

Exemple de configuration IPSec entre deux routeurs IOS avec chevauchement des réseaux privés

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer le routeur Cisco IOS dans un site à site IPsec VPN avec les adresses de réseau privé superposantes derrière des passerelles VPN.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations dans ce document sont basées sur le Cisco IOS 3640 Routeurs qui exécutent la version de logiciel 12.4.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

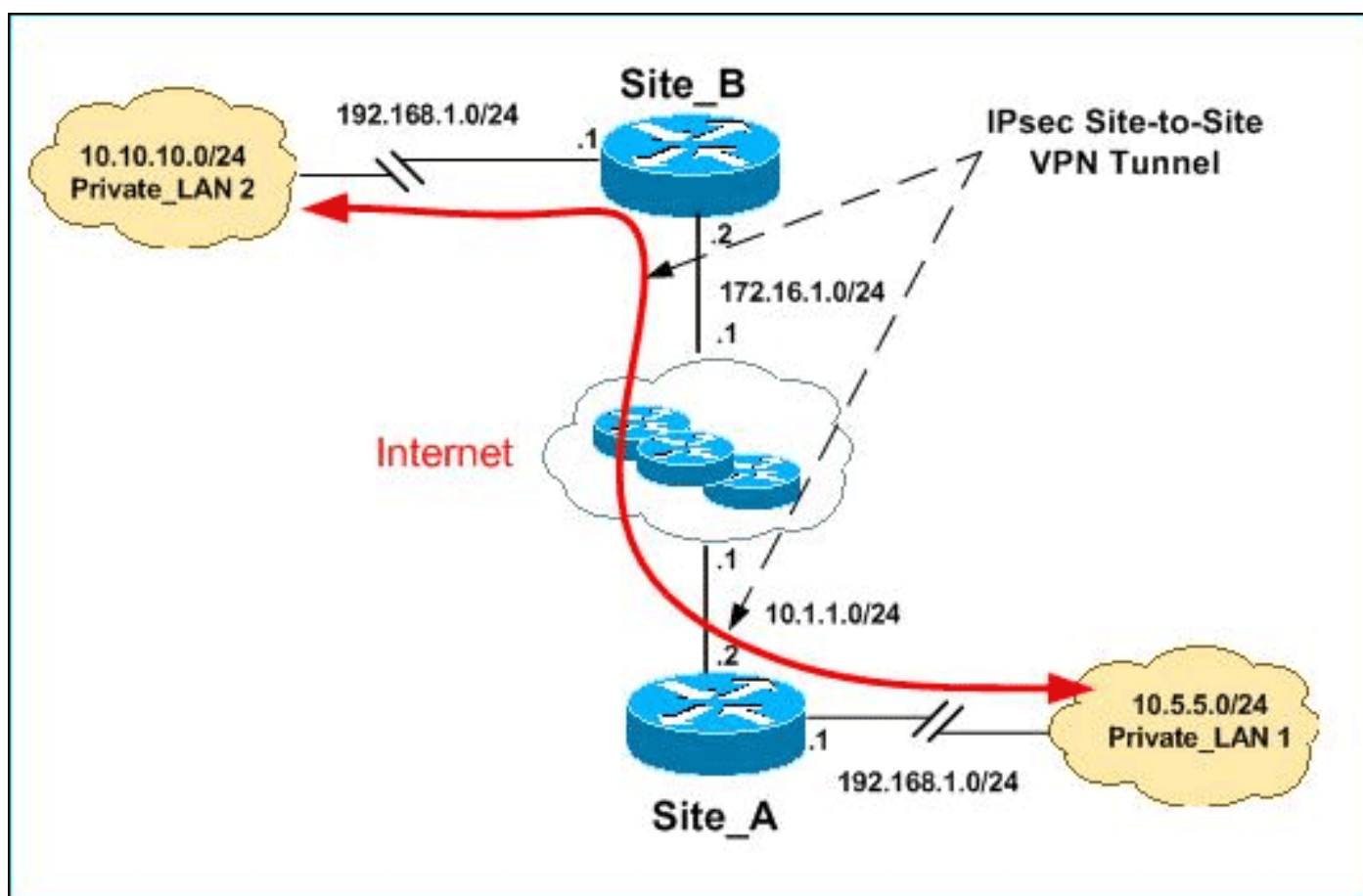
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

Private_LAN1 et Private_LAN2 ont un IP de sous-réseau de 192.168.1.0/24. Ceci simule l'espace d'adressage superposant derrière chaque côté du tunnel d'IPsec.

Dans cet exemple, le routeur de Site_A exécute une traduction bidirectionnelle de sorte que les deux réseaux locaux privés puissent communiquer au-dessus du tunnel d'IPsec. La traduction signifie que Private_LAN1 « voit » Private_LAN2 en tant que 10.10.10.0/24 par le tunnel d'IPsec, et Private_LAN2 « voit » Private_LAN1 en tant que 10.5.5.0/24 par le tunnel d'IPsec.

Configurations

Ce document utilise les configurations suivantes :

- [Configuration du routeur SDM de Site A](#)
- [Configuration CLI de routeur de Site A](#)
- [Configuration de routeur de Site B](#)

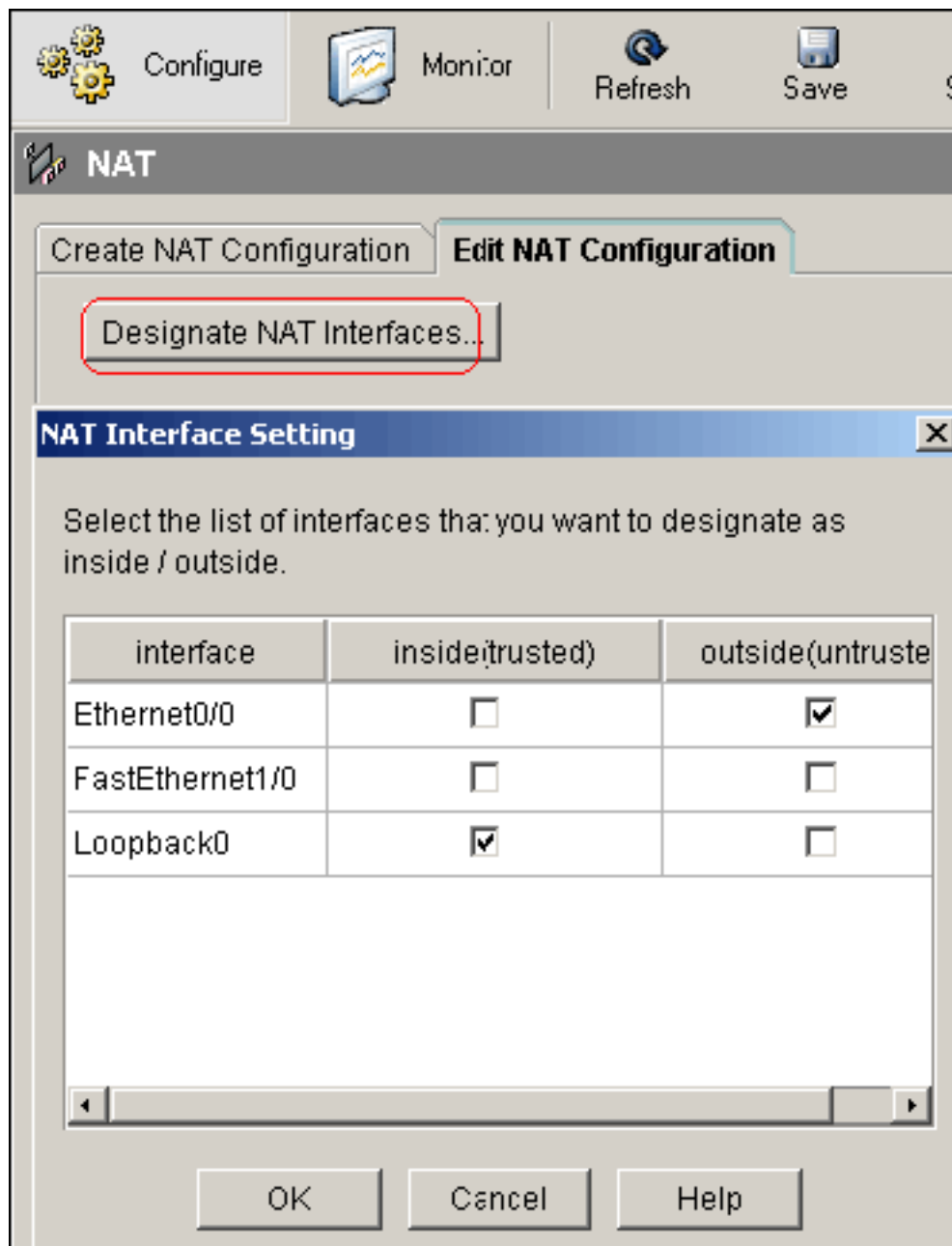
Configuration du routeur SDM de Site A

Remarque: Ce document suppose que le routeur est configuré avec des paramètres de base comme la configuration d'interface, etc. se rapportent à la [configuration de base du routeur utilisant le](#) pour en savoir plus [SDM](#).

Configuration NAT

Terminez-vous ces étapes afin de l'utiliser NAT pour configurer SDM sur le routeur de Site_A :

1. Choisissez le **Configure > NAT > Edit NAT Configuration**, et cliquez sur les **interfaces NAT désignées** afin de définir les interfaces de confiance et non approuvées comme



affichées.

2. Cliquez sur **OK**.
3. Cliquez sur Add afin de configurer la traduction NAT de l'intérieur à la direction extérieure comme

Add Address Translation Rule

Static Dynamic

Direction: From inside to outside

Translate from interface

Inside Interface(s): Loopback0
 IP address: 192.168.1.0
 Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Outside Interface(s): Ethernet0/0
 Type: IP address
 Interface: Ethernet0/0
 IP address: 10.5.5.0

Redirect Port
 TCP UDP
 Original Port: Translated Port:

OK Cancel Help

affichée.

4. Cliquez sur **OK**.

Network Address Translation Rules

Inside Interface(s): Loopback0

Outside Interface(s): Ethernet0/0

Original address	Translated address	Rule Type	Add...
192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static	

5. De nouveau, cliquez sur Add afin de configurer la traduction NAT de la direction d'externe vers interne comme

Add Address Translation Rule

Static Dynamic

Direction: From outside to inside

Translate from interface

Outside Interface(s): Ethernet0/0

IP address: 10.10.10.0

Network Mask(optional): 255.255.255.0 or 24

Translate to interface

Inside Interface(s): Loopback0

IP address: 192.168.1.0

Redirect Port

TCP UDP

Original Port: Translated Port:

OK Cancel Help

affichée.

6. Cliquez sur **OK**.

Network Address Translation Rules			
Inside Interface(s):		Loopback0	
Outside Interface(s):		Ethernet0/0	
	Original address	Translated address	Rule Type
	192.168.1.0-192.168.1.255	10.5.5.0-10.5.5.255	Static
	192.168.1.0-192.168.1.255	10.10.10.0-10.10.10.255	Static

Remarque: Voici la configuration équivalente CLI :

Configuration du VPN

Terminez-vous ces étapes afin d'employer le VPN pour configurer SDM sur le routeur de Site_A :

1. Choisissez **configurer > des composants VPN > VPN > IKE > stratégies IKE > ajoutent** afin de définir les stratégies IKE suivant les indications de cette

Configure IKE Policy

Priority: 10

Authentication: PRE_SHARE

Encryption: DES

D-H Group: group1

Hash: MD5

Lifetime: 24 0 0 HH:MM:SS

OK Cancel Help

image.

2. Cliquez sur **OK.**

IKE Policies							Add...	Edit...	Del
Priority	Encryption	Hash	D-H Group	Authentication	Type				
10	DES	MD5	group1	PRE SHARE	User Defined				

Remarque: Voici la configuration équivalente CLI :

3. Choisissez **configurer > des composants VPN > VPN > IKE > des clés pré-partagées > ajoutent** afin de placer la valeur principale pré-partagée avec l'adresse IP de

Key: *****

Re-enter Key: *****

Host/Network

Type: IP Address

IP Address: 172.16.1.2

Subnet Mask: 255.255.255.0 24

(Optional)

User Authentication (XAuth)

OK Cancel Help

pair.

4. Cliquez sur **OK.**

Pre-shared Keys			Add...
Peer IP/Name	Subnet Mask	pre-shared key	
172.16.1.2	255.255.255.0	*****	

Remarque: Voici la configuration équivalente CLI :

- Choisissez **configurent > VPN > composants > IPSec > jeux de transformations VPN > ajoutent** afin de créer un *myset* de jeu de transformations suivant les indications de cette

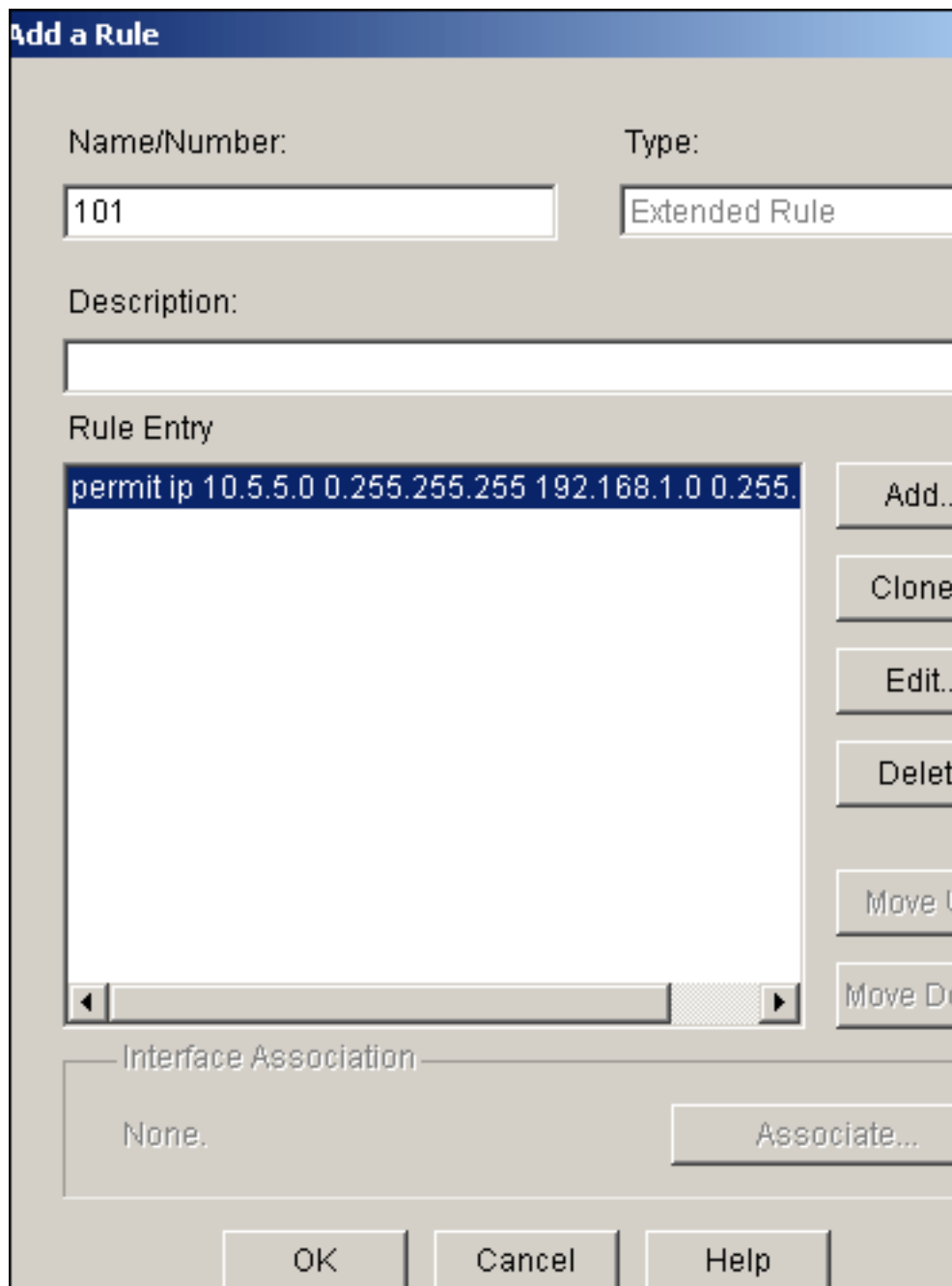
image.

- Cliquez sur **OK**.

Transform Set				Add...
Name	ESP Encryption	ESP Integrity	AH Integrity	
myset	ESP_DES	ESP_MD5_HMAC		

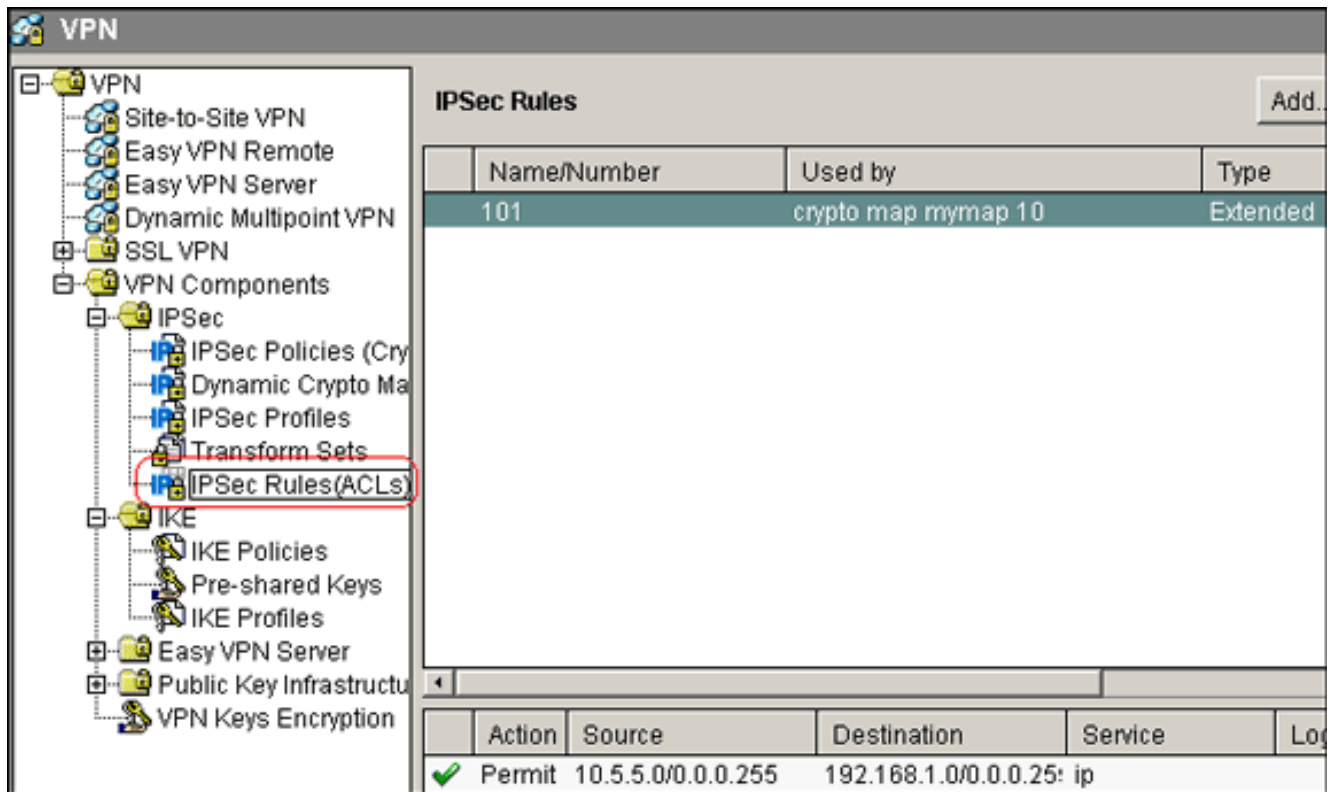
Remarque: Voici la configuration équivalente CLI :

- Choisissez **configurent > VPN > composants > IPSec > IPSec Rules(ACLs) VPN > ajoutent** afin de créer un crypto Access Control List(ACL)



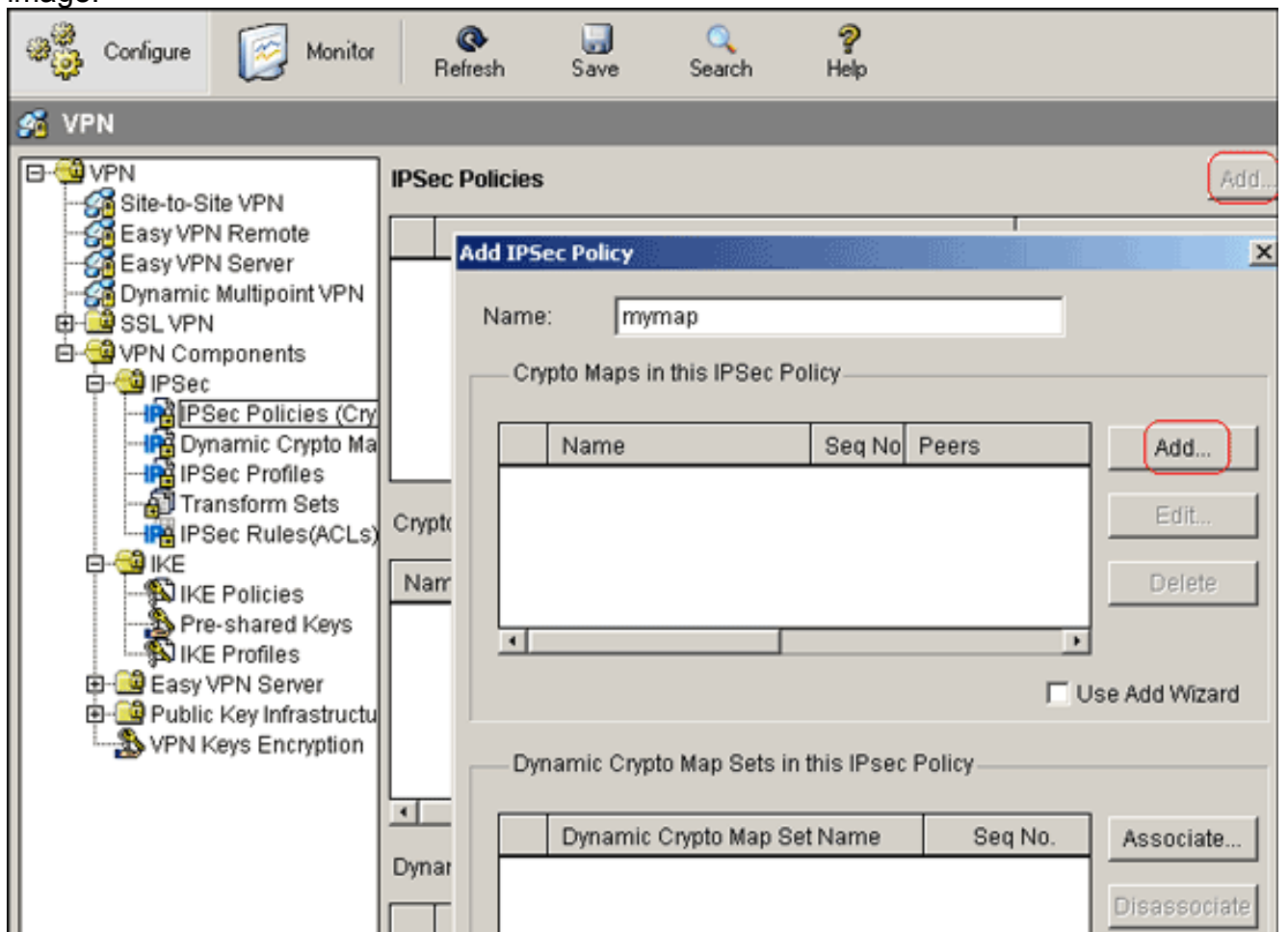
101.

8. Cliquez sur **OK**.



Remarque: Voici la configuration équivalente CLI :

- Choisissez **configurer > VPN > composants > IPsec > stratégies IPsec VPN > ajout** dans l'ordre pour créer le *mymap* de carte de crypto suivant les indications de cette image.



- Cliquez sur **Add**. Cliquez sur l'onglet **Général** et retenez les valeurs par

Add Crypto Map

General Peer Information Transform Sets IPsec Rule

Name of IPsec Policy: mymap

Description:

Sequence Number: 1

Security Association Lifetime:
1 0 0 HH:MM:SS 4608000 Kilobytes

Idle Time:
HH:MM:SS

Perfect Forward Secrecy group1

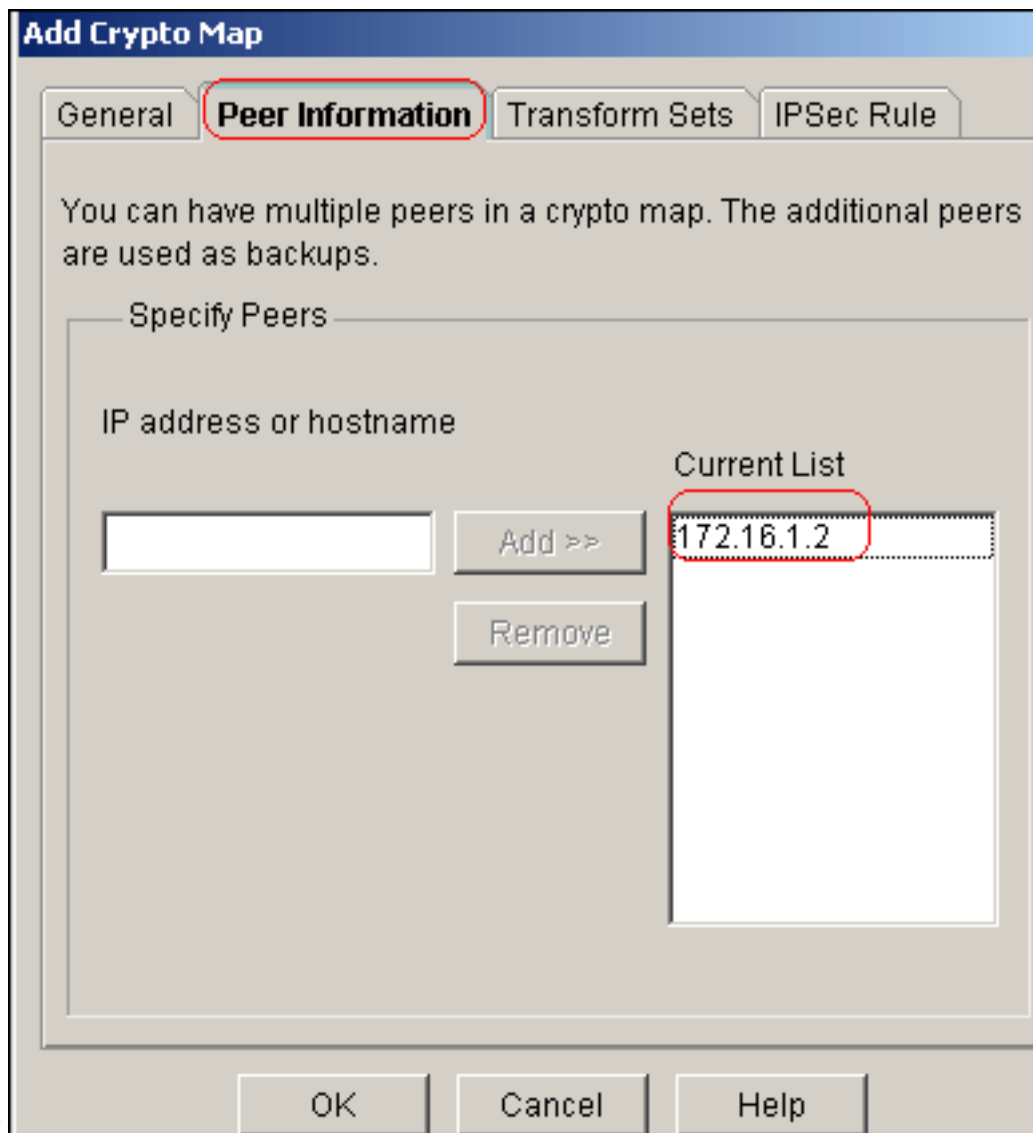
Reverse Route Injection

OK Cancel Help

défaut.

l'onglet de l'information de pair afin d'ajouter l'adresse IP 172.16.1.2 de

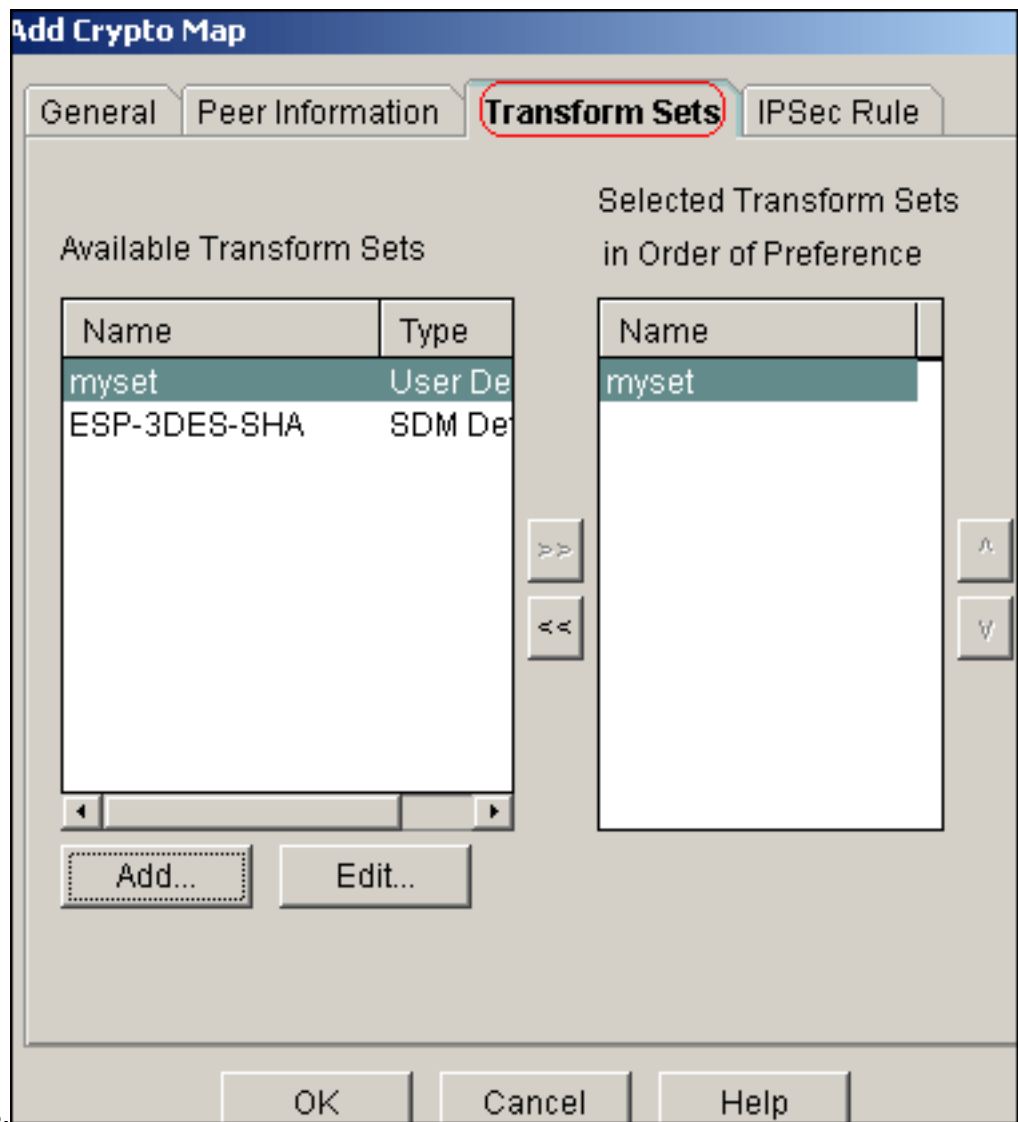
Cliquez sur



pair.

Cliquez sur

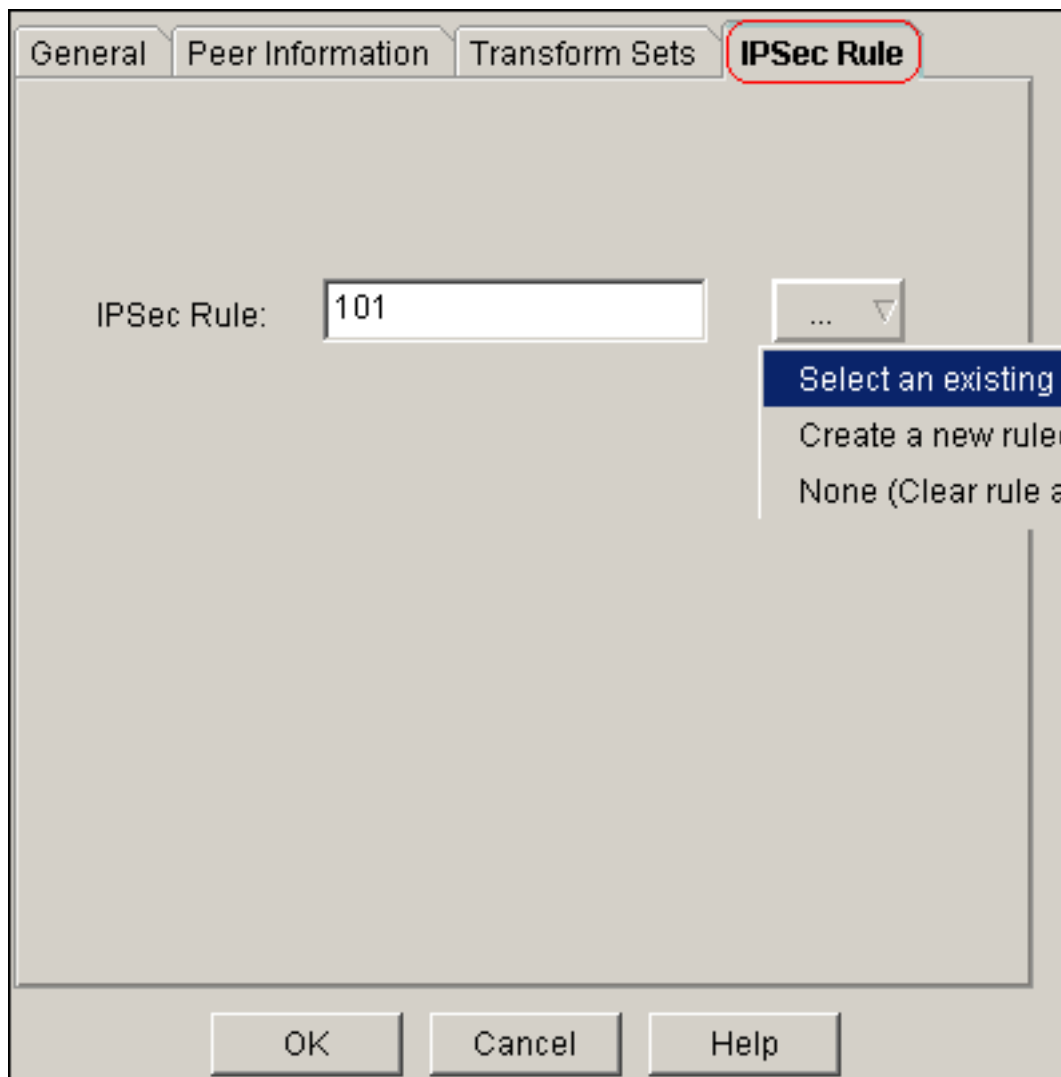
l'onglet de **jeux de transformations** afin de sélectionner le *myset* désiré de jeu de



transformations.

Cliquez sur l'onglet de règle IPsec afin de sélectionner le crypto ACL existant

Clq

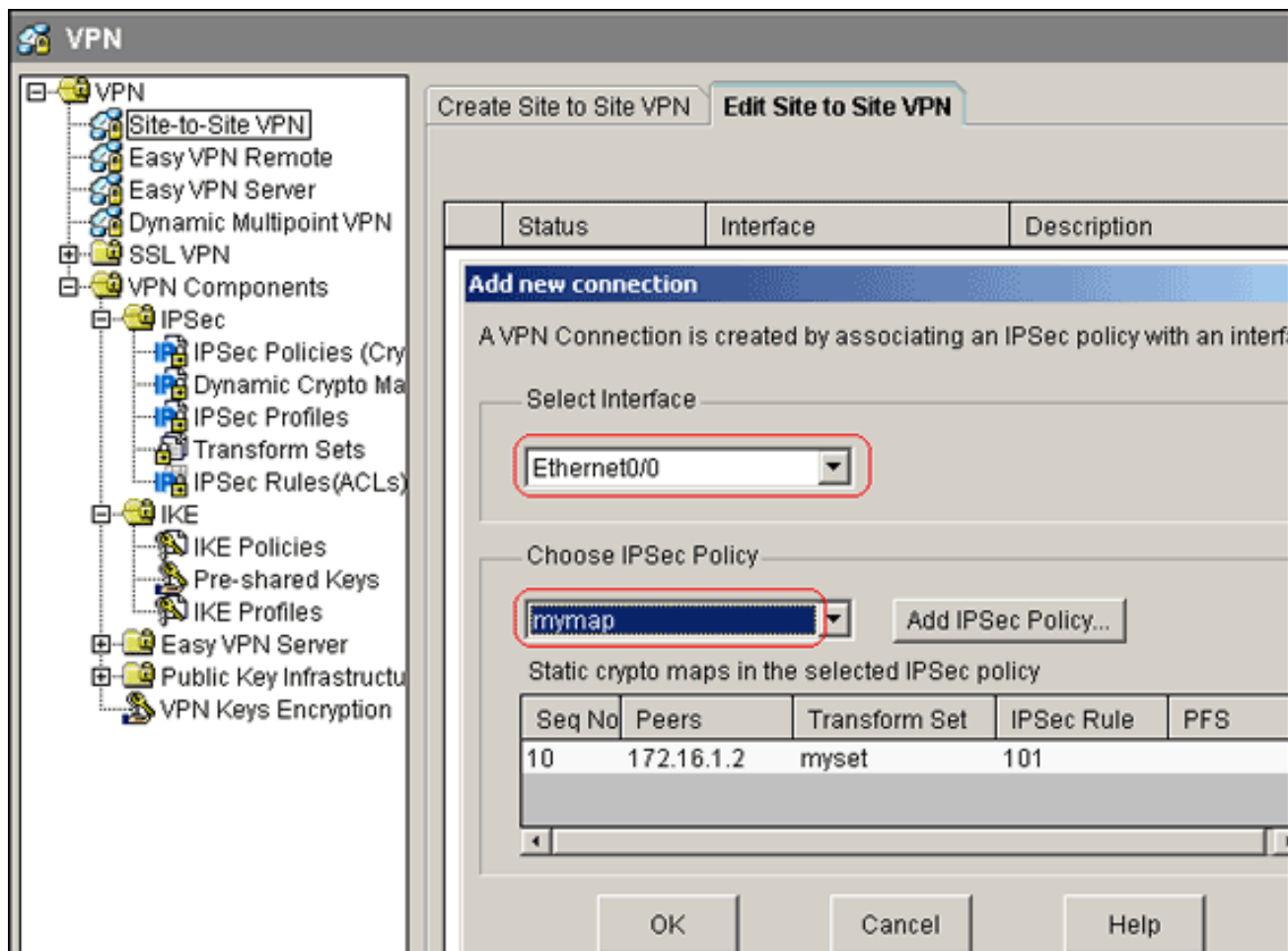


101.

Cliquez sur

OK. Remarque: Voici la configuration équivalente CLI :

11. Choisissez **configureur > VPN > site à site VPN > éditez le site à site VPN > ajoutent** afin d'appliquer le *mymap de crypto map* à l'interface Ethernet0/0.



12. Cliquez sur **OK**. **Remarque:** Voici la configuration équivalente CLI :

Configuration CLI de routeur de Site_A

```

Routeur de Site_A
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#

```

Configuration CLI de routeur de Site_B

Routeur de Site_B

```

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#

```

Véifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

- **show crypto isakmp sa** — Affiche toutes les associations de sécurité en cours d'Échange de clés Internet (IKE) (SAS) à un pair.
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** — Affiche les détails de tout l'IKE en cours SAS à un pair.Site_A#show crypto 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**—Affiche les paramètres utilisés par les SA.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#

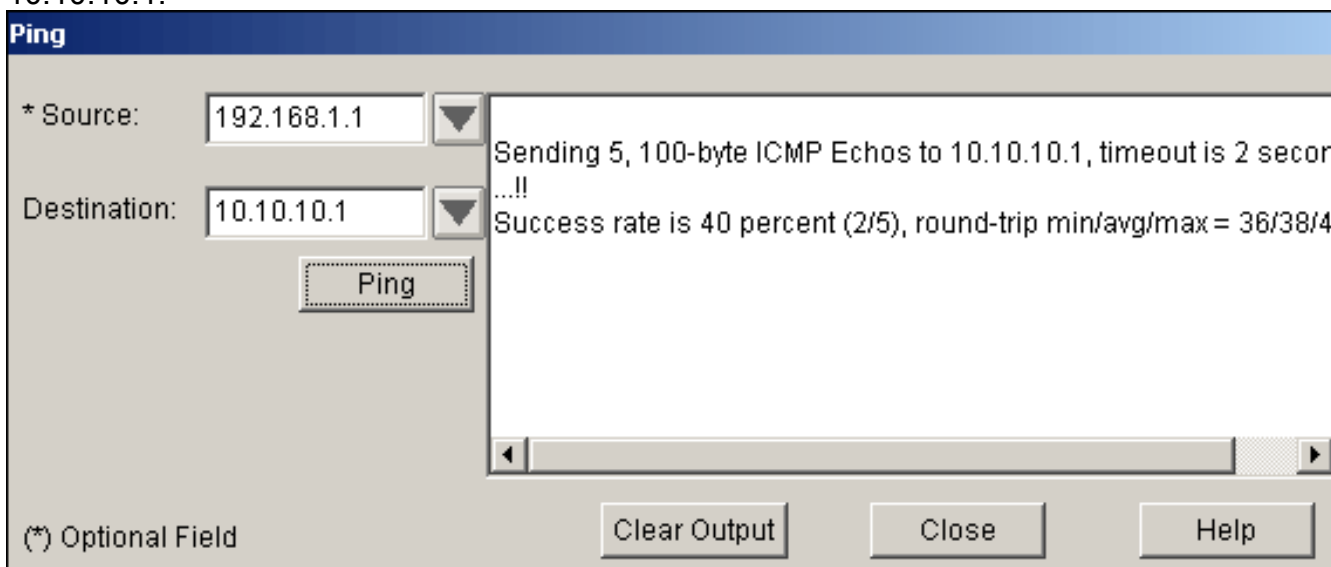
- **show ip nat translations** — Les informations d'emplacement de traduction d'affichages.Site_A#**show ip nat translations**

```
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** — Affiche des informations statiques sur la traduction.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#
```

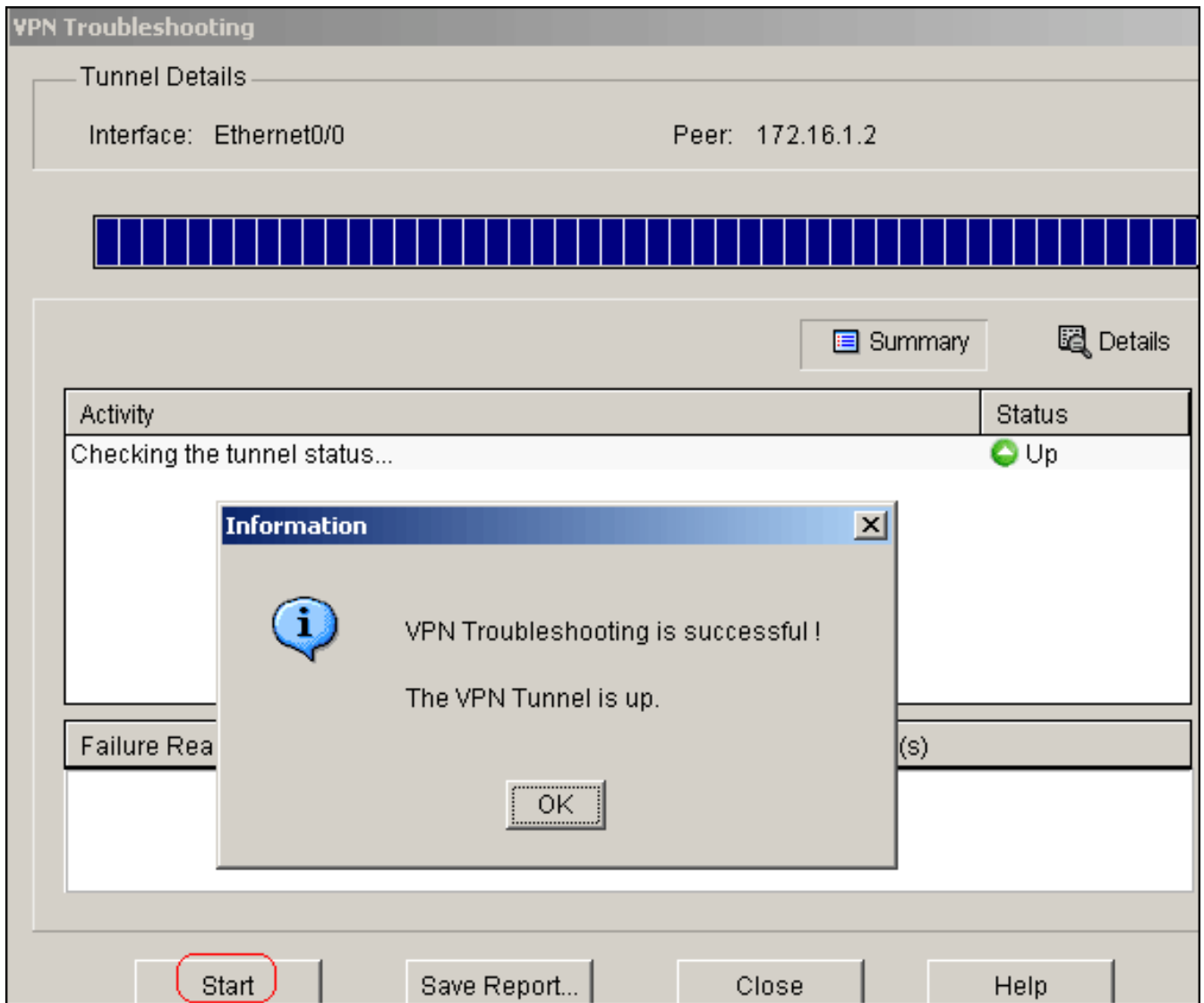
- Terminez-vous ces étapes afin de vérifier la connexion :Dans SDM, choisissez les **outils > le ping** afin d'établir le tunnel VPN d'IPsec avec le source ip comme 192.168.1.1 et l'IP de destination comme 10.10.10.1.



Le tunnel de test de clic afin de vérifier le tunnel VPN d'IPsec est établi suivant les indications de cette image.



Début de clic.



Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

```

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 (Ethernet0/0), 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, rcvd 4
*Sep 30 18:08:10.645: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), 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, rcvd 4
*Sep 30 18:08:10.685: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), 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, rcvd 4
*Sep 30 18:08:10.729: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), 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, rcvd 4
*Sep 30 18:08:10.773: IP: tableid=0, s=192.168.1.1 (local), d=10.10.10.1 (Ethernet0/0), 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, rcvd 4

[Informations connexes](#)

- [Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance](#)
- [IPSec entre ASA/PIX et concentrateur de Cisco VPN 3000 avec superposer l'exemple privé de configuration réseau](#)
- [Support et documentation techniques - Cisco Systems](#)