重複のプライベート ネットワークを持つ 2 台の IOS ルータ間の IPSec の設定例

目次

概要

このドキュメントでは、VPN ゲートウェイの背後でプライベート ネットワーク アドレスが重複しているサイト間 IPSec VPN 内で Cisco IOS ルータを設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 12.4 が稼働している Cisco IOS 3640 ルータに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

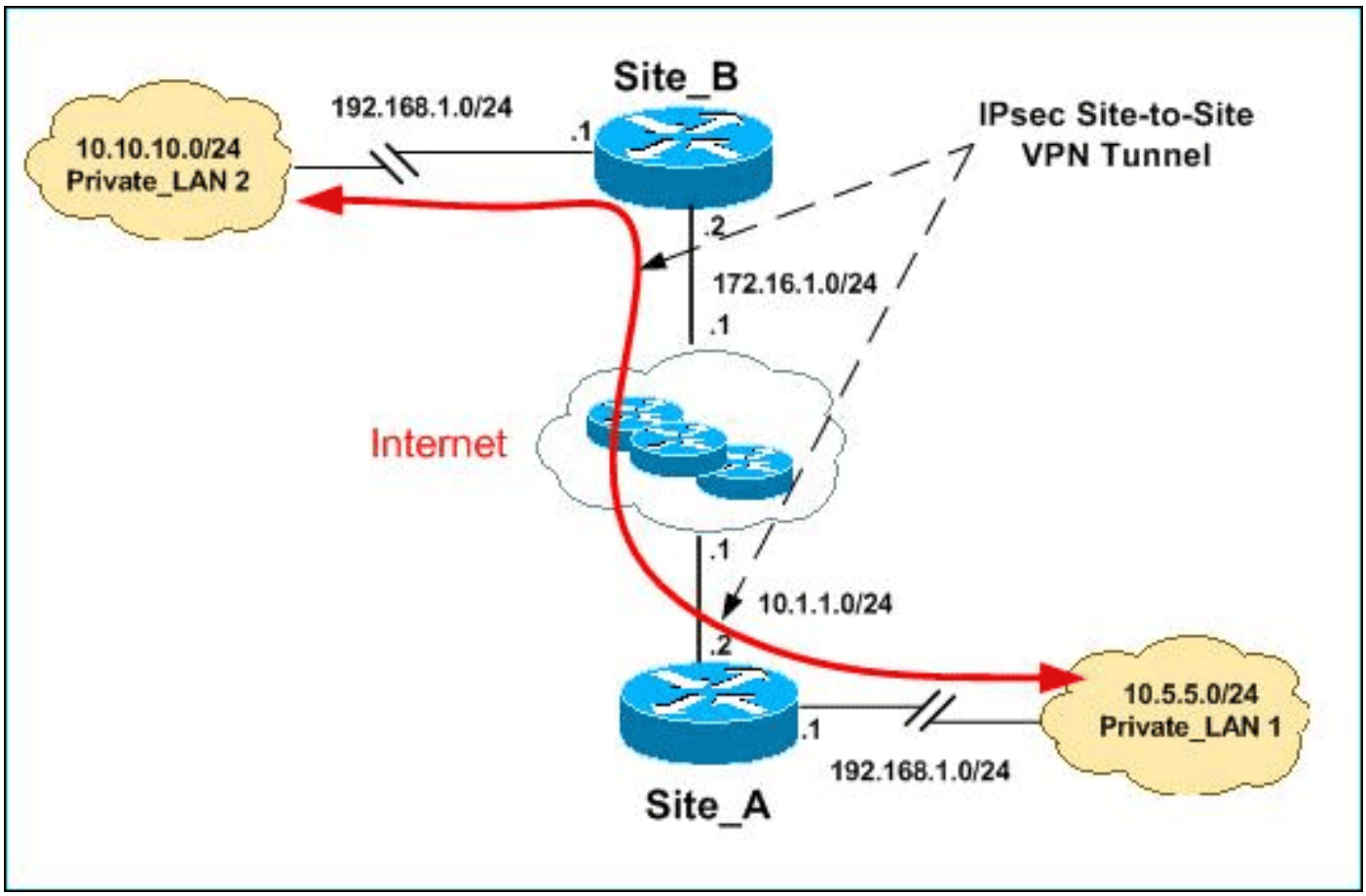
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらはラボ環境で使用された RFC 1918 でのアドレスです。

Private_LAN1 と Private_LAN2 の両方に、192.168.1.0/24 の IP サブネットがあります。 これは、IPSec トンネルのそれぞれの側の背後にある重複しているアドレス空間をシミュレートします。

この例では、Site_A ルータが双方向の変換を実行するため、2 つのプライベート LAN が IPSec トンネルを介して通信できます。 変換は、Private_LAN1 が IPSec トンネルを介して Private_LAN2 を 10.10.10.0/24 と見なし、Private_LAN2 は IPSec トンネルを介して Private_LAN1 を 10.5.5.0/24 と見なすことを意味します。

設定

このドキュメントでは、次の設定を使用します。

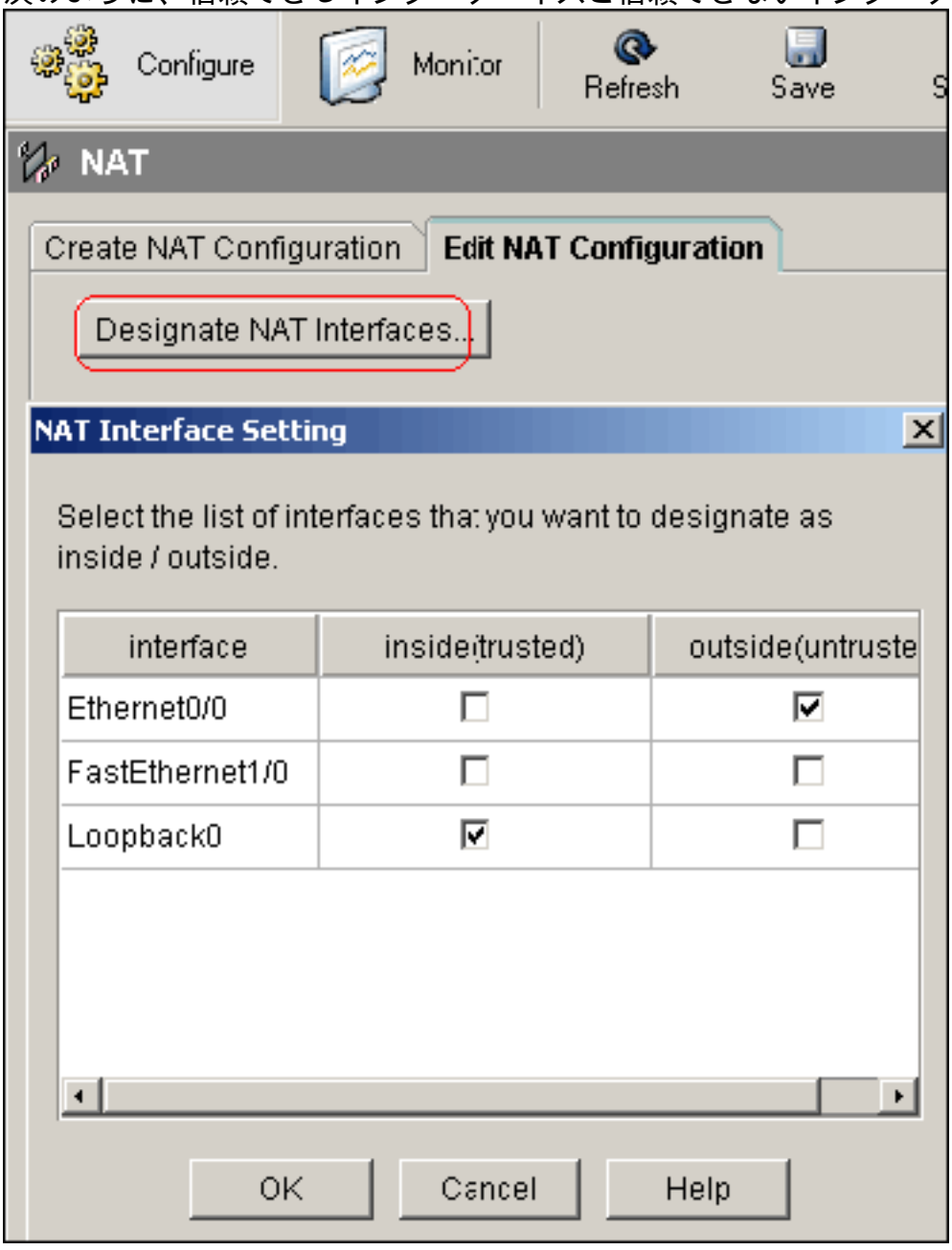
Site_A ルータの SDM 設定

注: このドキュメントでは、ルータはインターフェイスの設定などの基本設定が使用されていることを前提としています。詳細については、『SDM を使用した基本的なルータ設定』を参照してください。

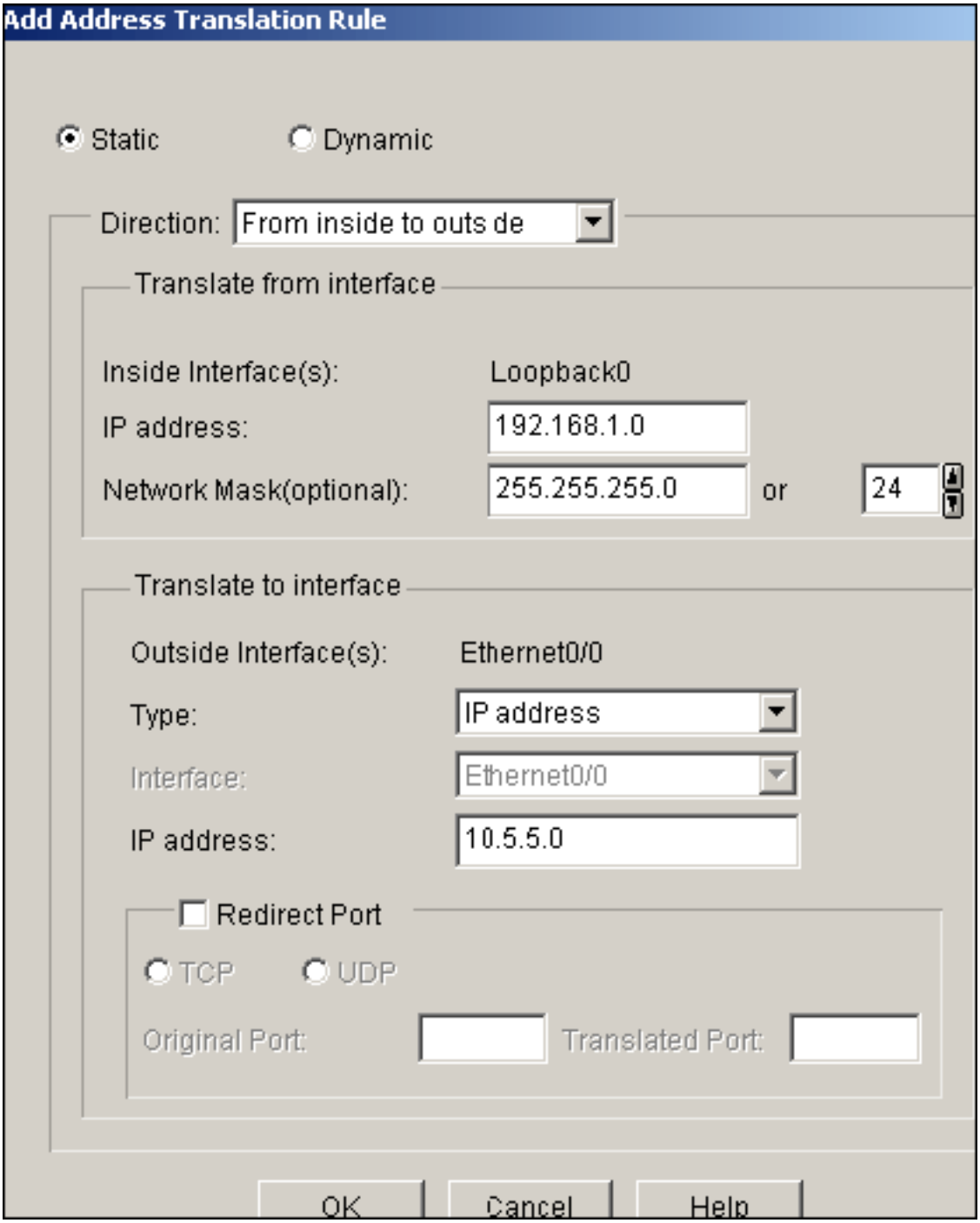
NAT 設定

NAT を使用して Site_A ルータで SDM を設定するには、次の手順を実行してください。

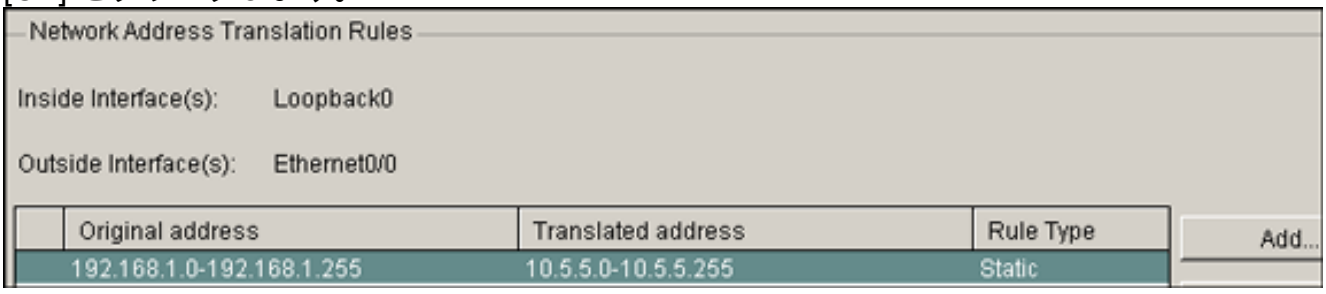
1. [Configure] > [NAT] > [Edit NAT Configuration] を選択し、[Designate NAT Interfaces] をクリックして、次のように、信頼できるインターフェイスと信頼できないインターフェイスを定義します。



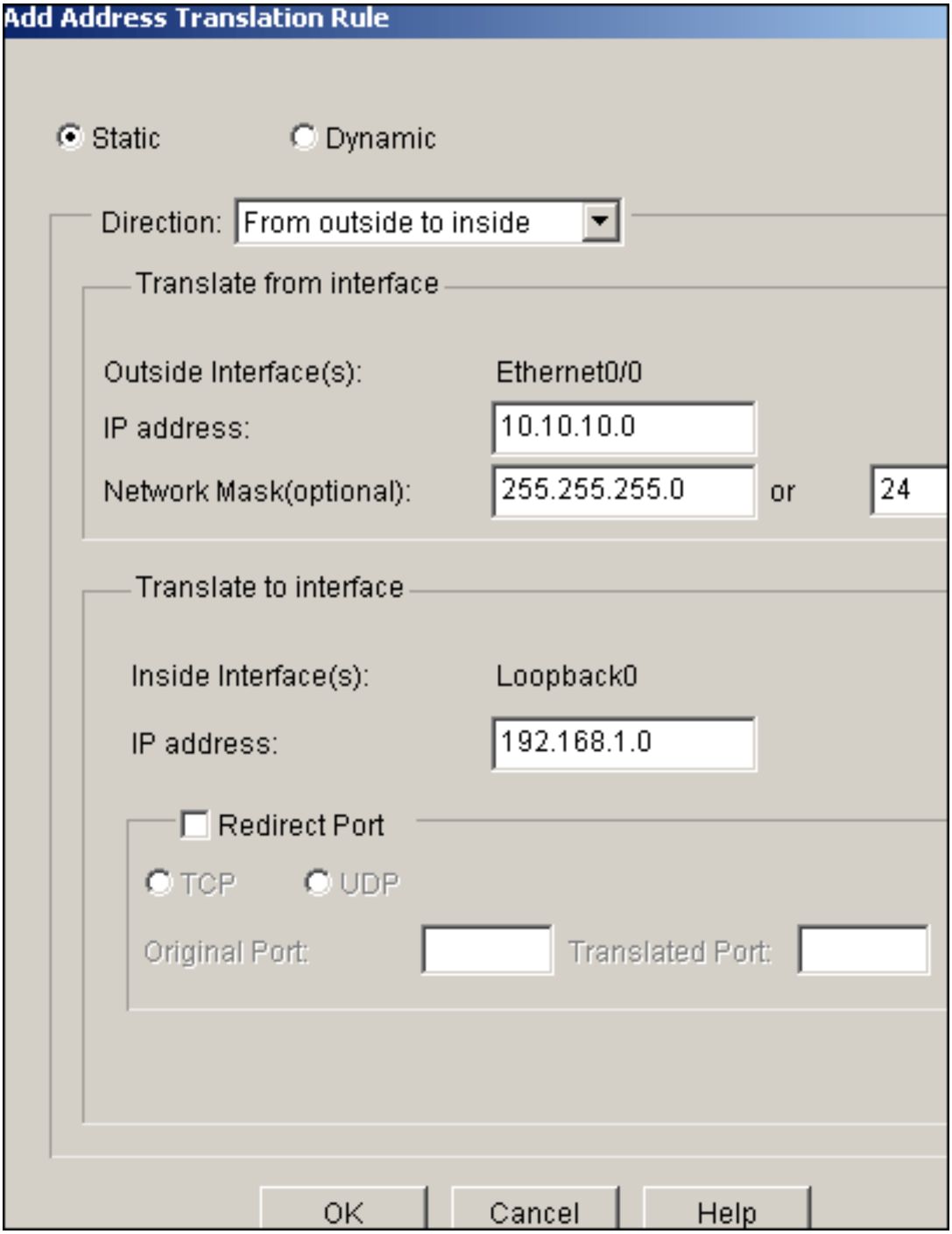
2. [OK] をクリックします。
3. [Add] をクリックして、次のように内部から外部方向の NAT 変換を設定します。



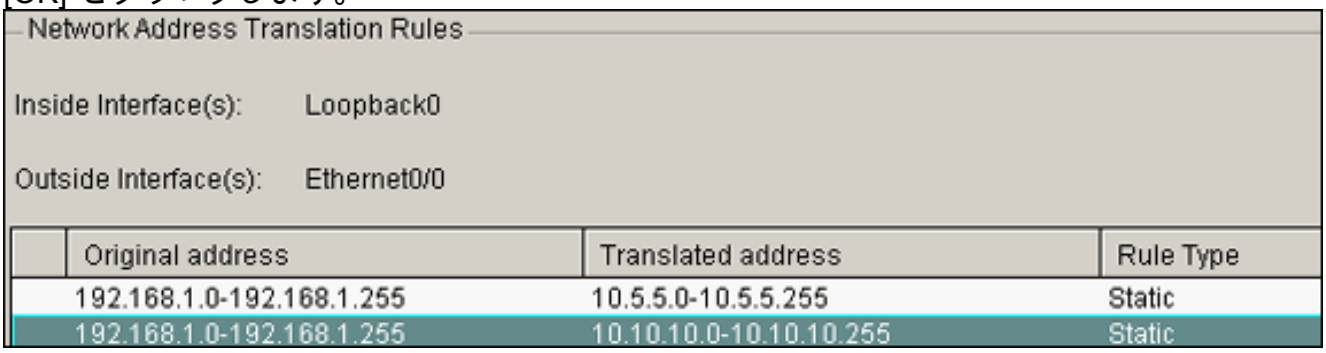
4. [OK] をクリックします。



5. もう一度 [Add] をクリックして、次のように外部から内部方向の NAT 変換を設定します。



6. [OK] をクリックします。



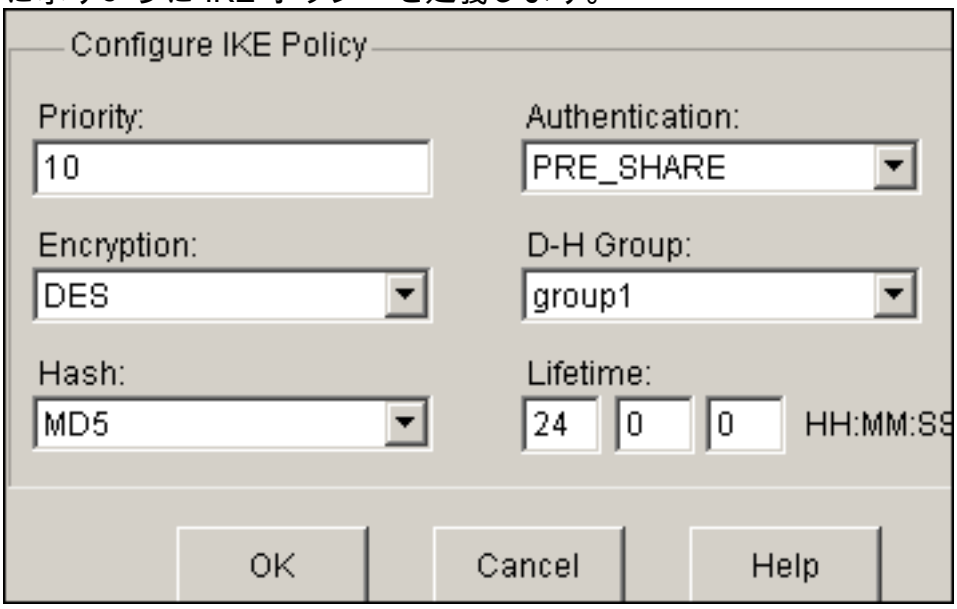
注: 同等の CLI 設定は次のようになります。

VPN の設定

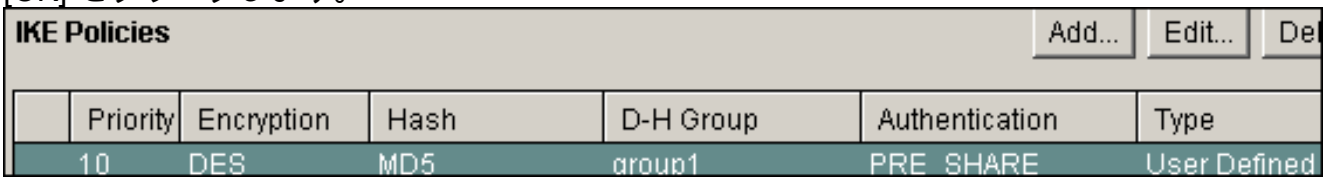
VPN を使用して Site_A ルータで SDM を設定するには、次の手順を実行してください。

1. [Configure] > [VPN] > [VPN Components] > [IKE] > [IKE Policies] > [Add] を選択し、次の図

に示すように IKE ポリシーを定義します。

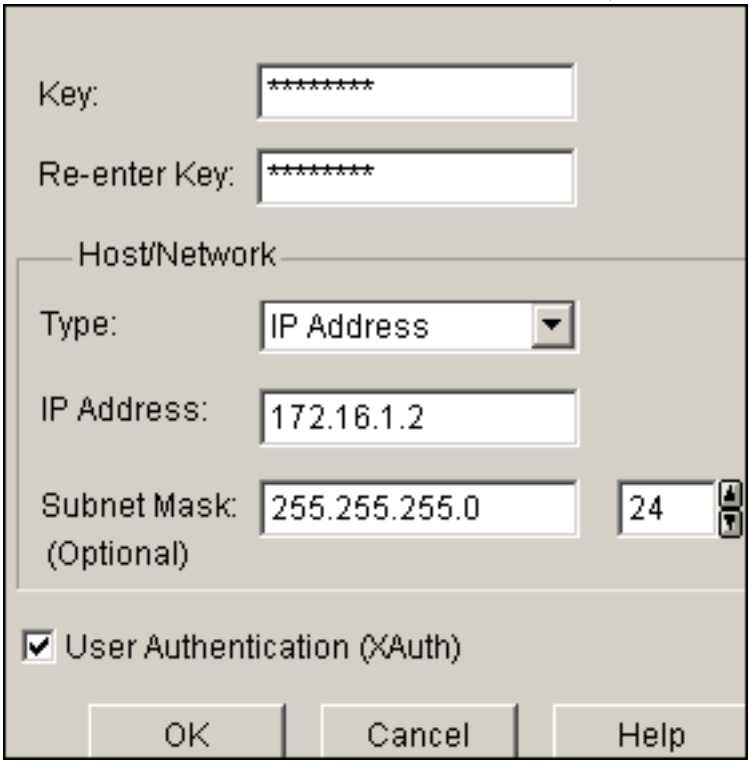


2. [OK] をクリックします。

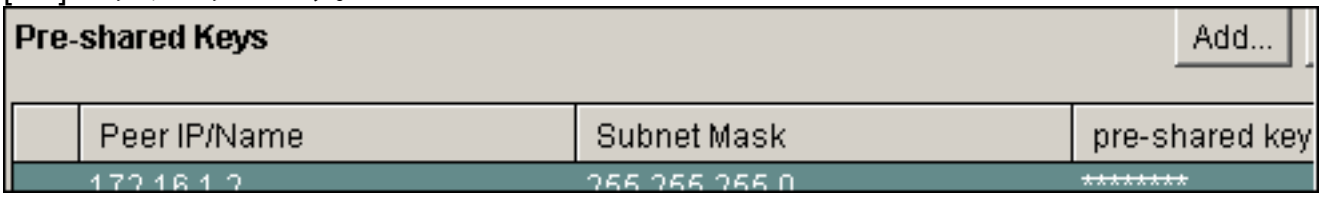


注: 同等の CLI 設定は次のようになります。

3. [Configure] > [VPN] > [VPN Components] > [IKE] > [Pre-shared Keys] > [Add] を選択し、ピア IP アドレスと事前共有キーを設定します。

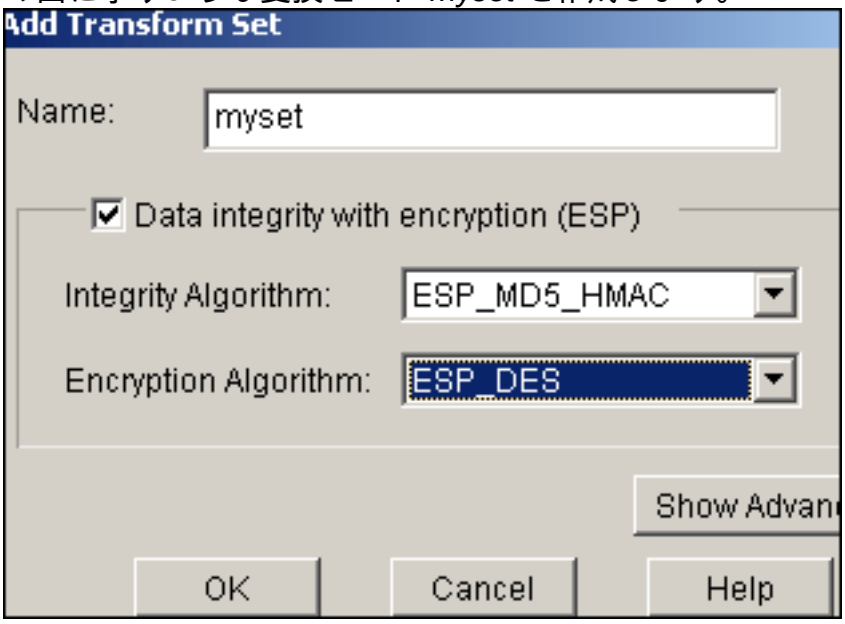


4. [OK] をクリックします。



注: 同等の CLI 設定は次のようになります。

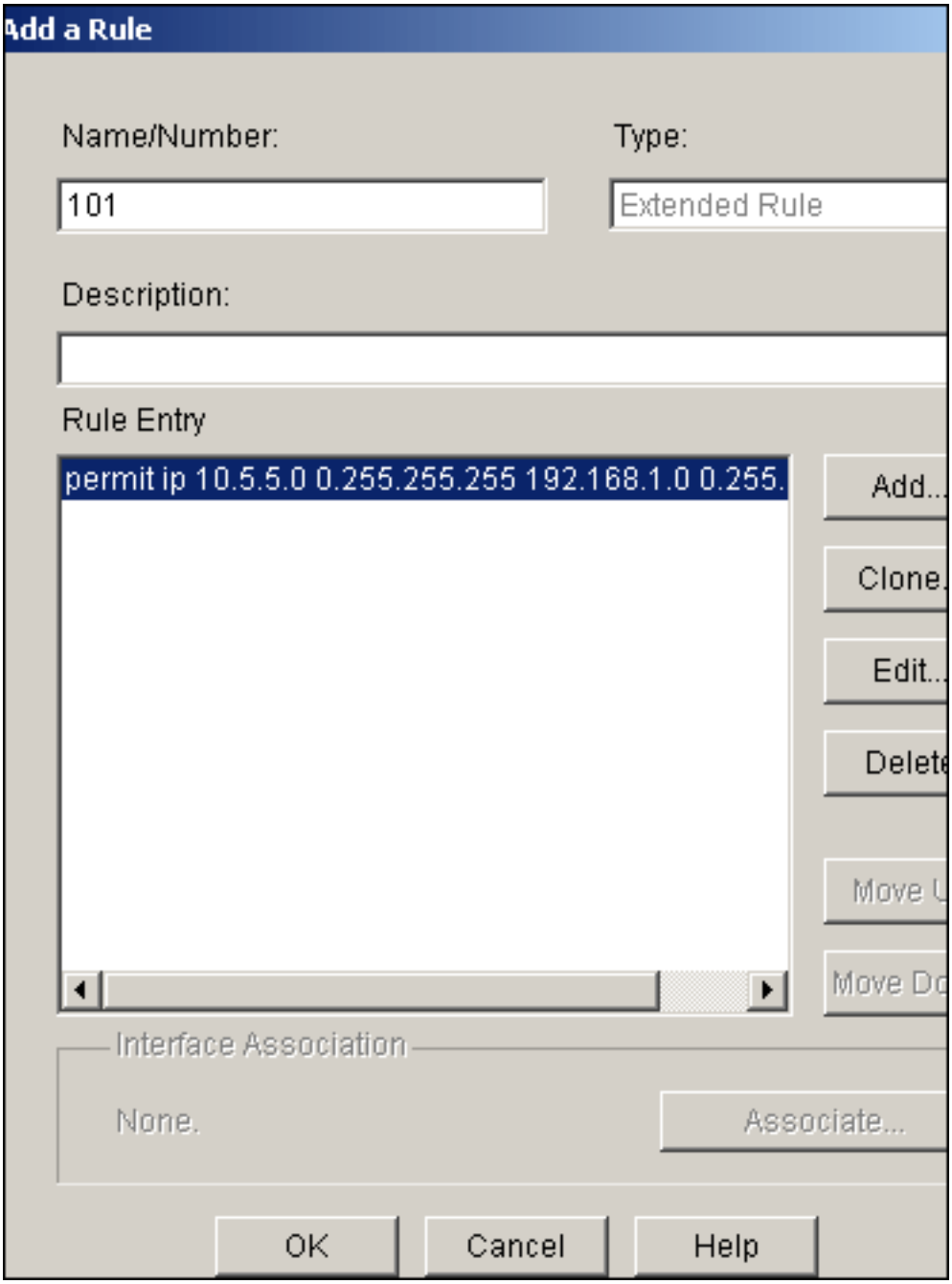
5. [Configure] > [VPN] > [VPN Components] > [IPSec] > [Transform Sets] > [Add] を選択し、次の図に示すような変換セット *myset* を作成します。



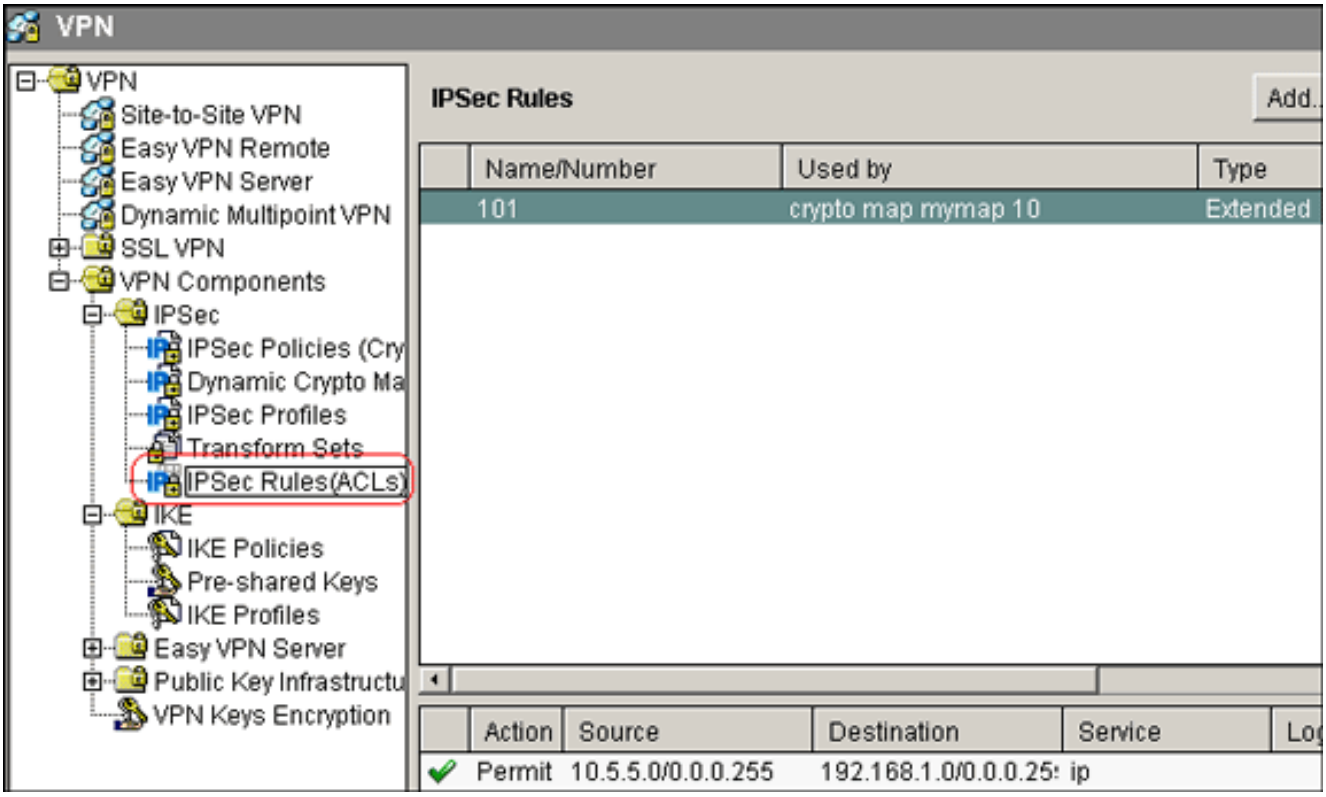
6. [OK] をクリックします。

注: 同等の CLI 設定は次のようになります。

7. [Configure] > [VPN] > [VPN Components] > [IPSec] > [IPSec Rules(ACLs)] > [Add] を選択し、暗号化アクセス コントロール リスト（ACL）*101* を作成します。

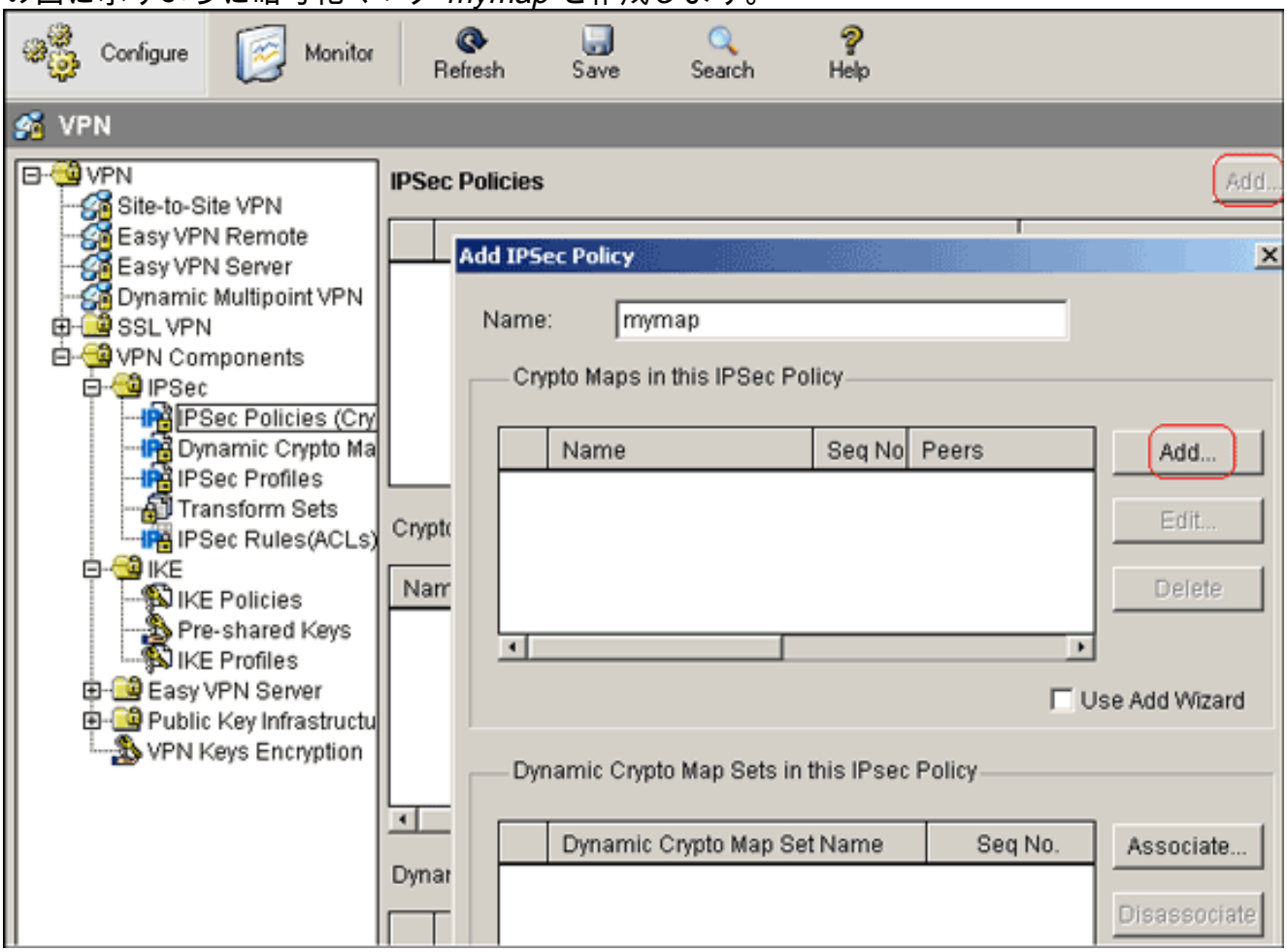


8. [OK] をクリックします。

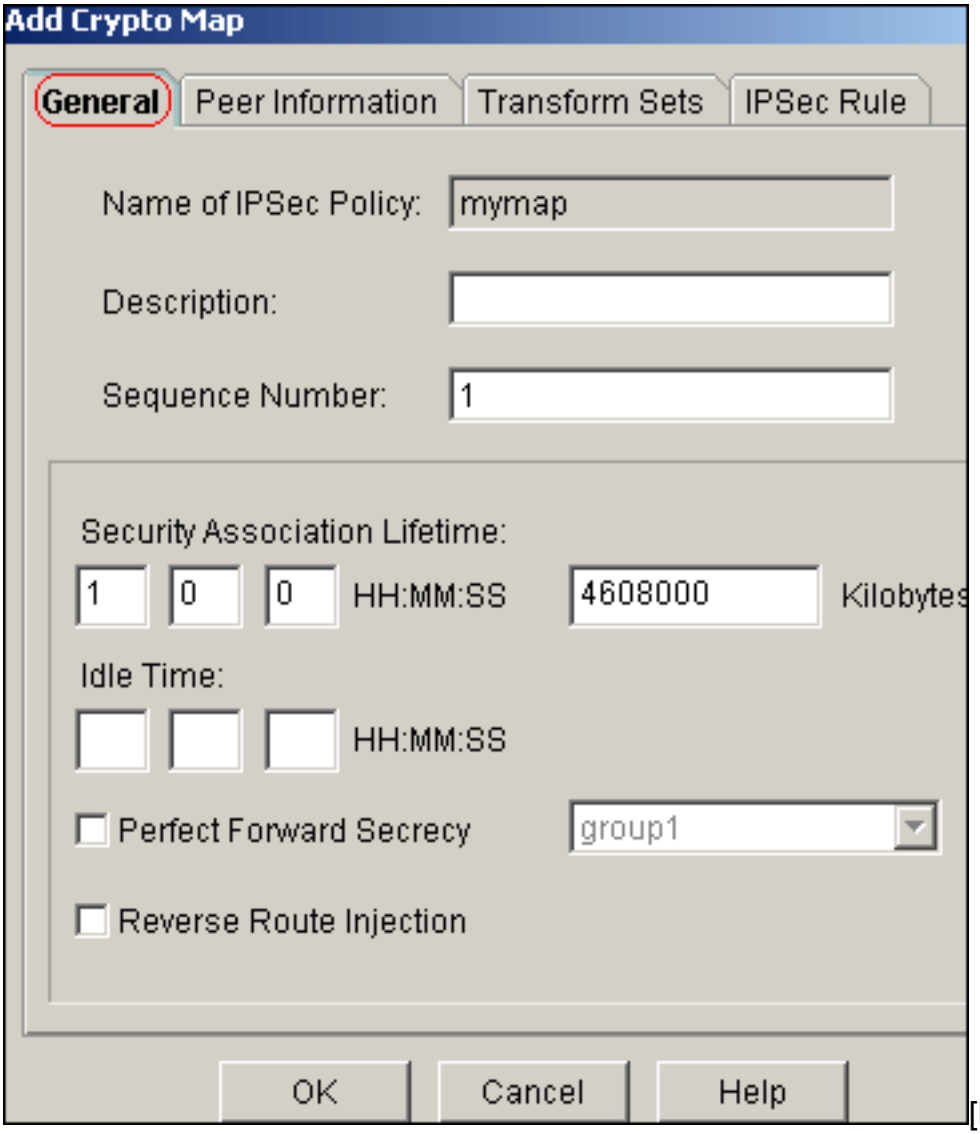


注: 同等の CLI 設定は次のようになります。

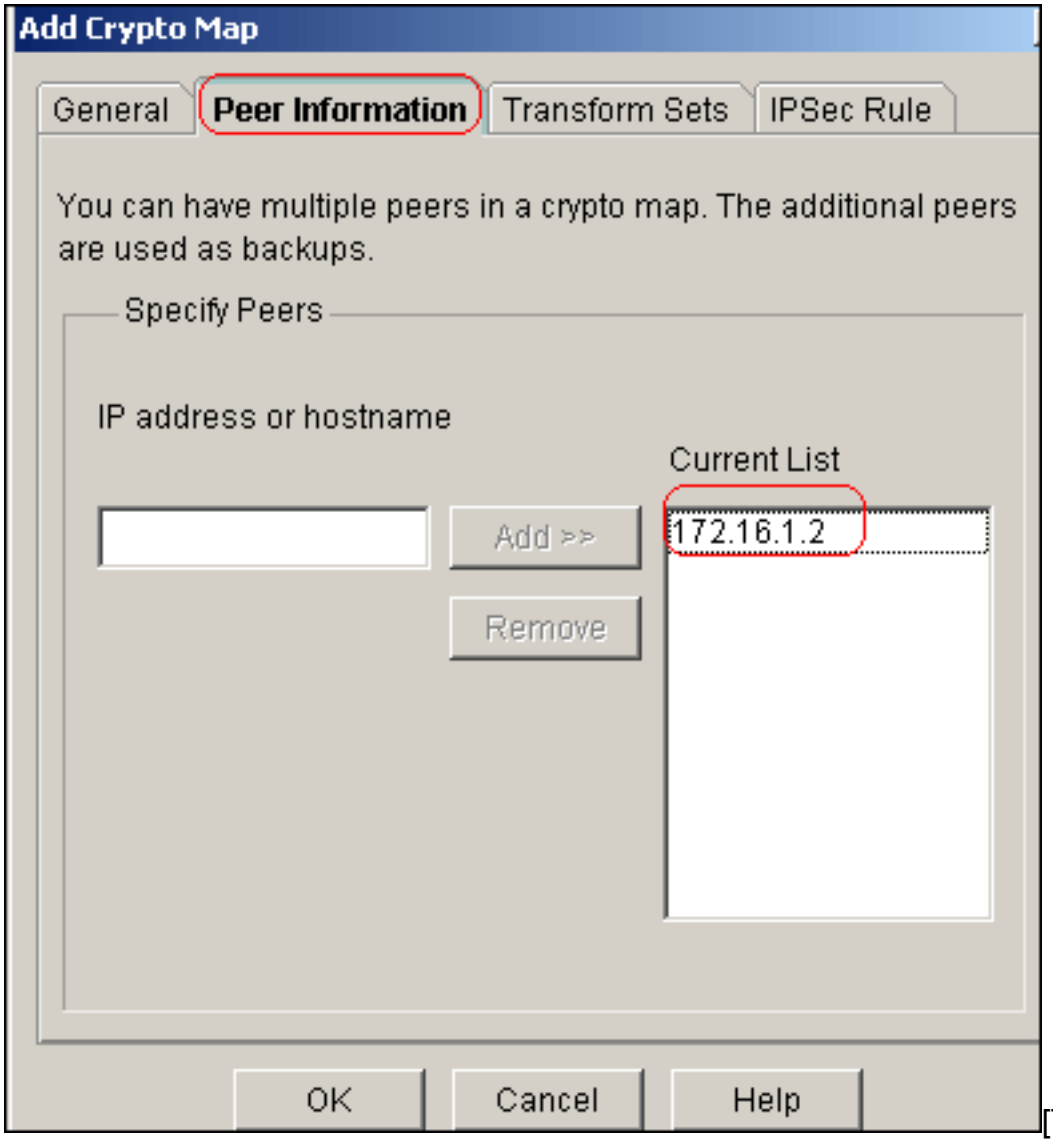
9. [Configure] > [VPN] > [VPN Components] > [IPSec] > [IPSec Policies] > [Add] を選択し、次の図に示すように暗号化マップ *mymap* を作成します。



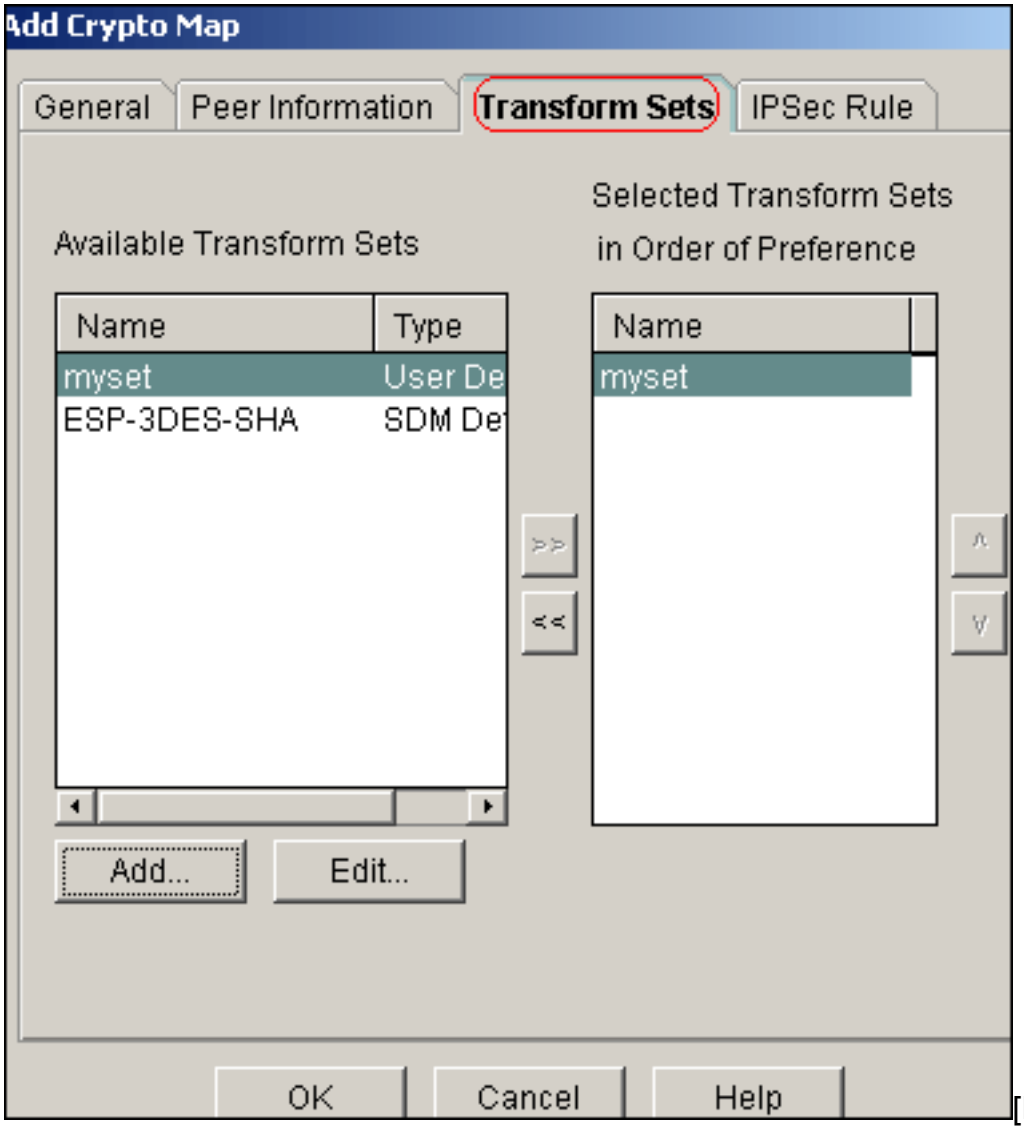
10. [Add] をクリックします。[General] タブをクリックし、デフォルトの設定のままにしてお



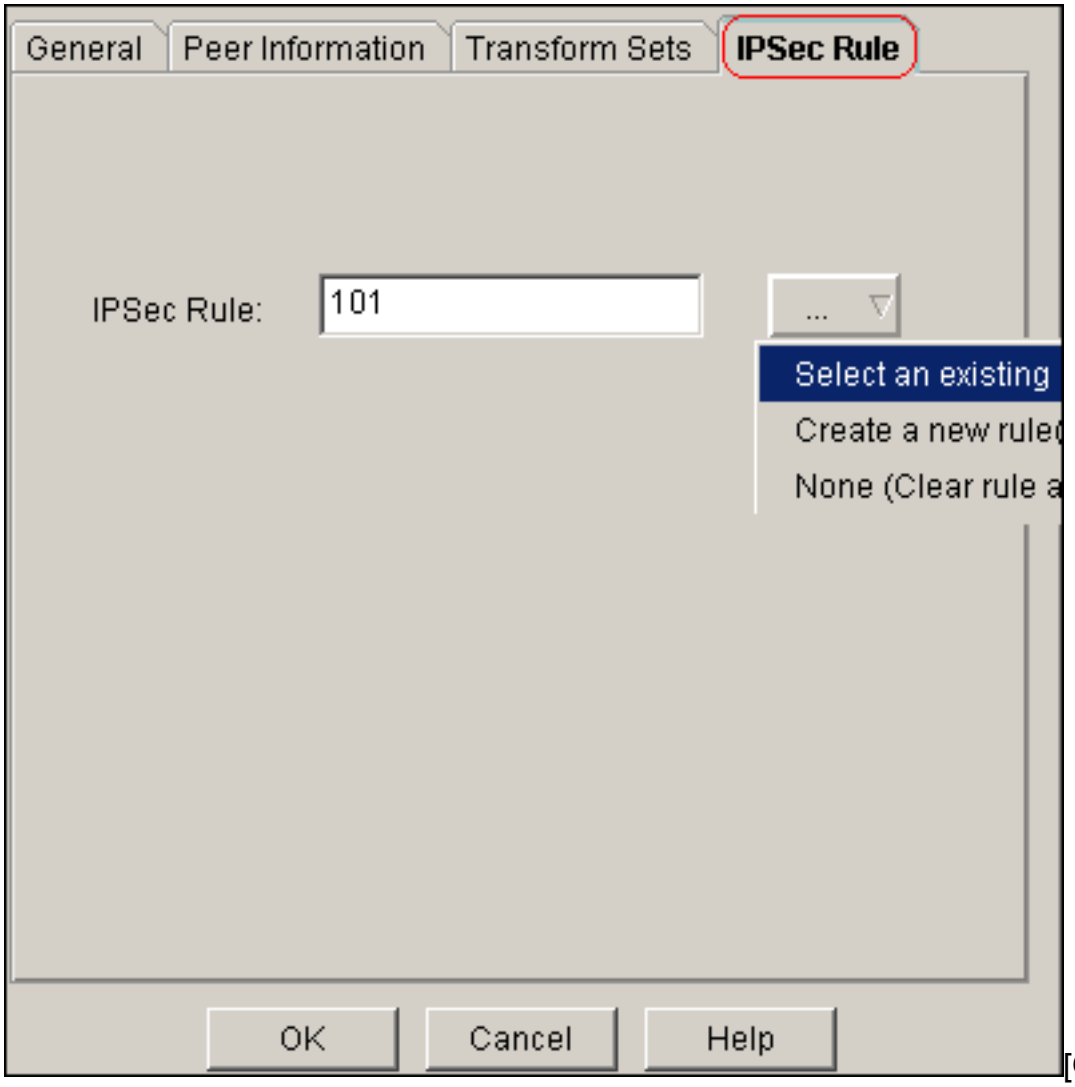
きます。[Peer Information] タブをクリックして、ピア IP アドレス 172.16.1.2 を追加します。



[Transform Sets] タブをクリックして、対象の変換セット *myset* を選択します。

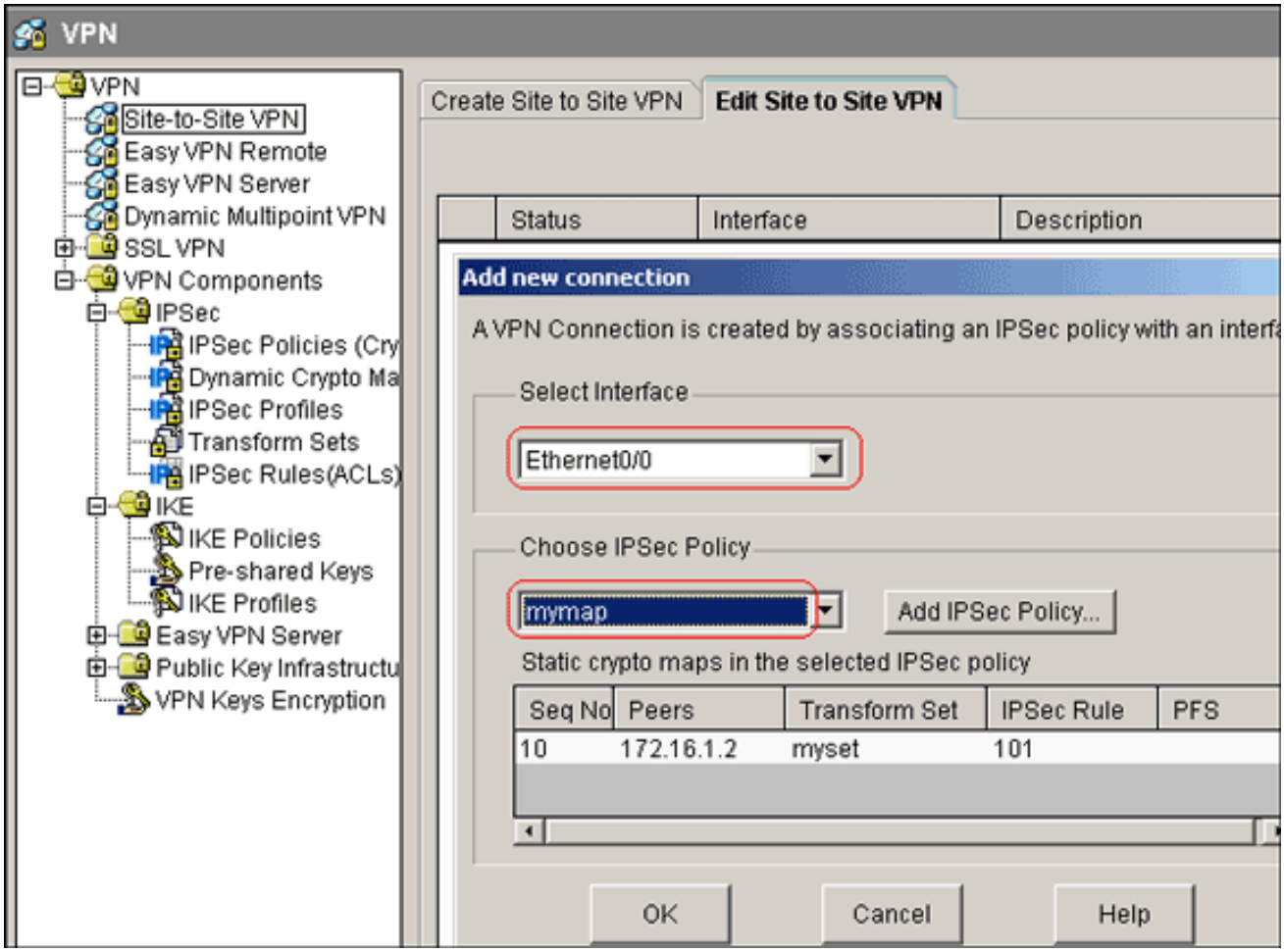


[IPSec Rule] タブをクリックして、既存の暗号化 ACL 101 を選択します。



[OK] をクリックします。**注:** 同等の CLI 設定は次のようになります。

11. [Configure] > [VPN] > [Site-to-Site VPN] > [Edit Site-to-Site VPN] > [Add] を選択して、暗号化マップ *mymap* をインターフェイス Ethernet0/0 へ適用します。



12. [OK] をクリックします。**注:** 同等の CLI 設定は次のようになります。

Site_A ルータの CLI 設定

Site_A ルータ

```
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#
```

Site_B ルータ の CLI 設定

Site_B ルータ

```
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#
```

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show crypto isakmp sa**：ピアにおける現在のインターネット鍵交換（IKE）セキュリティ アソシエーション（SA）をすべて表示します。`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**：ピアにおける現在の IKE SA の詳細を表示します。`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**：現在の SA で使用されている設定を表示します。`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#
```

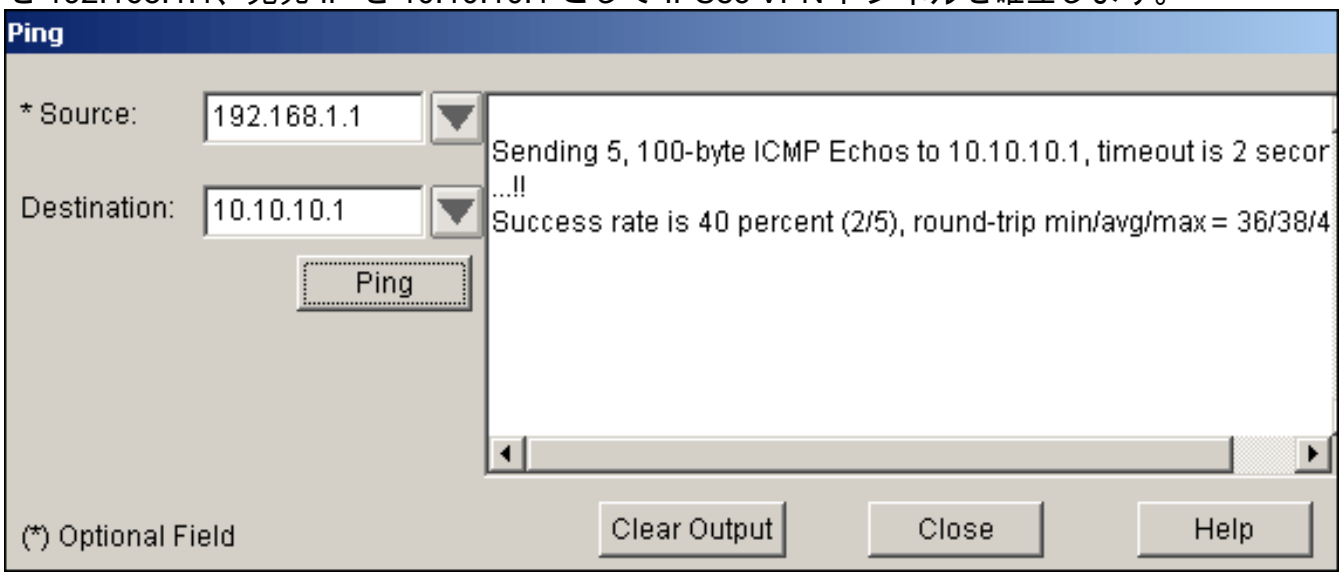
- **show ip nat translations** ：変換スロットの情報を表示します。`Site_A#show ip nat translations`

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

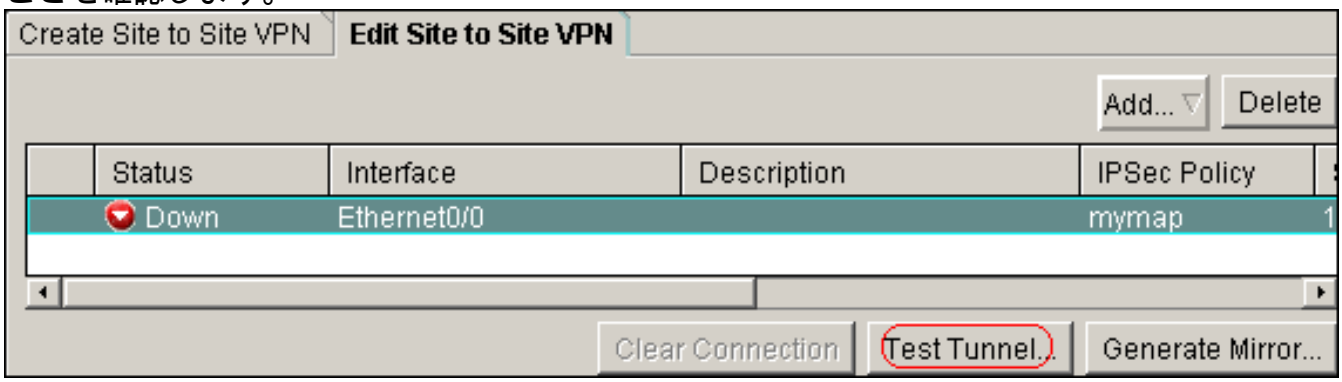
- **show ip nat statistics** ：変換に関する静的な情報を表示します。`Site_A#show ip nat statistics`

```
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#
```

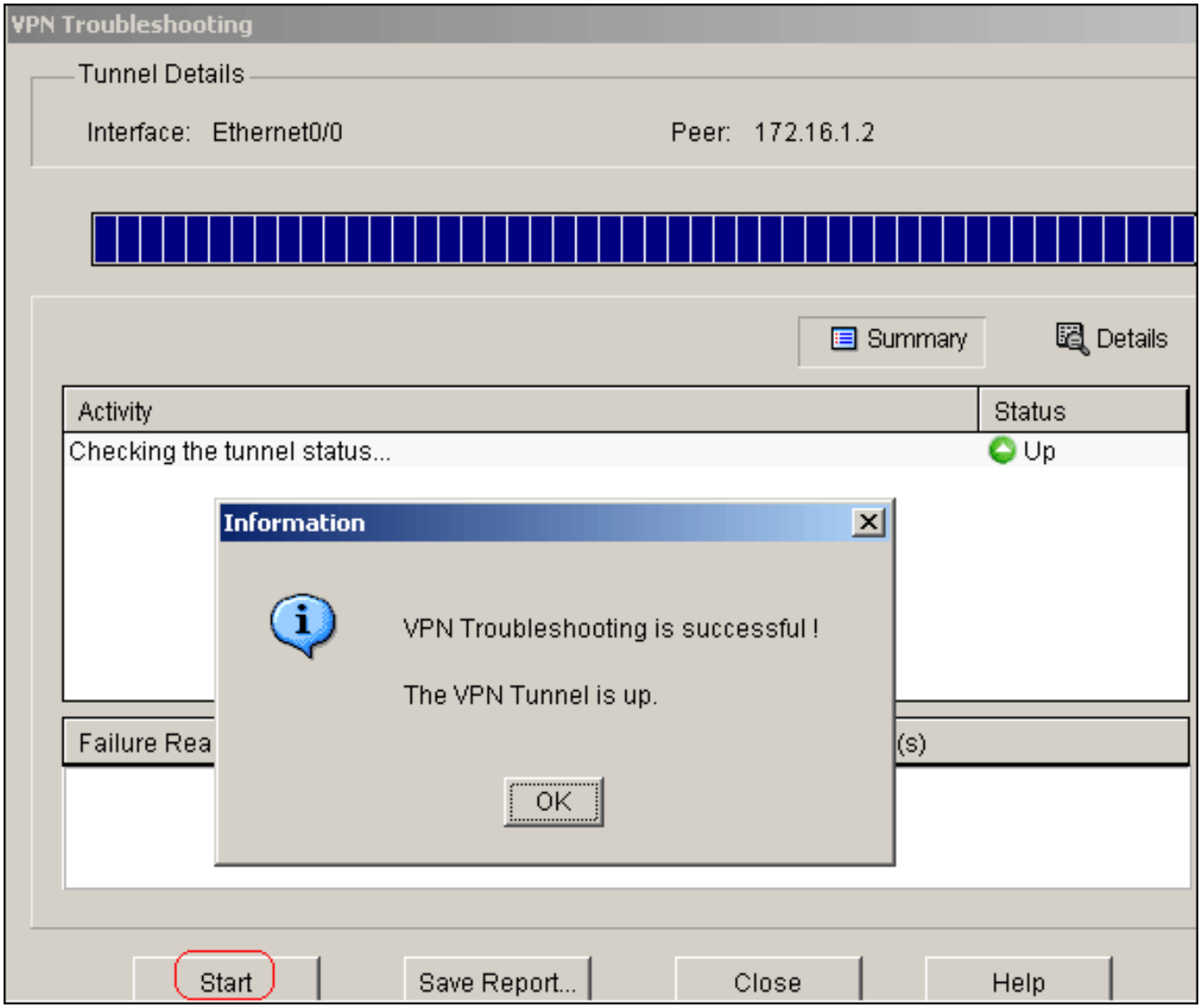
- 接続を確認するには、次の手順を実行します。SDM で [Tools] > [Ping] を選択し、送信元 IP を 192.168.1.1、宛先 IP を 10.10.10.1 として IPSec VPN トンネルを確立します。



[Test Tunnel] をクリックして、次の図に示すように、IPSec VPN トンネルが確立されていることを確認します。



[Start] をクリックします。



トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

```
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
```

関連情報

- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- オーバーラップするプライベート ネットワークを持つ ASA/PIX と Cisco VPN 3000 コンセントレータ間の IPSec 設定例
- テクニカルサポートとドキュメント - Cisco Systems