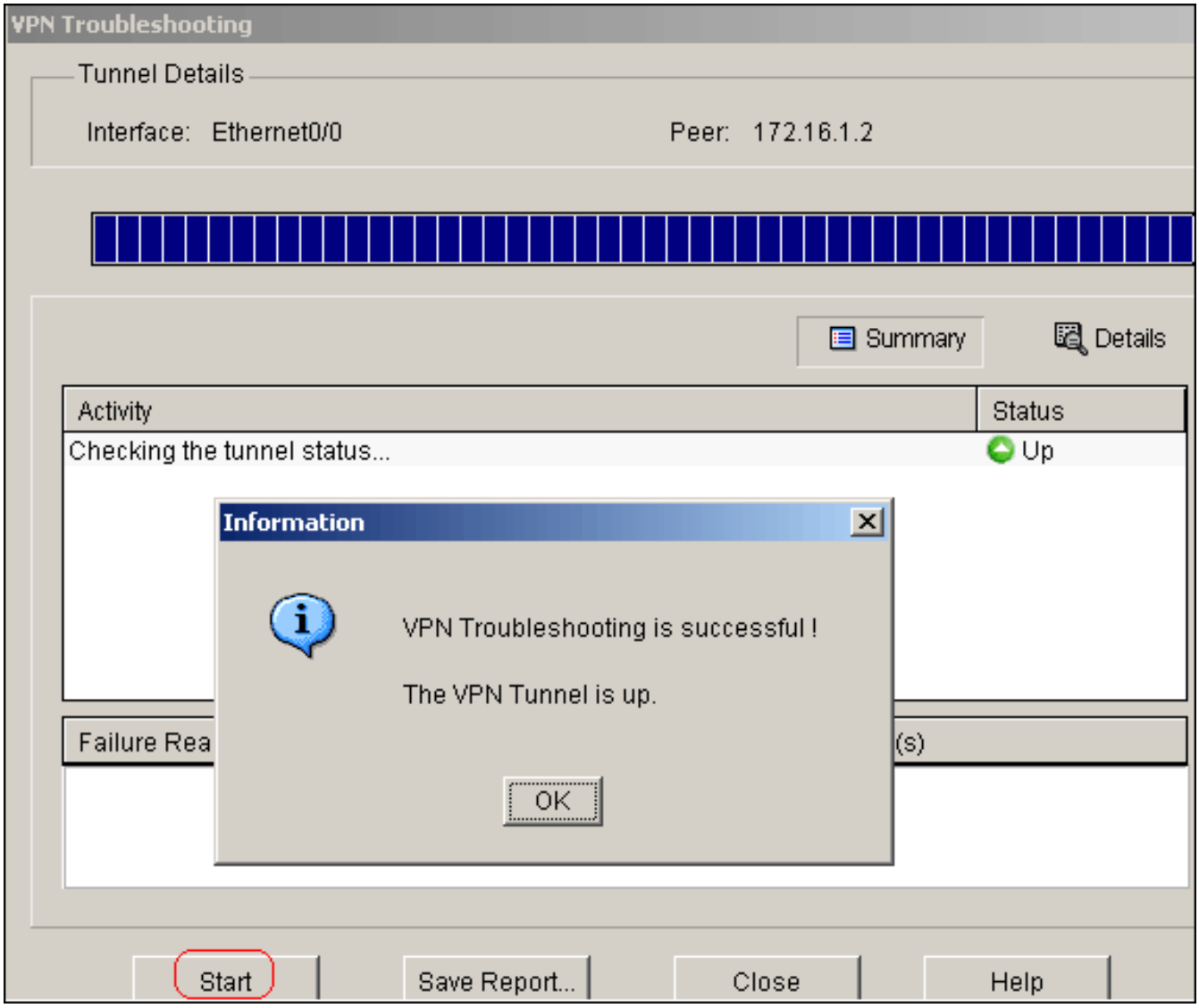
- Voltooi deze stappen om de verbinding te controleren:In het programma dm, kies **Gereedschappen > Ping** om de IPsec VPN-tunnel met bron IP als 192.168.1.1 en bestemming IP als 10.10.10 op te zetten.



Klik op **Test Tunnel** om te controleren of de IPsec VPN-tunnel is ingesteld zoals in deze afbeelding.



Klik op
Start.



Problemen oplossen

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

```
Site_A#debug ip packet
IP packet debugging is on
Site_A#ping
Protocol [ip]:
Target IP address: 10.10.10.1
Repeat count [5]:
```

```
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/45/52 ms
Site_A#
*Sep 30 18:08:10.601: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.601: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.641: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.641: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.645: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.685: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.685: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.689: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.729: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.729: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.729: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.769: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.769: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethern
et0/0), routed via FIB
*Sep 30 18:08:10.773: IP: s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), len
 100, sending
*Sep 30 18:08:10.813: IP: tableid=0, s=10.10.10.1 (Ethernet0/0), d=192.168.1.1 (
Loopback0), routed via RIB
*Sep 30 18:08:10.813: IP: s=10.10.10.1 (Ethernet0/0), d=192.168.1.1, len 100, rc
vd 4
```

Gerelateerde informatie

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- IPsec tussen ASA/PIX en Cisco VPN 3000 Concentrator met Overlappend Configuratievoorbeeld voor Private Networks

- Technische ondersteuning en documentatie – Cisco Systems