Konfigurationsbeispiel für IPsec zwischen zwei IOS-Routern mit sich überschneidenden privaten Netzwerken

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Cisco IOS-Router in einem standortübergreifenden IPsec-VPN mit sich überschneidenden privaten Netzwerkadressen hinter VPN-Gateways konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS 3640-Routern, auf denen die Softwareversion 12.4 ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

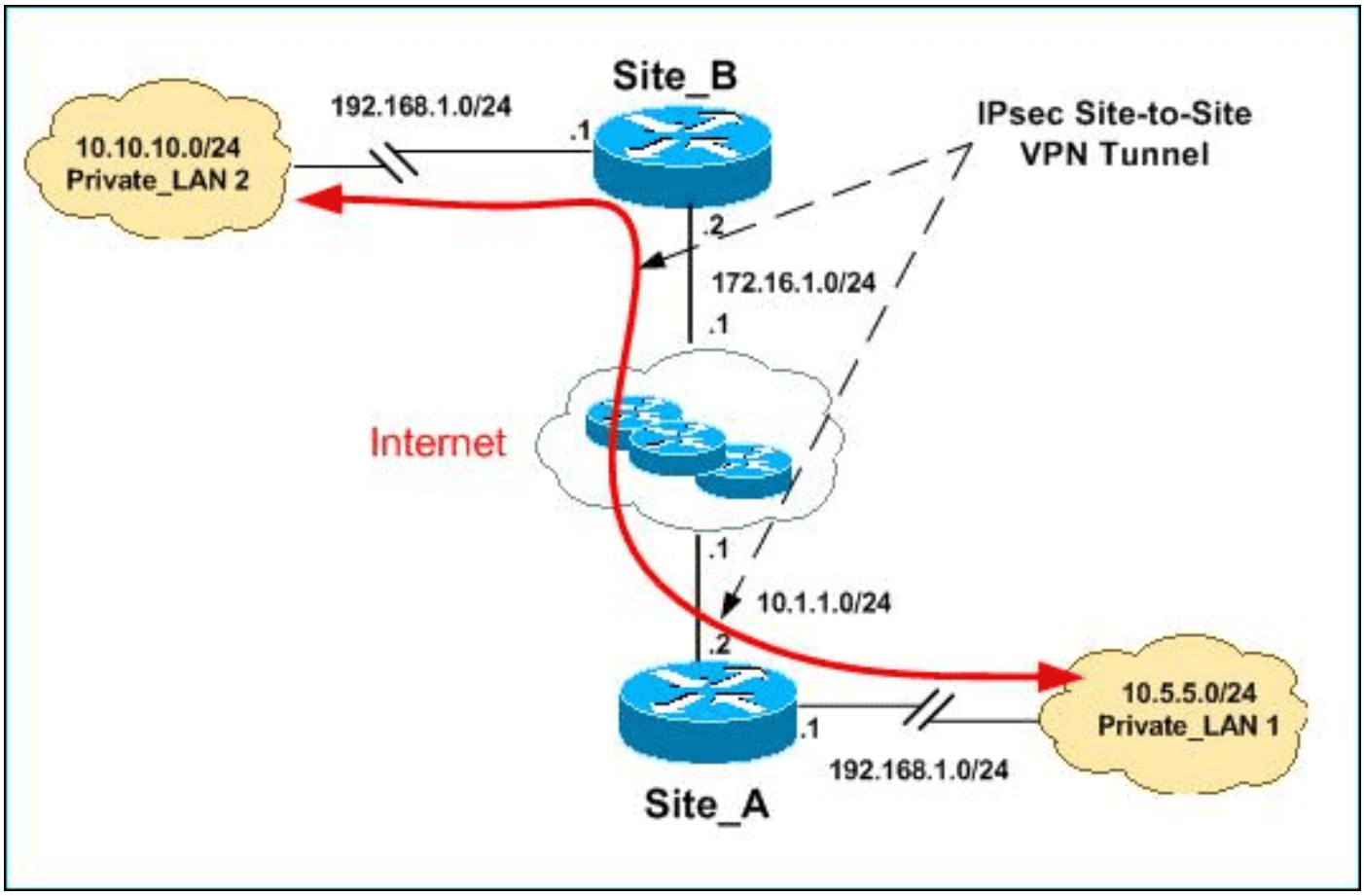
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

Sowohl Private_LAN1 als auch Private_LAN2 verfügen über das IP-Subnetz 192.168.1.0/24. Dadurch wird der sich überschneidende Adressbereich hinter jeder Seite des IPsec-Tunnels simuliert.

In diesem Beispiel führt der Site_A-Router eine bidirektionale Übersetzung durch, sodass die beiden privaten LANs über den IPsec-Tunnel kommunizieren können. Die Übersetzung bedeutet, dass Private_LAN1 Private_LAN2 durch den IPsec-Tunnel als 10.10.10.0/24 und Private_LAN2 durch den IPSec-Tunnel Private_LAN1 als 10.5.5.0/24 "erkennt".

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- SDM-Konfiguration für Standort_A-Router
- CLI-Konfiguration für Standort_A-Router
- Konfiguration des Standorts_B-Routers

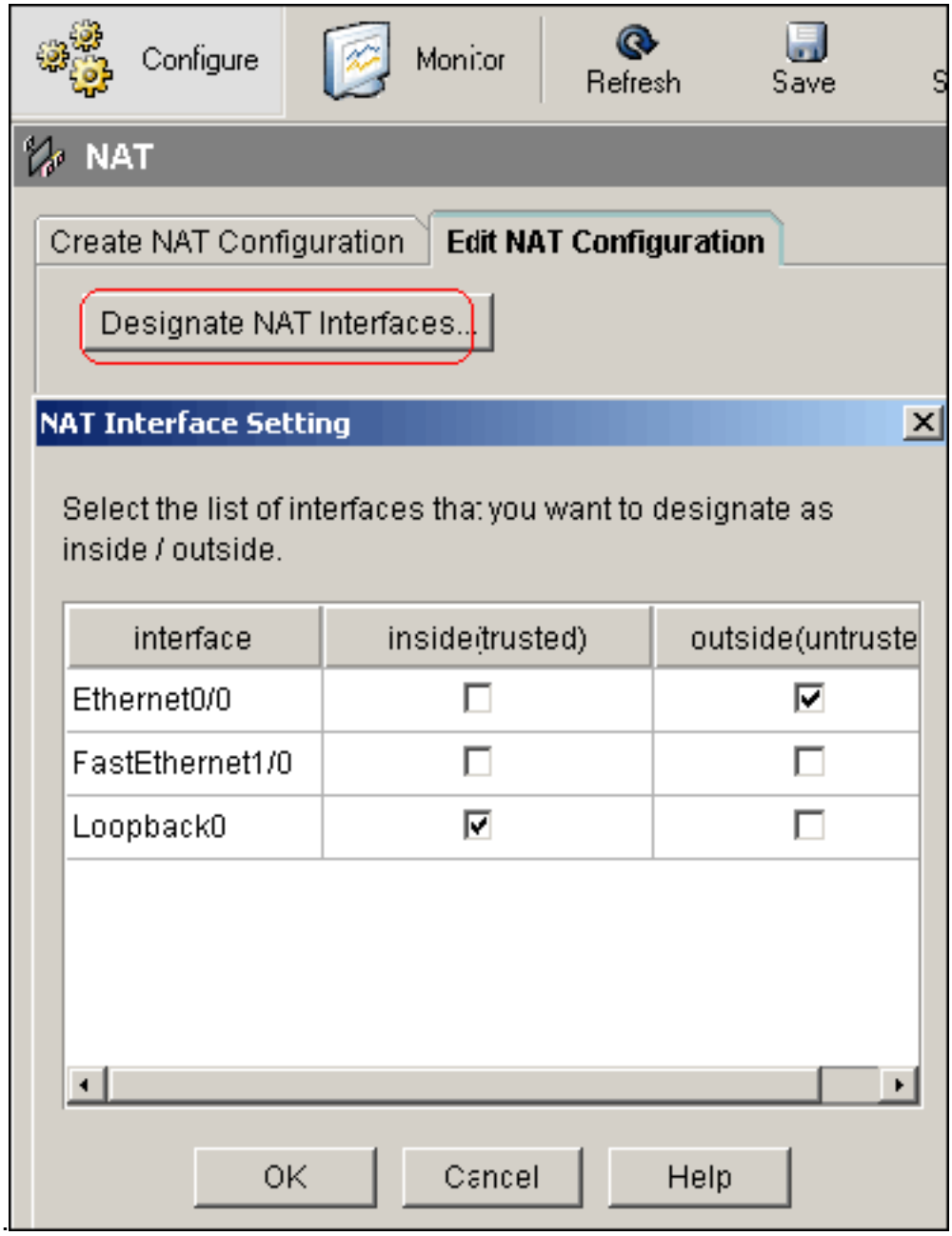
SDM-Konfiguration für Standort_A-Router

Hinweis: In diesem Dokument wird davon ausgegangen, dass der Router mit grundlegenden Einstellungen wie Schnittstellenkonfiguration usw. konfiguriert ist. Weitere Informationen finden Sie unter Grundlegende Routerkonfiguration mit SDM.

NAT-Konfiguration

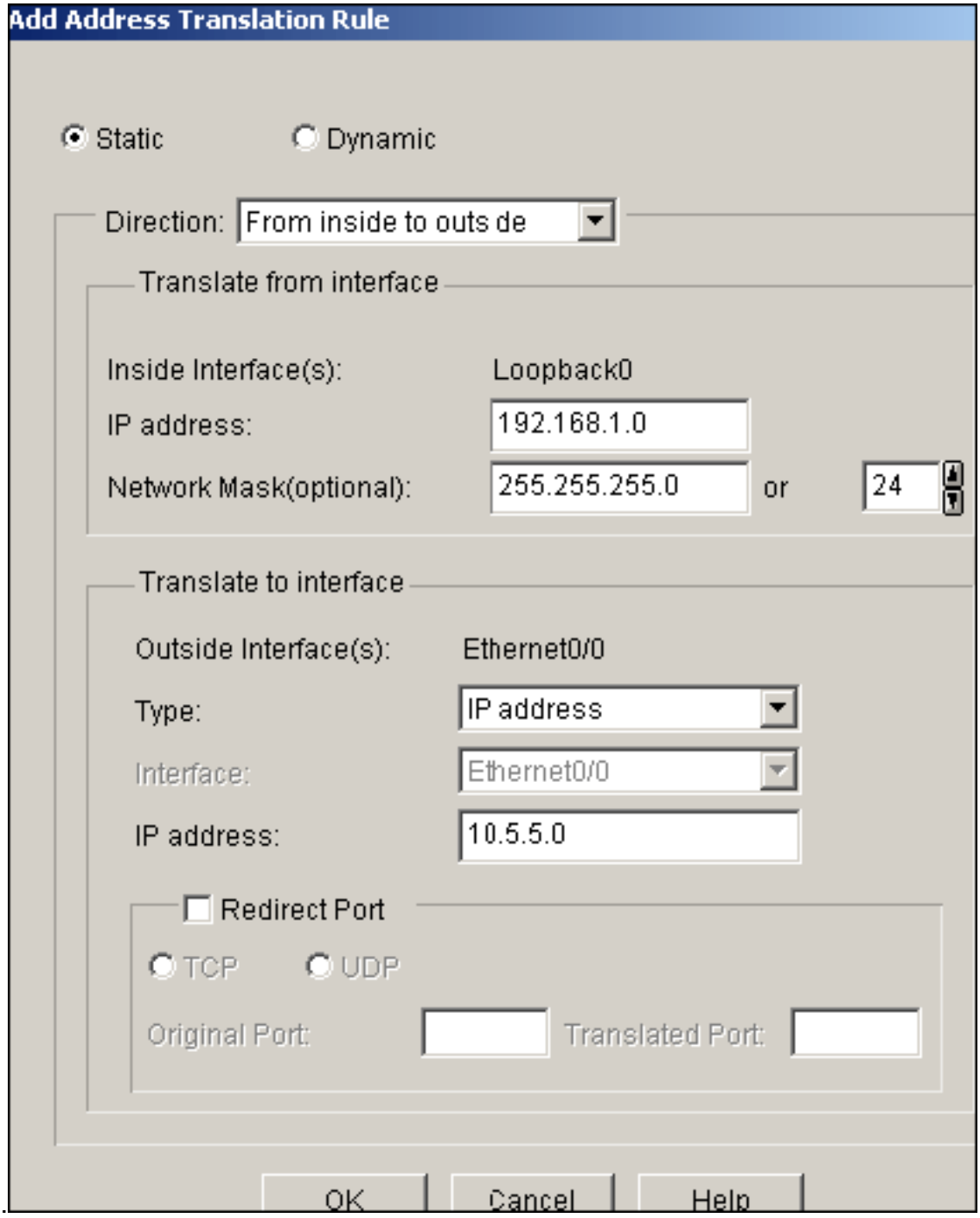
Gehen Sie wie folgt vor, um mithilfe von NAT SDM auf dem Site_A-Router zu konfigurieren:

1. Wählen Sie **Configure > NAT > Edit NAT Configuration**, und klicken Sie auf **Designate NAT Interfaces (NAT-Schnittstellen festlegen),** um vertrauenswürdige und nicht vertrauenswürdige Schnittstellen wie gezeigt zu



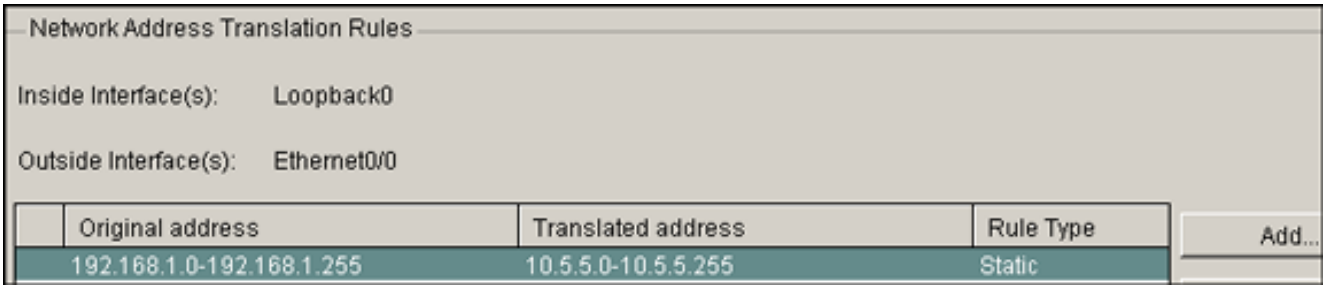
definieren.

2. Klicken Sie auf **OK**.
3. Klicken Sie auf **Hinzufügen**, um die NAT-Übersetzung wie dargestellt von innen nach außen zu



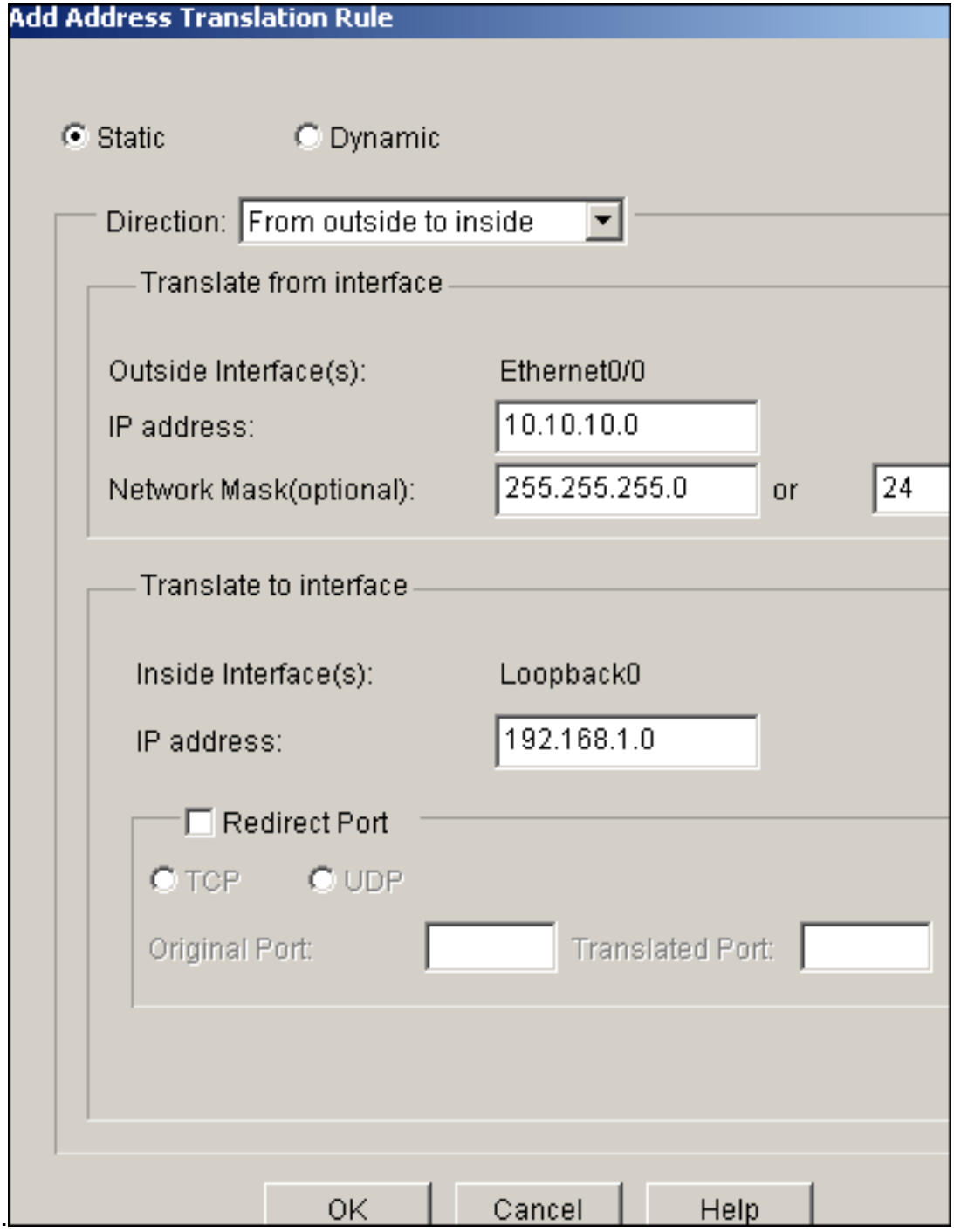
konfigurieren.

4. Klicken Sie auf **OK**.

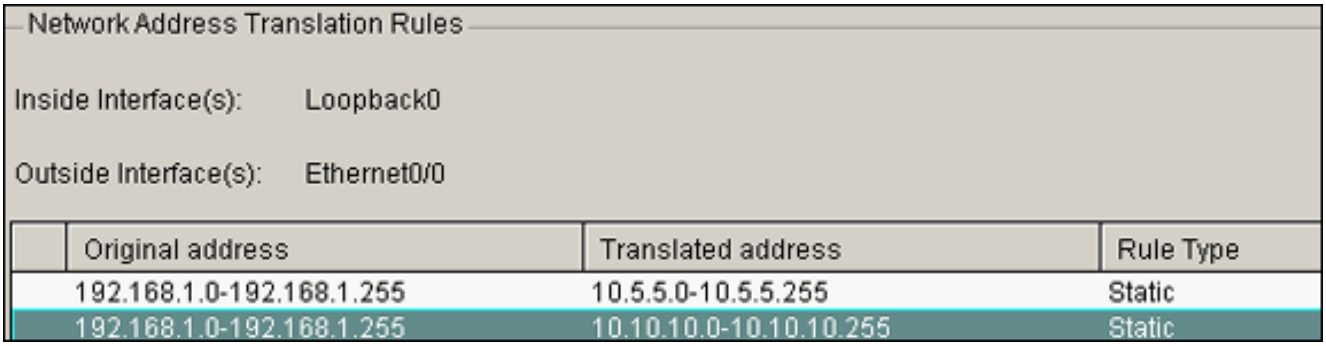


5. Klicken Sie erneut auf **Hinzufügen**, um die NAT-Übersetzung wie dargestellt von außen in die Richtung von innen zu

konfigurieren.



6. Klicken Sie auf **OK**.

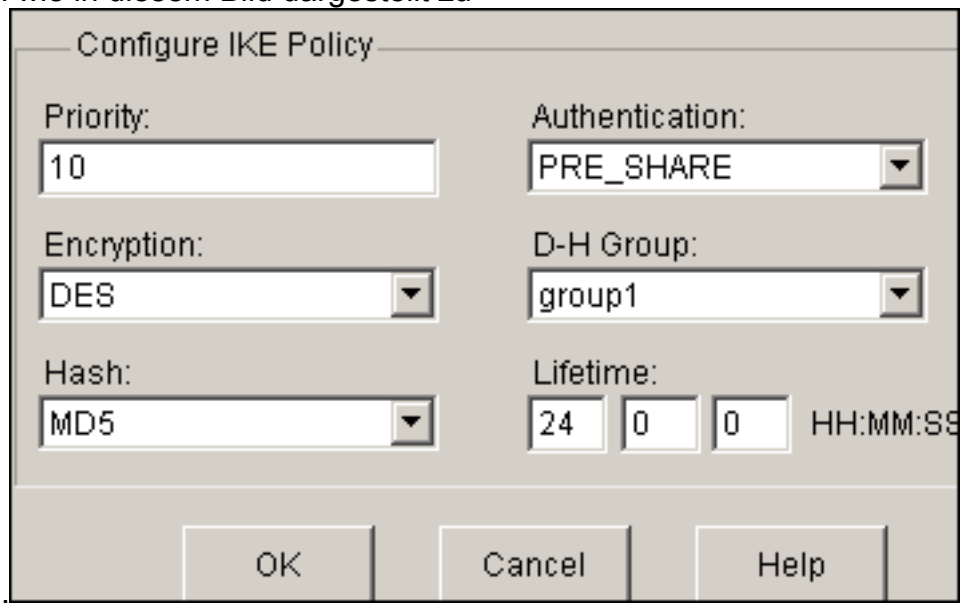


Hinweis: Dies ist die entsprechende CLI-Konfiguration:

VPN-Konfiguration

Gehen Sie wie folgt vor, um mithilfe von VPN SDM auf dem Site_A-Router zu konfigurieren:

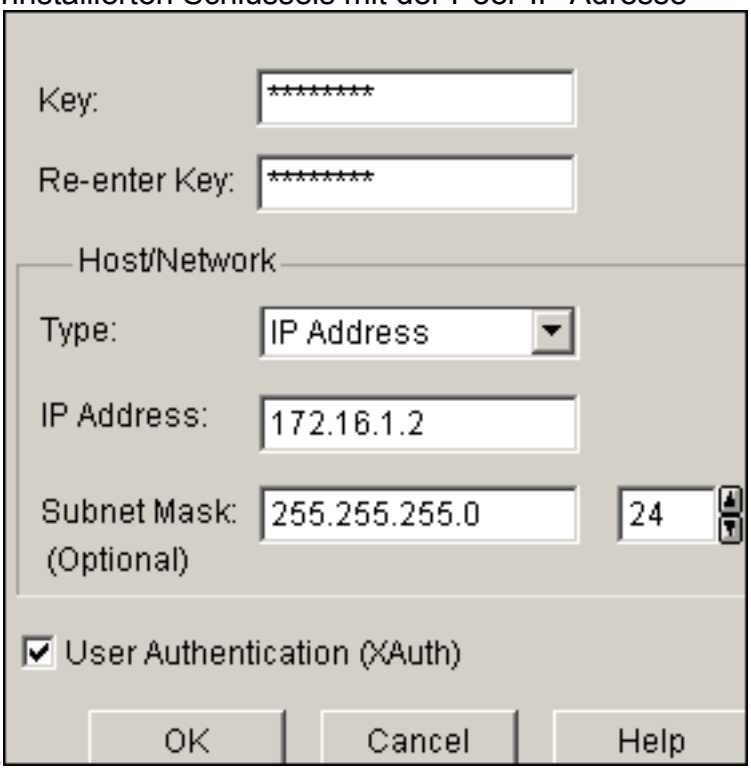
1. Wählen Sie **Configure > VPN > VPN Components > IKE > IKE Policies > Add**, um die IKE-Richtlinien wie in diesem Bild dargestellt zu definieren.



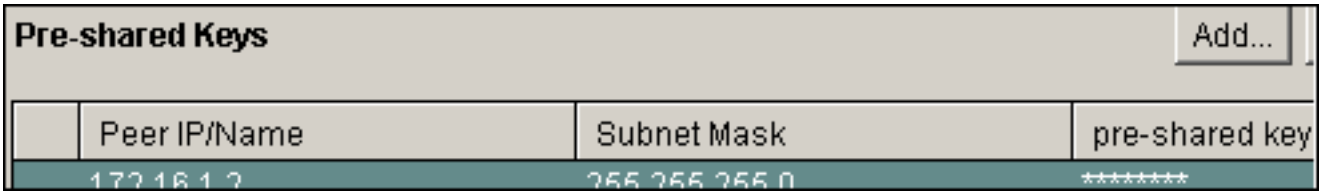
2. Klicken Sie auf **OK**.

Hinweis: Dies ist die entsprechende CLI-Konfiguration:

3. Wählen Sie **Configure > VPN > VPN Components >IKE > Pre-shared Keys > Add**, um den Wert des vorinstallierten Schlüssels mit der Peer-IP-Adresse festzulegen.

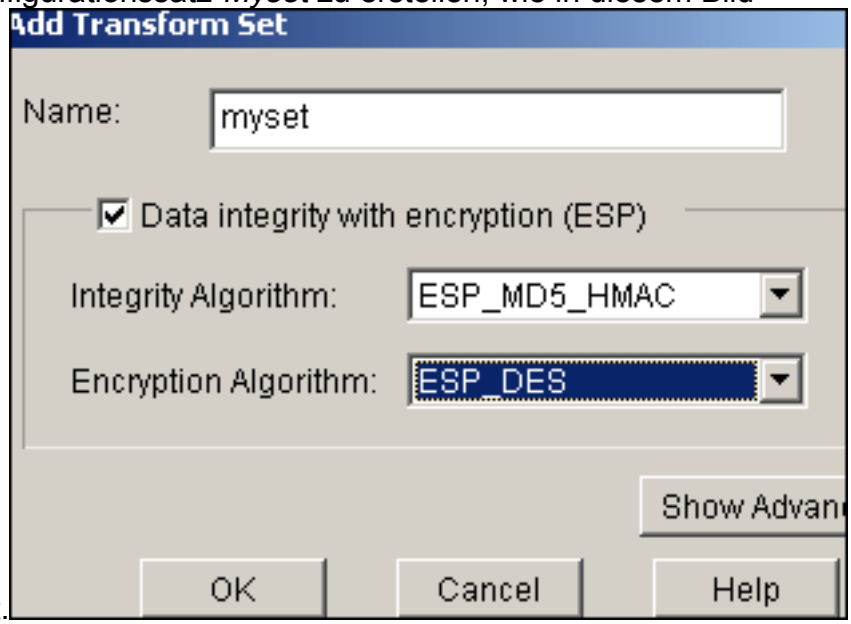


4. Klicken Sie auf **OK**.



Hinweis: Dies ist die entsprechende CLI-Konfiguration:

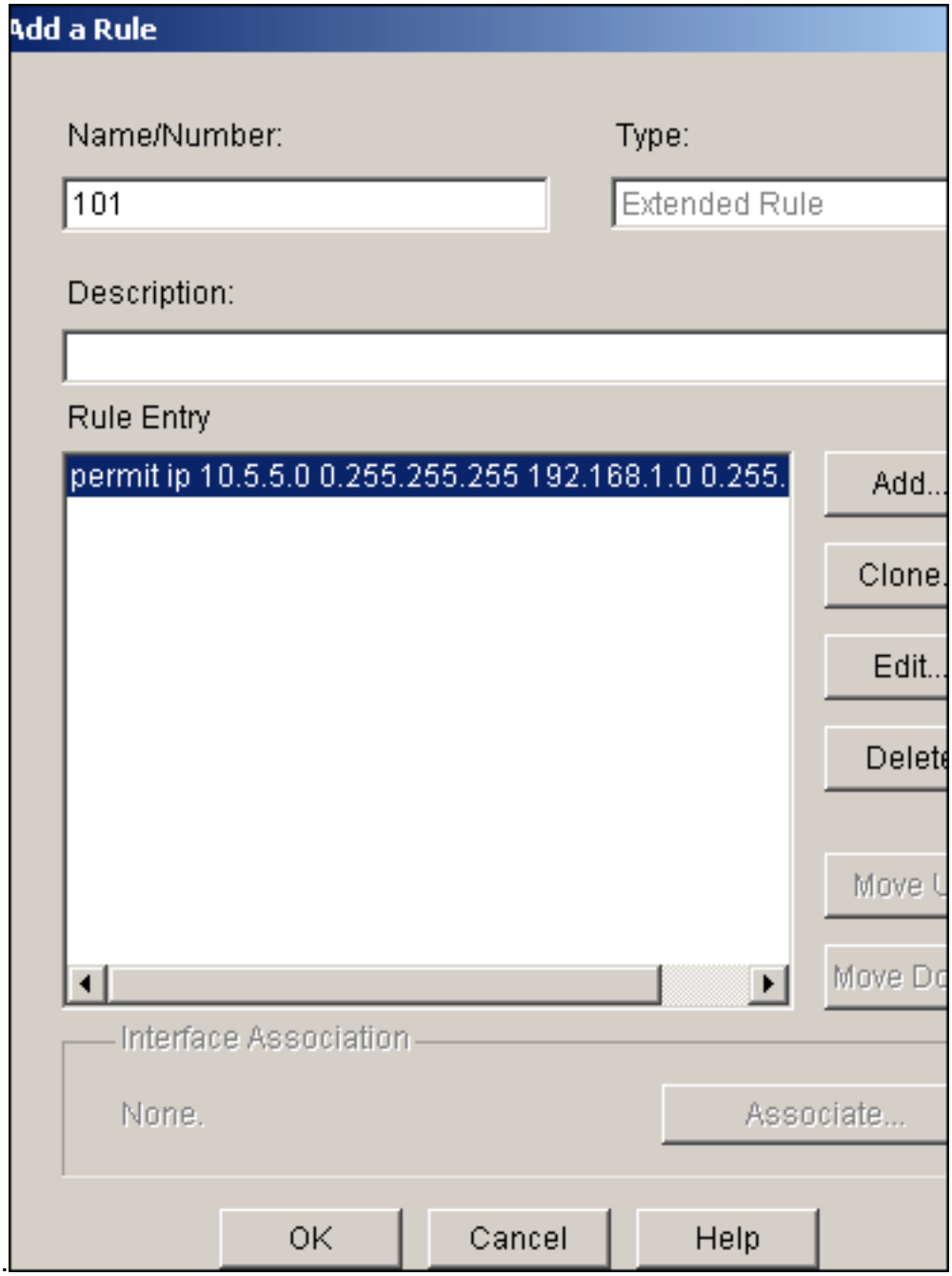
5. Wählen Sie **Configure > VPN > VPN Components > IPSec > Transform Sets > Add** aus, um ein Konfigurationssatz-*Myset* zu erstellen, wie in diesem Bild gezeigt.



6. Klicken Sie auf **OK**.

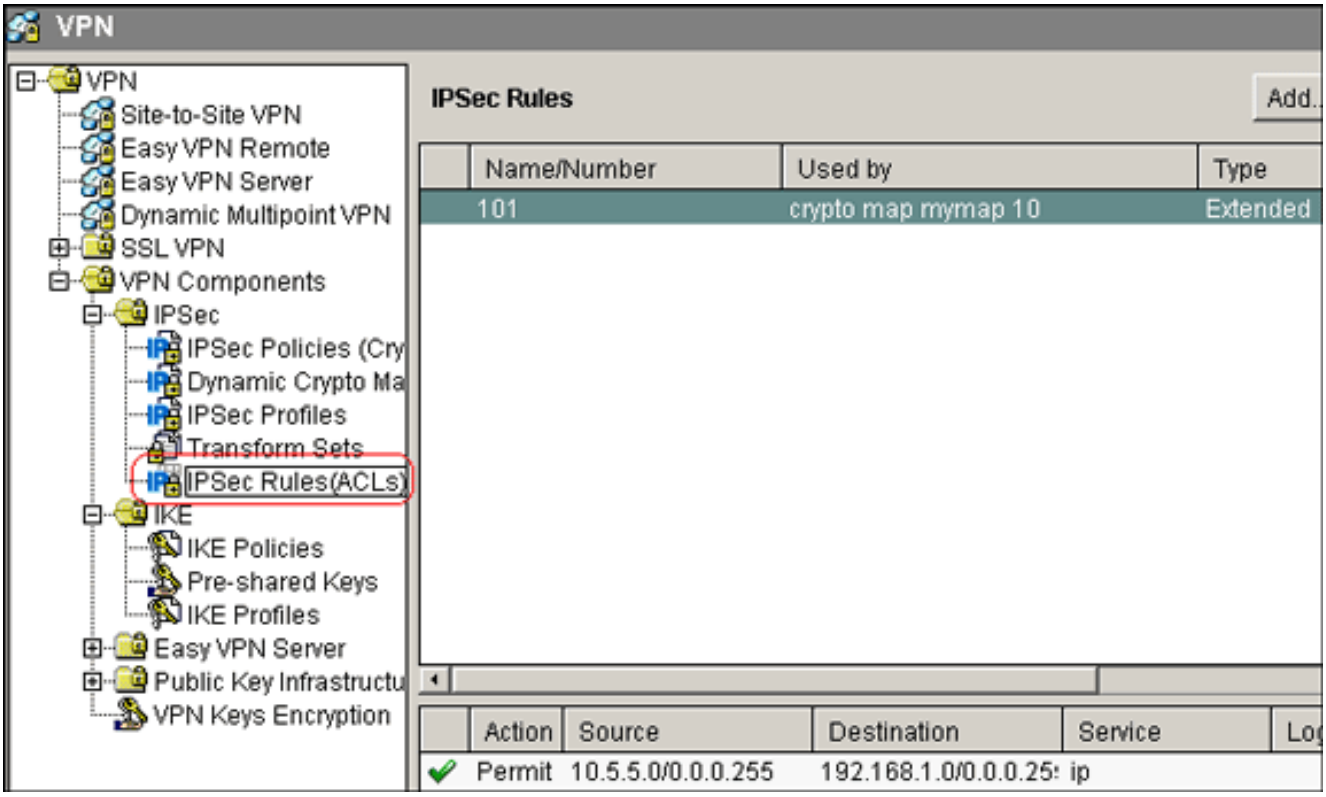
Hinweis: Dies ist die entsprechende CLI-Konfiguration:

7. Wählen Sie **Configure > VPN > VPN Components > IPSec > IPSec Rules(ACLs) > Add**, um eine Crypto Access Control List (ACL) *101* zu



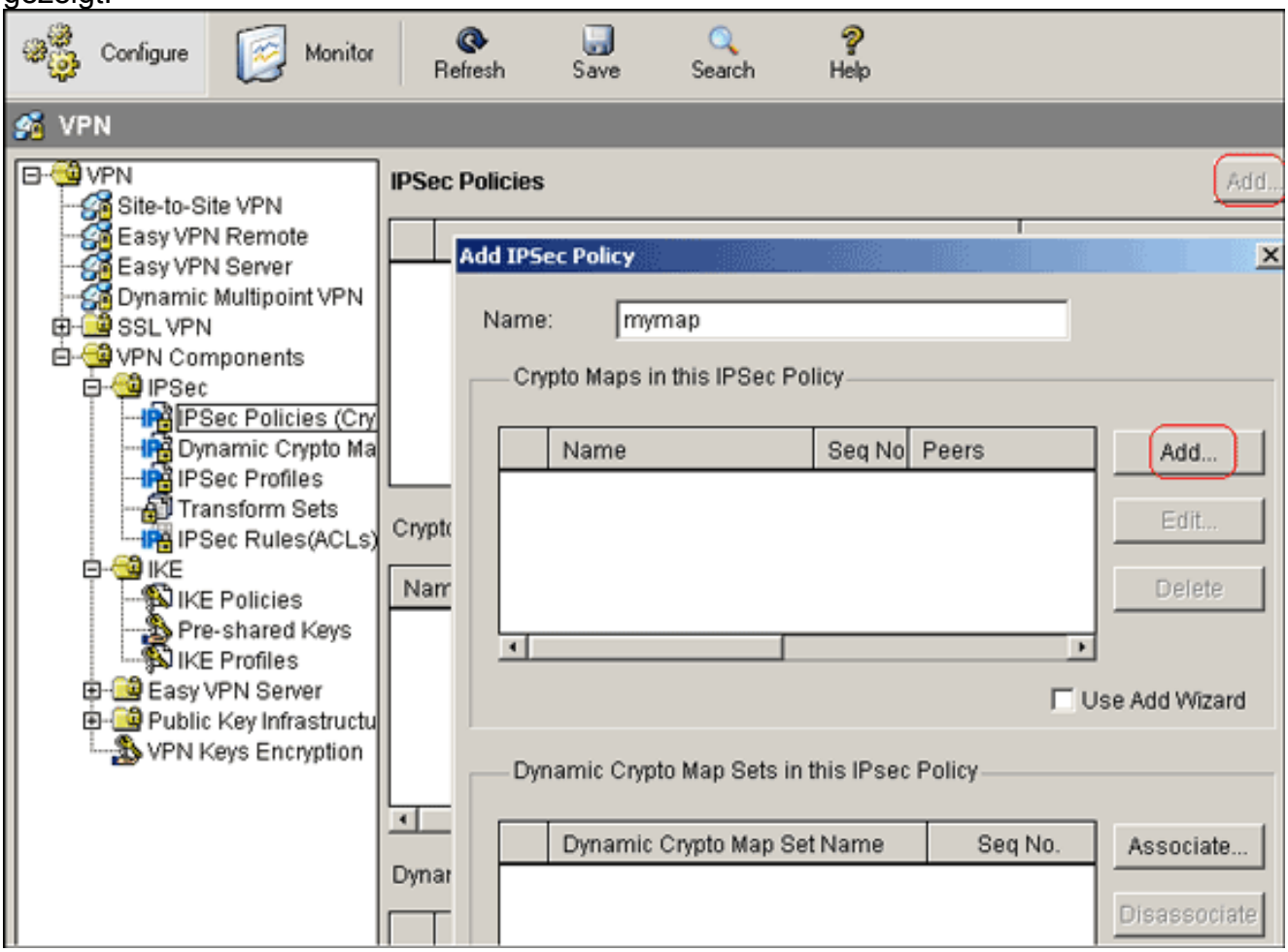
erstellen.

8. Klicken Sie auf **OK**.

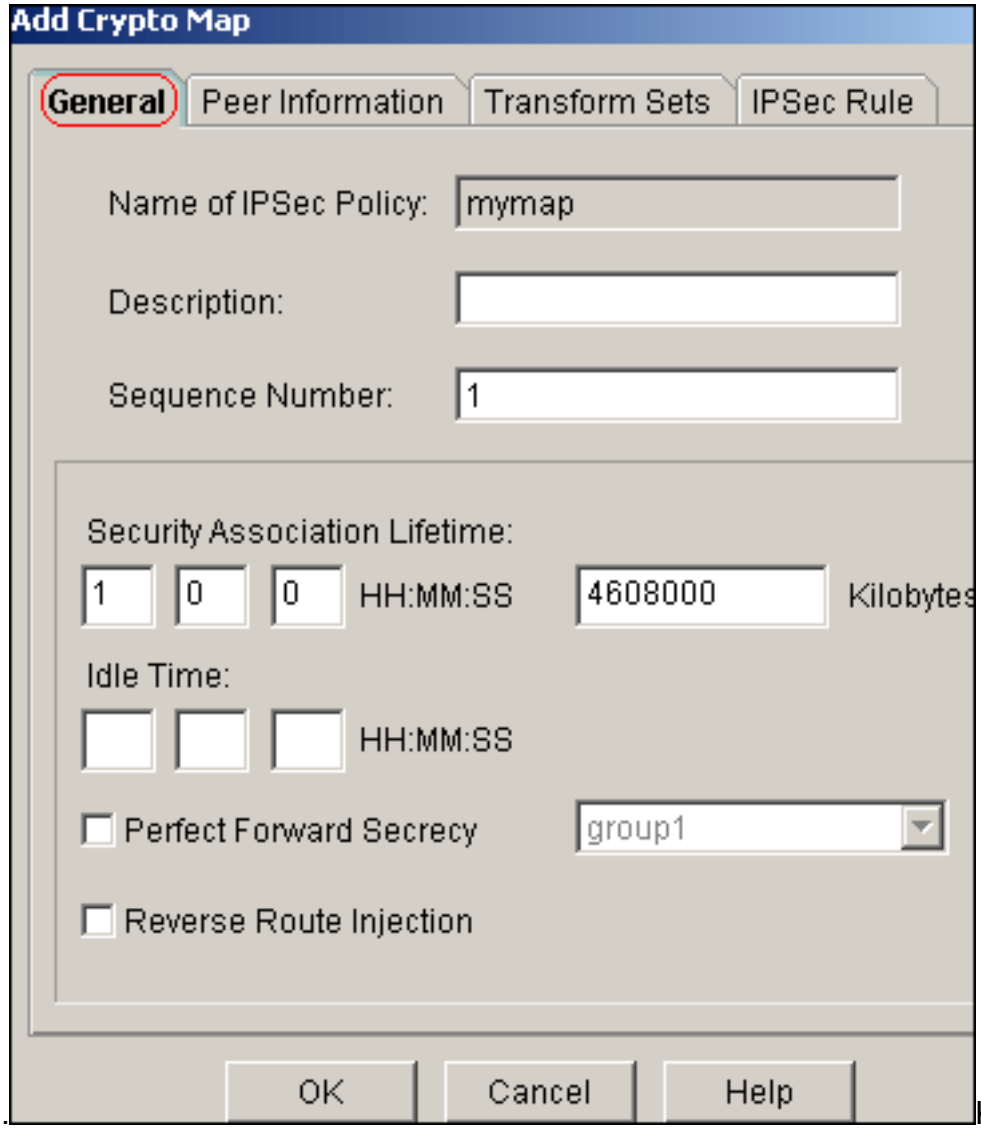


Hinweis: Dies ist die entsprechende CLI-Konfiguration:

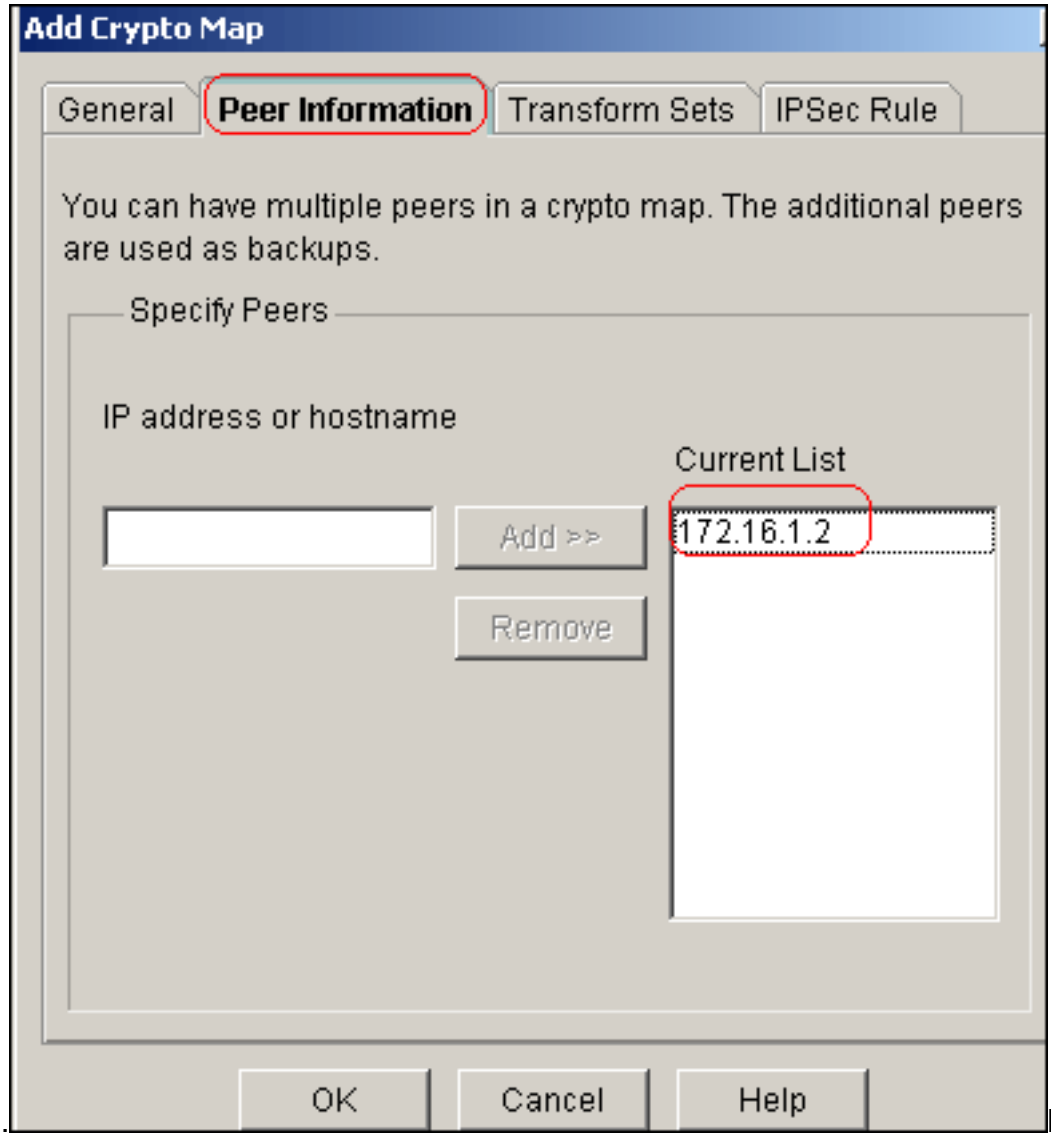
9. Wählen Sie **Configure > VPN > VPN Components > IPSec > IPSec Policies > Add** aus, um Cryto Map *mymap* zu erstellen, wie in diesem Bild gezeigt.



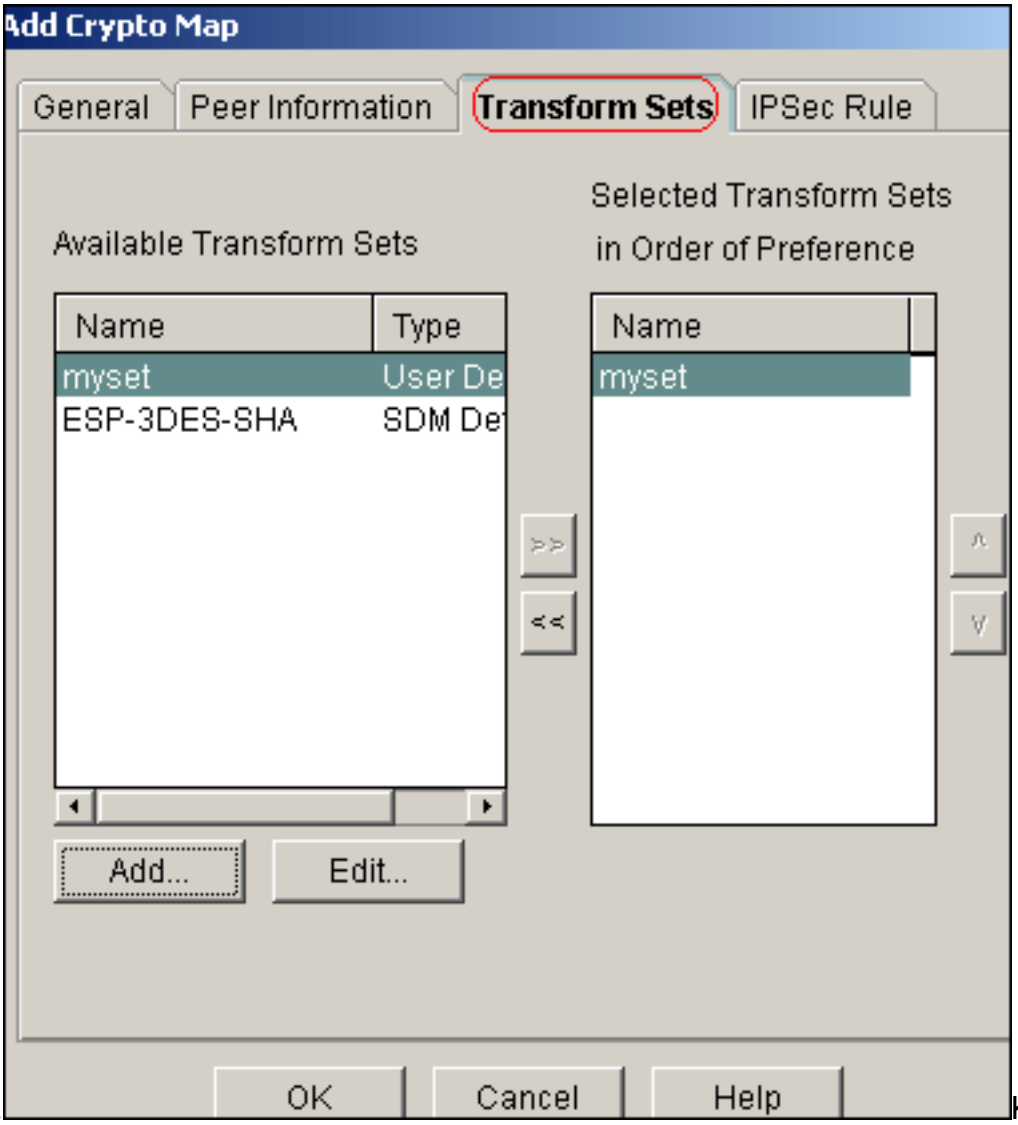
10. Klicken Sie auf **Hinzufügen**.Klicken Sie auf die Registerkarte **Allgemein**, und behalten Sie die Standardeinstellungen



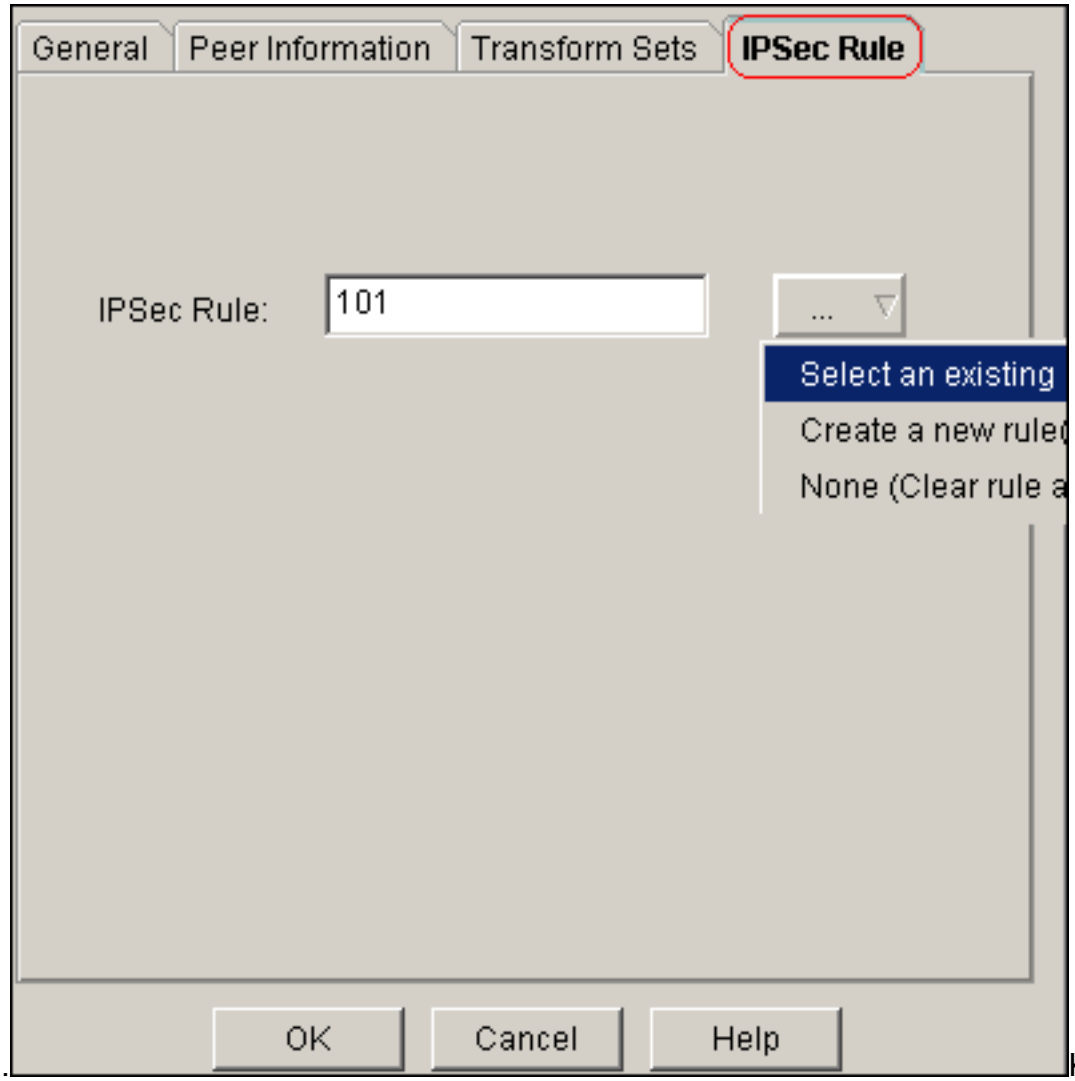
bei. Klicken Sie auf die Registerkarte **Peer Information** (Peer-IP-Adresse), um die Peer-IP-Adresse 172.16.1.2



hinzuzufügen. Klicken Sie auf die Registerkarte **Transform Sets**, um den gewünschten Transform Set *myset*

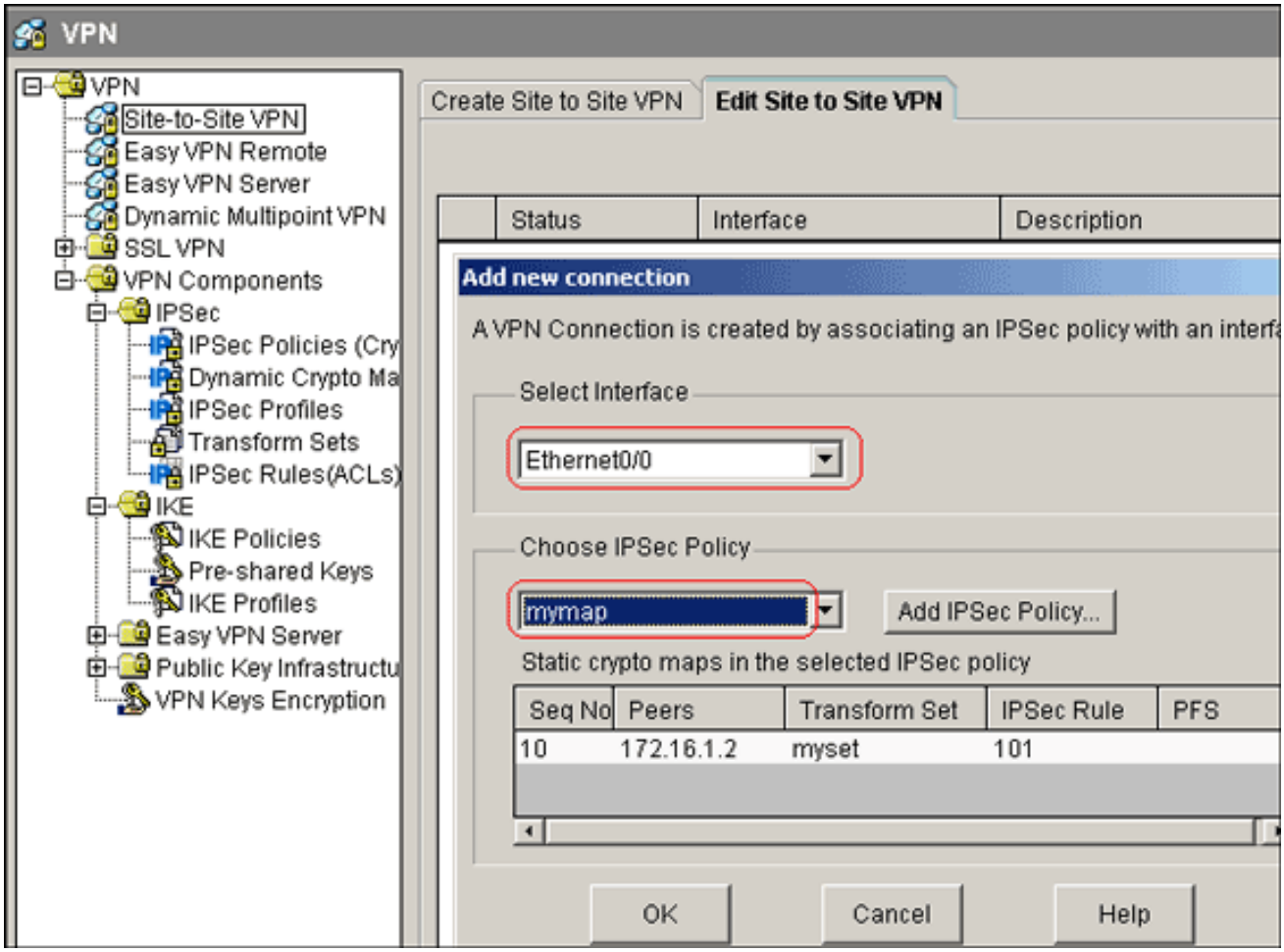


auszuwählen. Klicken Sie auf die Registerkarte **IPSec Rule** (IPSec-Regel), um die vorhandene Krypto-ACL 101



auszuwählen. Klicken Sie auf **OK**.**Hinweis:** Dies ist die entsprechende CLI-Konfiguration:

11. Wählen Sie **Configure > VPN > Site-to-Site VPN > Edit Site-to-Site VPN > Add** aus, um crypto map *mymap* auf die Schnittstelle Ethernet0/0 anzuwenden.



12. Klicken Sie auf **OK**.**Hinweis:** Dies ist die entsprechende CLI-Konfiguration:

[CLI-Konfiguration für Standort_A-Router]

Standort_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#
```

CLI-Konfiguration des Standorts_B-Routers

Standort_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#
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show crypto isakmp sa**: Zeigt alle aktuellen Sicherheitszuordnungen (SAs) für Internet Key Exchange (IKE) auf einem Peer an.

```
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
```

- **show crypto isakmp sa detail**: Zeigt die Details aller aktuellen IKE-SAs in einem Peer an.

```
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)
```

- **show crypto ipsec sa**: Zeigt die von aktuellen SAs verwendeten Einstellungen an.

```
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#
```

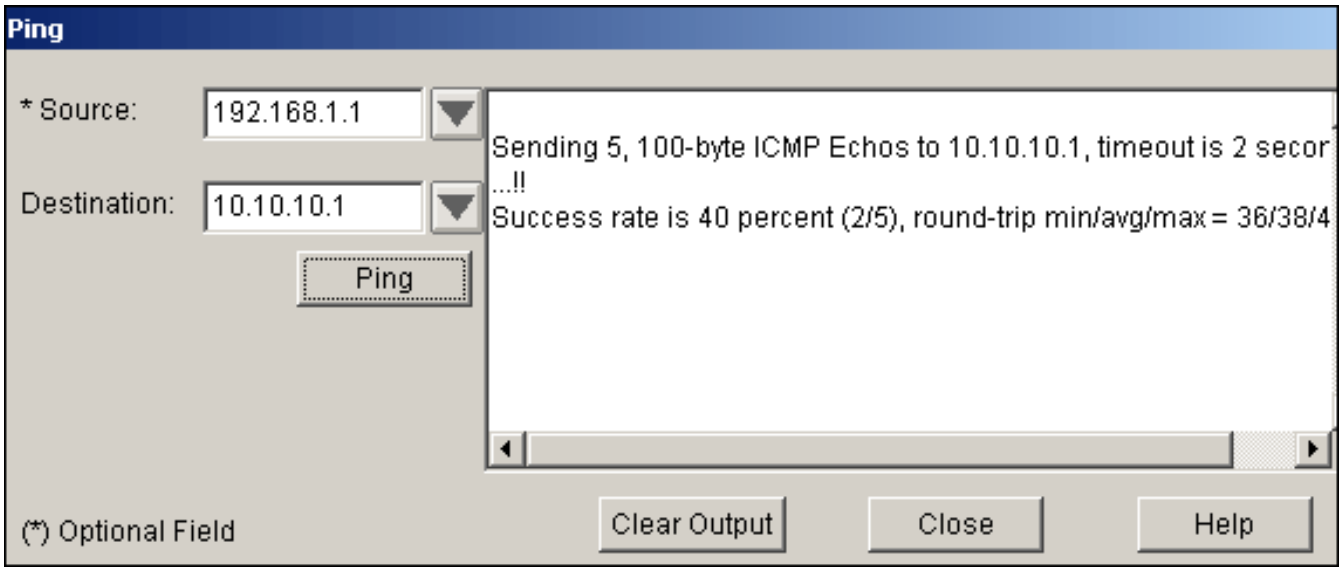
- **show ip nat translations**: Zeigt Informationen zu Übersetzungssteckplätzen an.

```
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        ---                ---
```

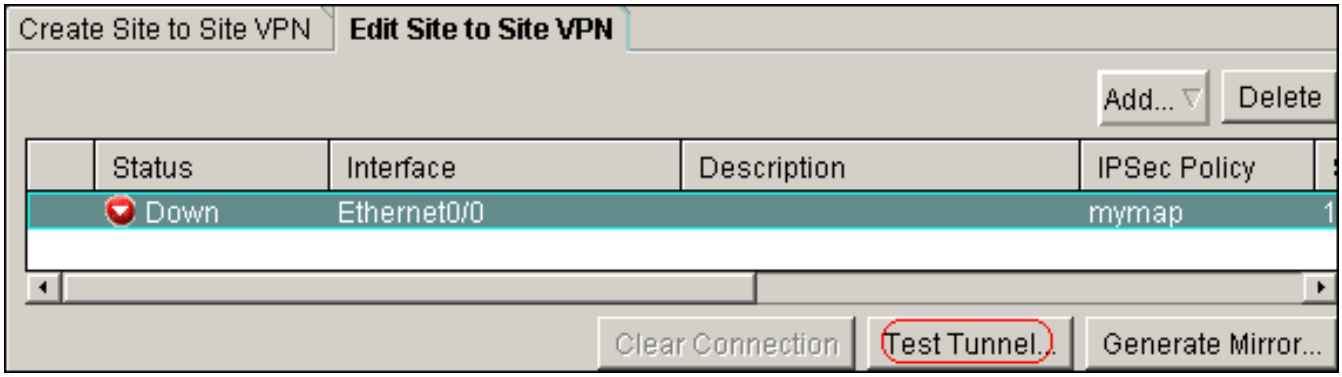
- **show ip nat statistics**: Zeigt statische Informationen über die Übersetzung an.

```
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#
```

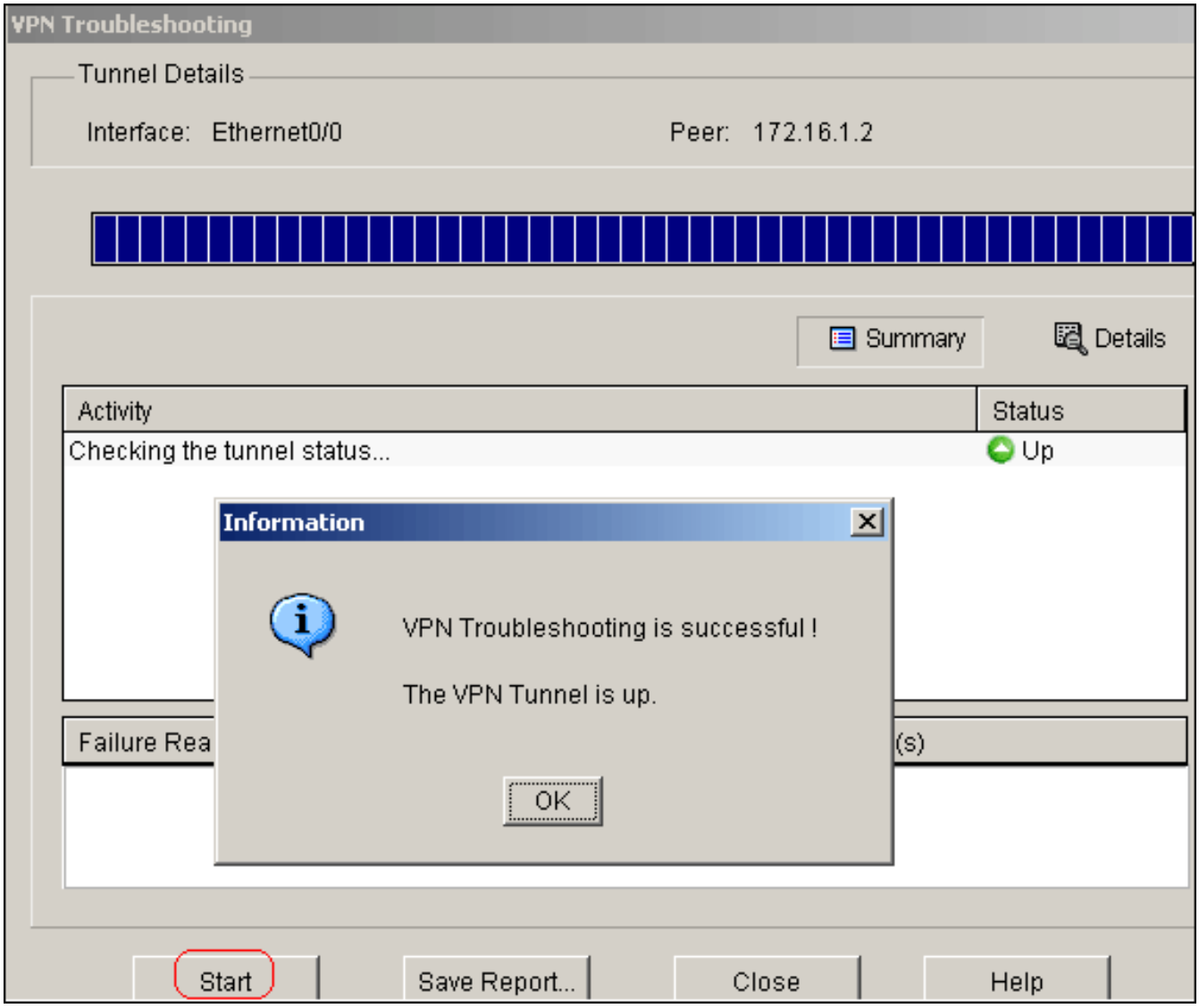
- Gehen Sie wie folgt vor, um die Verbindung zu überprüfen:Wählen Sie in SDM **Extras > Ping** aus, um den IPsec-VPN-Tunnel mit der Quell-IP als 192.168.1.1 und der Ziel-IP als 10.10.10.1
einzurichten.



Klicken Sie auf **Test Tunnel**, um zu überprüfen, ob der IPsec VPN-Tunnel wie in diesem Bild gezeigt eingerichtet
ist.



Klicken Sie auf
Start.



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

```
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
```

Zugehörige Informationen

- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Konfigurationsbeispiel für IPSec zwischen ASA/PIX und dem Cisco VPN 3000-Concentrator mit sich überschneidenden privaten Netzwerken

- Technischer Support und Dokumentation - Cisco Systems