Configuration d'un tunnel IPSec entre un concentrateur Cisco VPN 3000 et un pare-feu Checkpoint NG

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Diagramme du réseau
Configurations
Configurez le concentrateur VPN 3000
Configurez Checkpoint NG
Vérifiez
Vérifiez la communication réseau
État de tunnel de vue sur Checkpoint NG
État de tunnel de vue sur le concentrateur VPN
Dépannez
Récapitulation de réseau
Debugs pour Checkpoint NG
Debugs pour le concentrateur VPN
Informations connexes

Introduction

Ce document explique comment configurer un tunnel d'IPSec avec des clés pré-partagées pour communiquer entre deux réseaux privés. Dans cet exemple, les réseaux de communication sont le réseau 192.168.10.x privé à l'intérieur du concentrateur de Cisco VPN 3000 et le réseau 10.32.x.x privé à l'intérieur du Pare-feu de la nouvelle génération de point de reprise (NG).

Conditions préalables

Conditions requises

- Le trafic de l'intérieur du concentrateur et de l'intérieur VPN que Checkpoint NG à l'Internet — représenté ici par les réseaux 172.18.124.x — doit circuler avant de commencer cette configuration.
- Les utilisateurs doivent être au courant de la négociation IPSec. Ce processus peut être

décomposé en cinq étapes, y compris deux phases d'Échange de clés Internet (IKE).Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les pairs sont authentifiés, un tunnel sécurisé est créé avec le Protocole ISAKMP (Internet Security Association and Key Management Protocol).Dans le Phase 2 d'IKE, les pairs d'IPSec utilisent authentifié et sécurisent le tunnel afin de négocier IPSec SA transforme. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.Le tunnel d'IPSec est créé, et des données sont transférées entre les pairs d'IPSec basés sur les paramètres d'IPSec configurés dans les jeux de transformations d'IPSec.Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

Composants utilisés

Cette configuration a été développée et testée avec les versions de logiciel et de matériel suivantes :

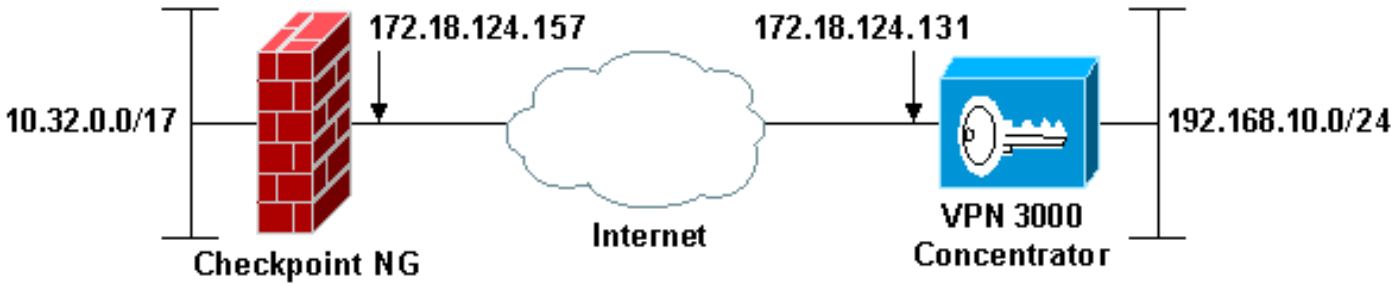
- Concentrateur 3.5.2 de la gamme VPN 3000
- Pare-feu Checkpoint NG

Conventions

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

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Note: Le schéma d'adressage IP utilisé dans cette configuration n'est pas légalement routable sur l'Internet. Ce sont des adresses RFC 1918 qui ont été utilisées dans un environnement de laboratoire.

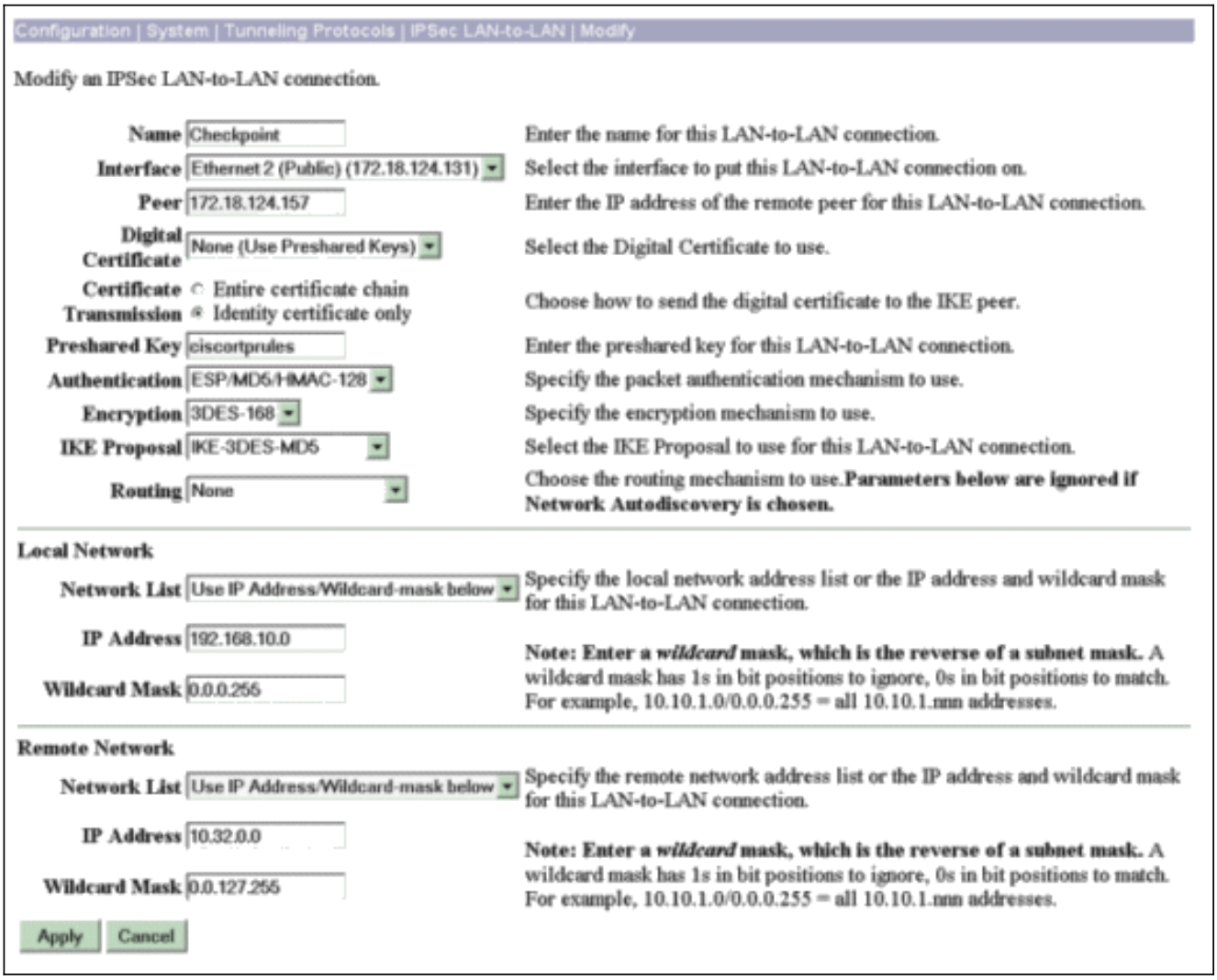
Configurations

Configurez le concentrateur VPN 3000

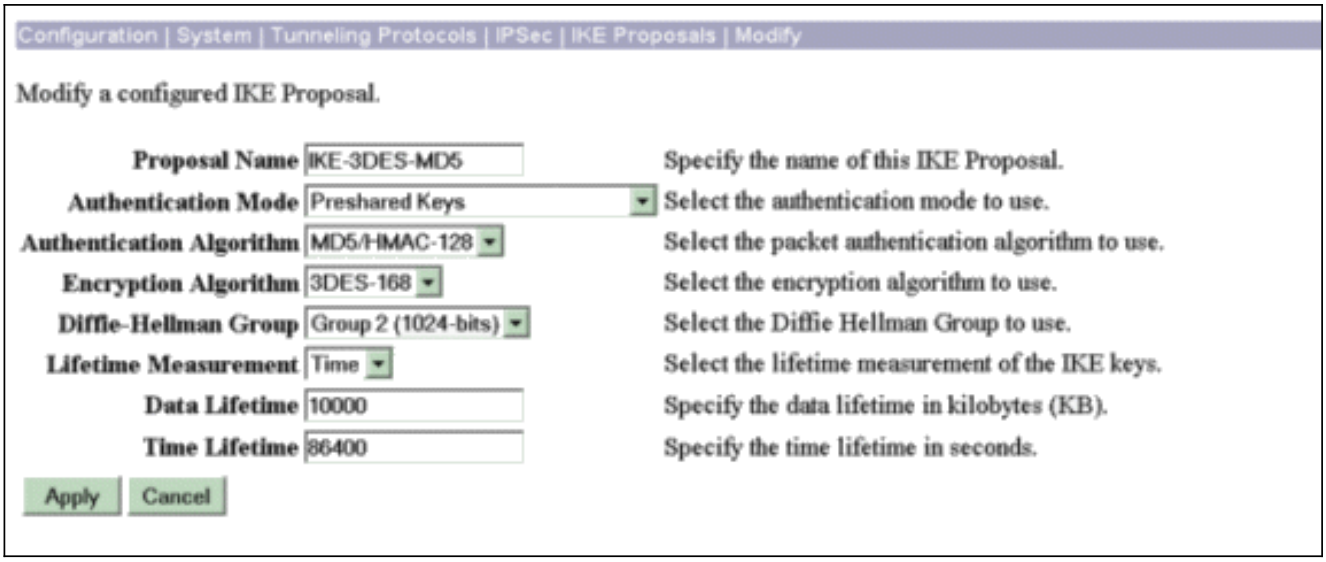
Terminez-vous ces étapes afin de configurer le concentrateur VPN 3000 :

1. Allez à la **configuration > aux protocoles de système > de Tunnellisation > à l'entre réseaux**

locaux d'IPSec afin de configurer la session entre réseaux locaux. Placez les options pour l'authentification et les algorithmes d'IKE, la clé pré-partagée, l'adresse IP de pair, et les paramètres de gens du pays et de réseau distant. Cliquez sur **Apply**.Dans cette configuration, l'authentification a été placée pendant qu'ESP-MD5-HMAC et cryptage étaient placés comme
3DES.

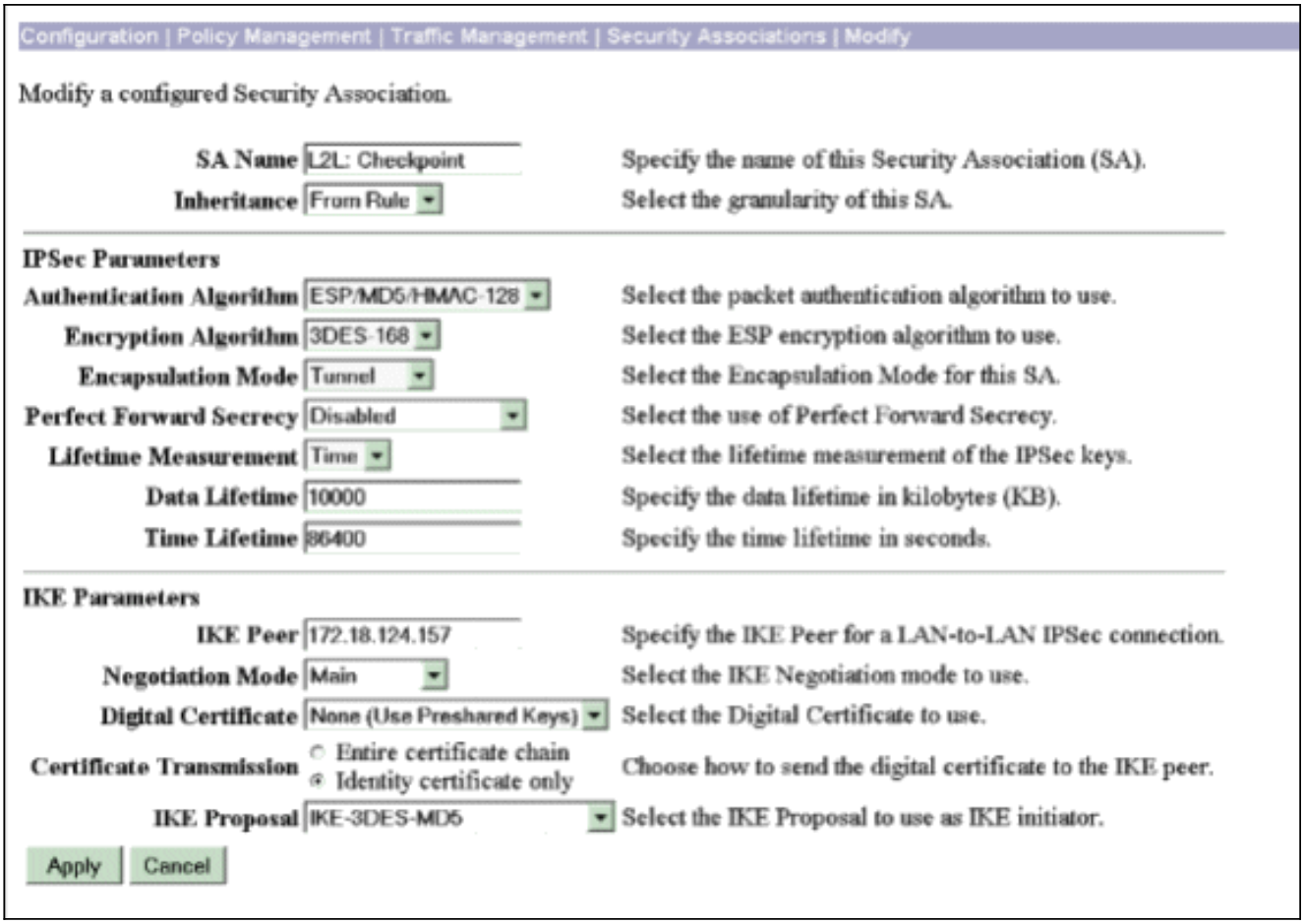


2. Allez à la **configuration > aux protocoles de système > de Tunnellisation > à l'IPSec > aux propositions d'IKE** et placez les paramètres requis.Sélectionnez la proposition IKE-3DES-MD5 d'IKE et vérifiez les paramètres sélectionnés pour la proposition. Cliquez sur Apply afin de configurer la session entre réseaux locaux.Ce sont les paramètres pour cette configuration
:



3. Allez à la **configuration > à la Gestion des stratégies > à la gestion de trafic > aux associations de sécurité**, sélectionnez IPSec SA créé pour la session, et vérifiez les paramètres d'IPSec SA choisis pour la session entre réseaux locaux.Dans cette configuration le nom de session entre réseaux locaux était « point de reprise, « ainsi IPSec SA a été créé automatiquement comme "L2L : Point de reprise. »

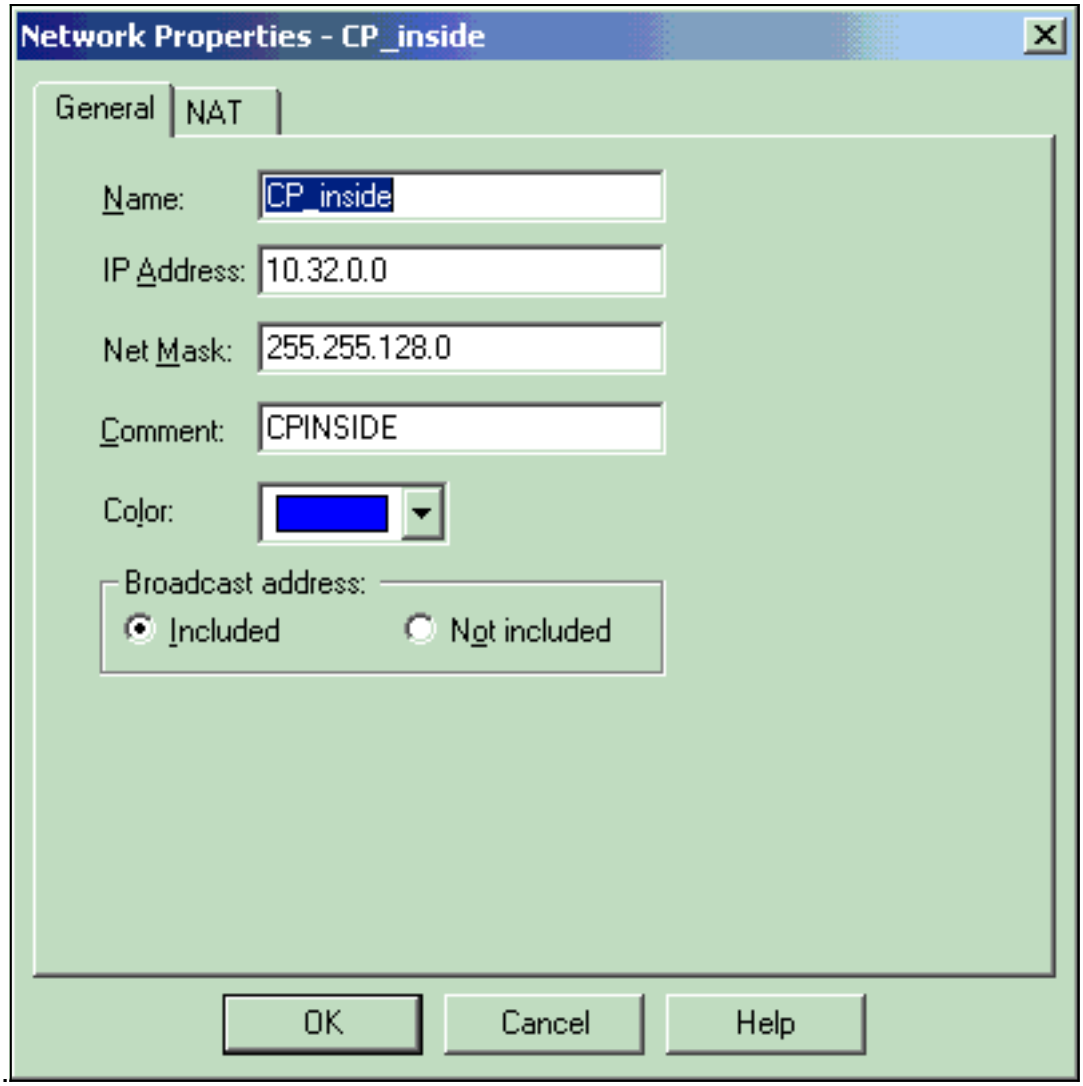
Ce sont les paramètres pour cette SA
:



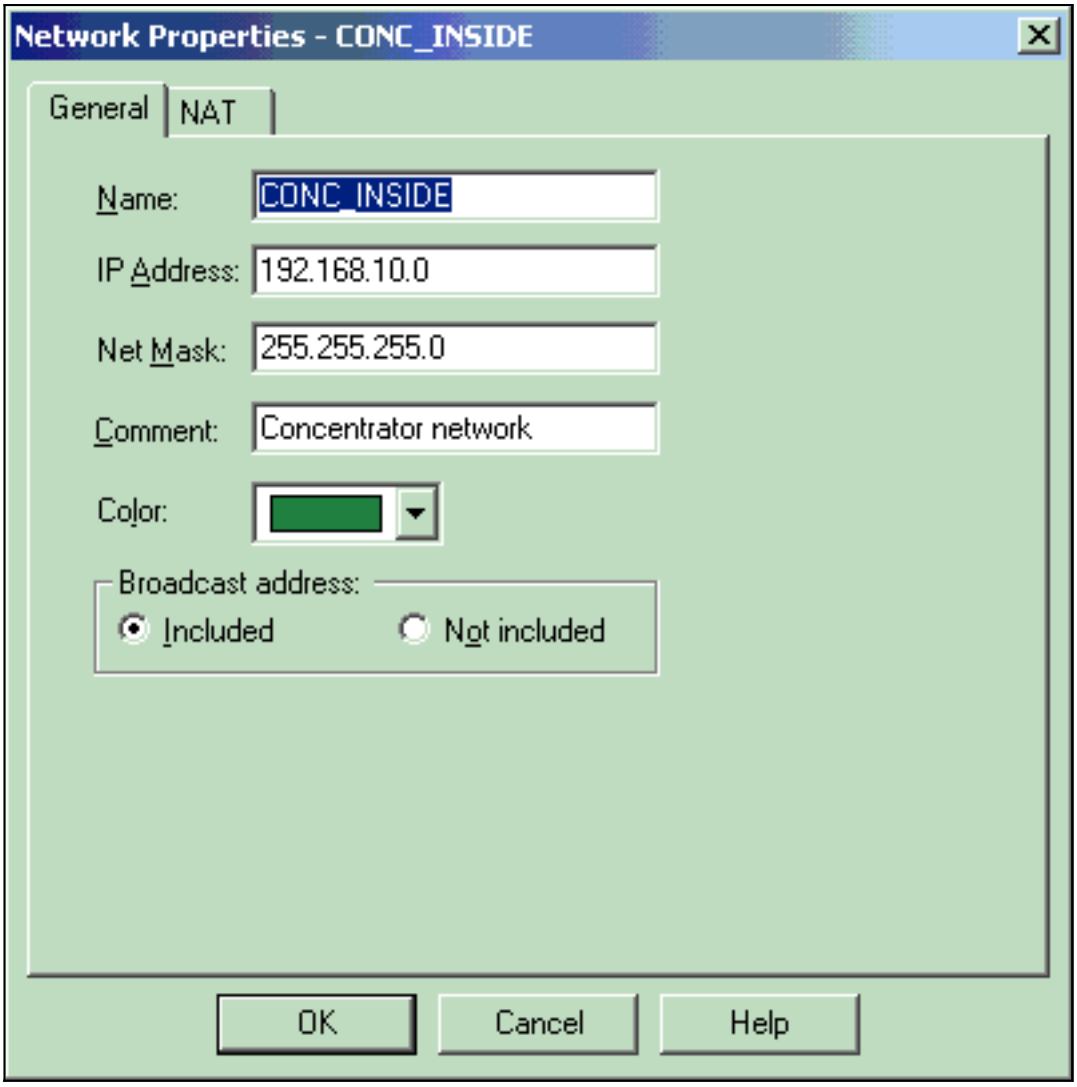
Configurez Checkpoint NG

Des objets de réseau et les règles sont définis sur Checkpoint NG afin de composer la stratégie qui concerne la configuration du VPN à installer. Cette stratégie est alors installée avec l'éditeur de stratégie de Checkpoint NG pour se terminer le côté de Checkpoint NG de la configuration.

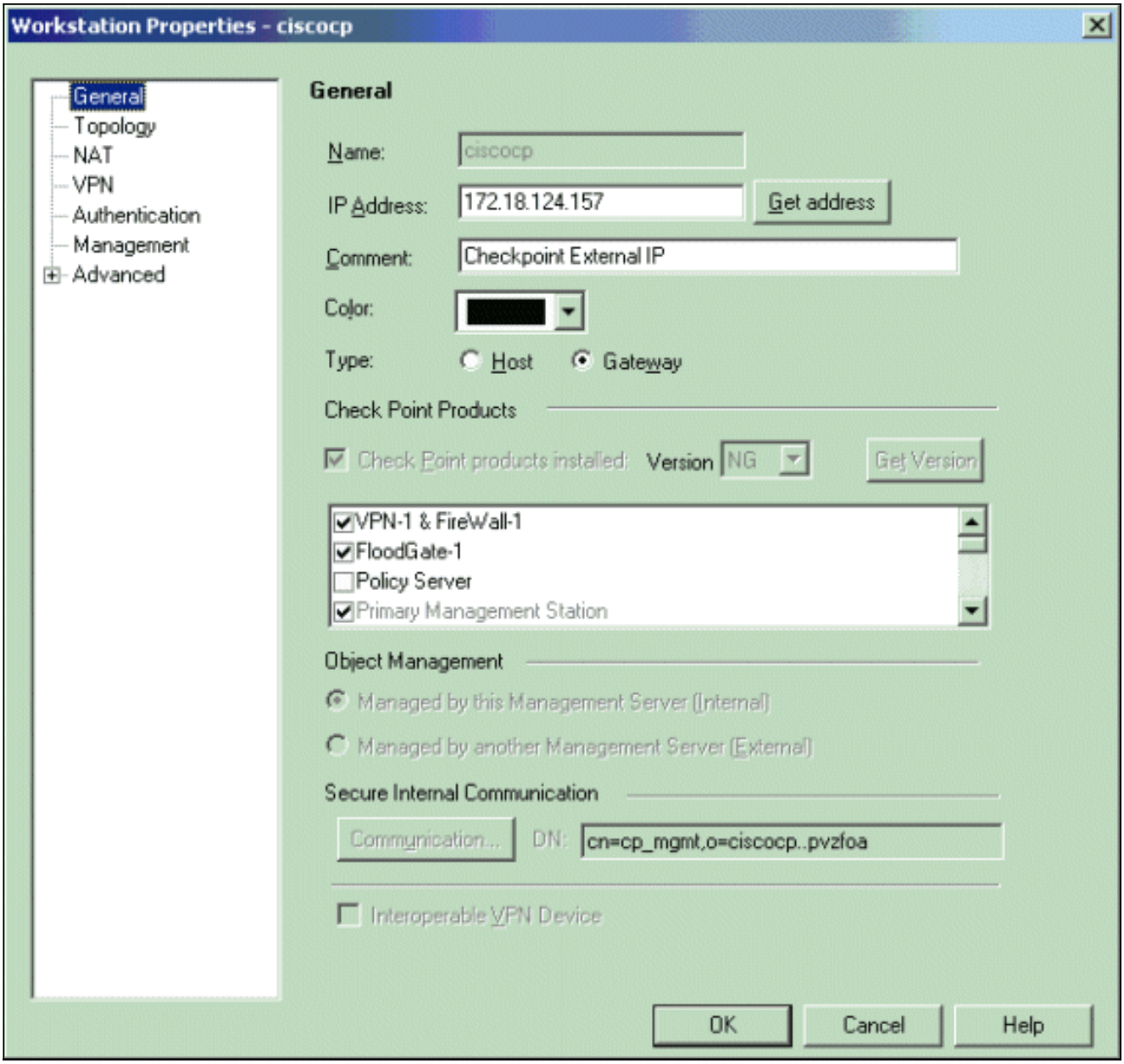
1. Créez les deux objets de réseau pour le réseau de Checkpoint NG et le réseau de concentrateur VPN qui chiffreront le trafic intéressant.afin de créer des objets, choisis **gérez > des objets de réseau**, puis sélectionnez **nouveau > réseau**. Écrivez l'information réseau appropriée, puis cliquez sur OK.Ces exemples affichent l'installation des objets de réseau appelés CP_inside (le réseau intérieur de Checkpoint NG) et le CONC_INSIDE (le réseau intérieur du concentrateur

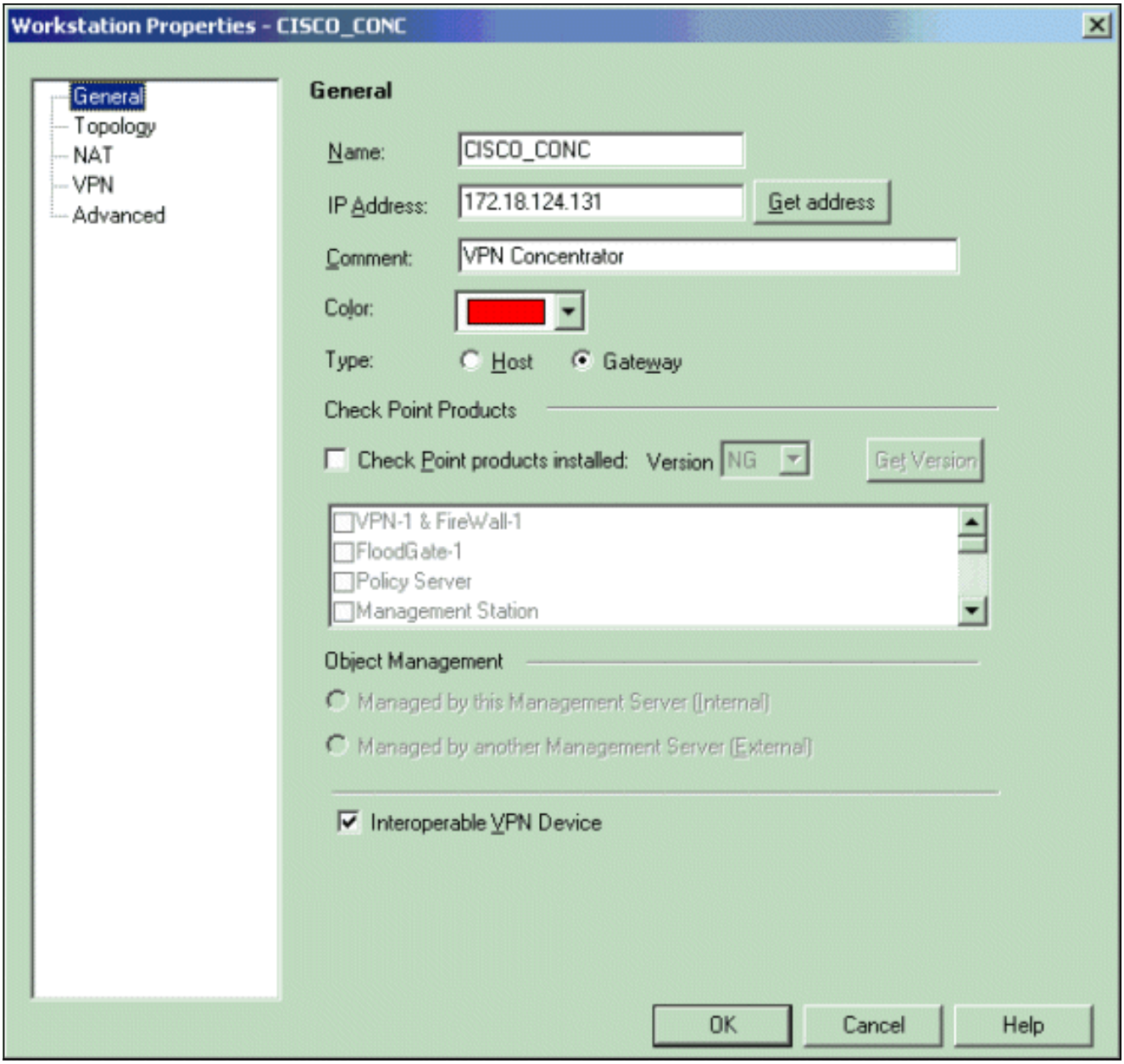

Network Properties - CP_inside
General
NAT
Name:
CP_inside
IP Address:
10.32.0.0
Net Mask:
255.255.128.0
Comment:
CPINSIDE
Color:
Broadcast address:
Included
Not included
OK
Cancel
Help

VPN).

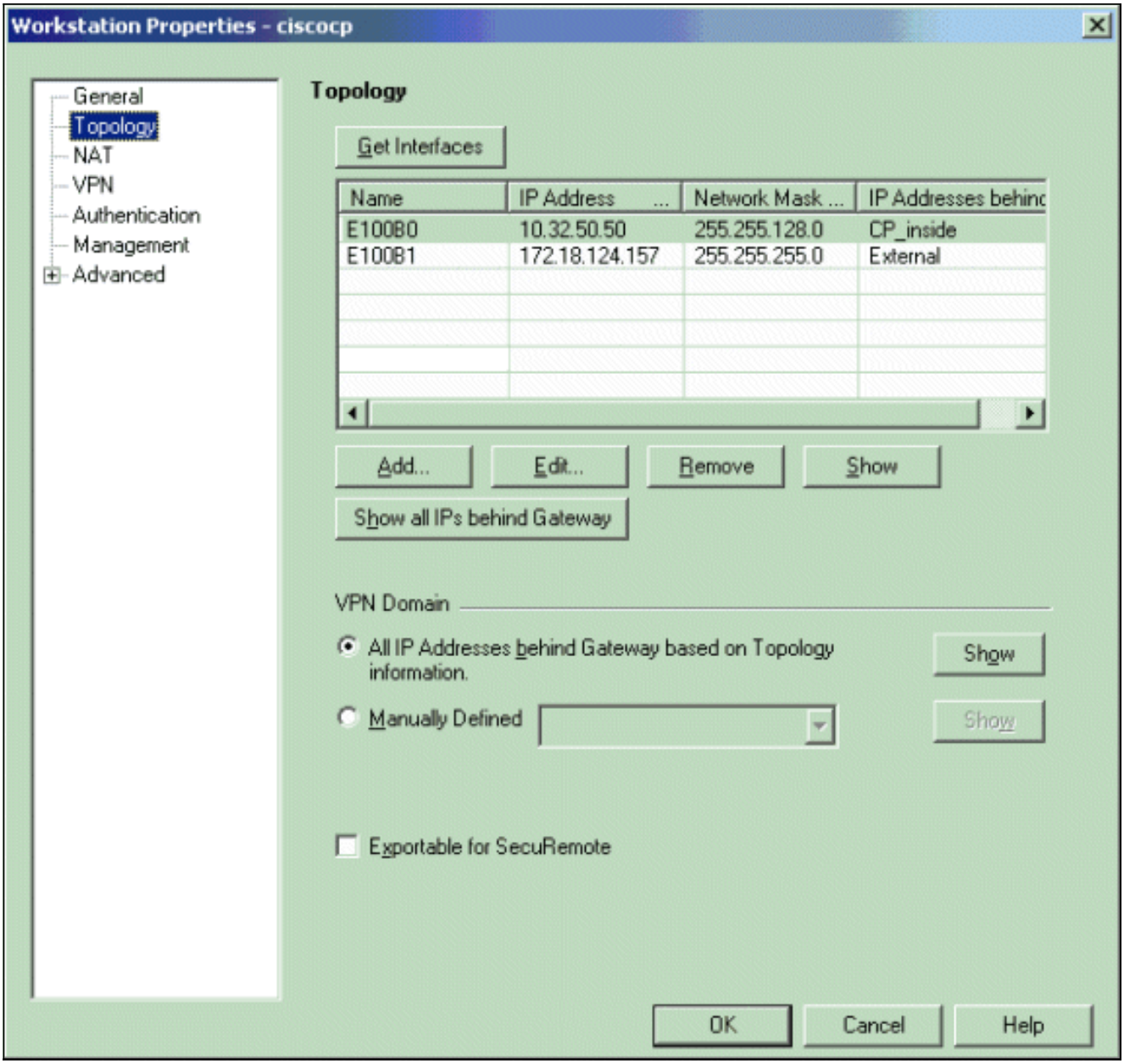


2. Allez **gérer > des objets de réseau** et sélectionner **nouveaux > poste de travail** afin de créer des objets de poste de travail pour les périphériques VPN, Checkpoint NG et le concentrateur VPN.**Note**: Vous pouvez utiliser l'objet de poste de travail de Checkpoint NG créé pendant l'installation initiale de Checkpoint NG. Sélectionnez les options de placer le poste de travail comme passerelle et périphérique VPN interopérable, puis cliquez sur OK.Ces exemples affichent l'installation des objets appelés ciscocp (Checkpoint NG) et le CISCO_CONC (concentrateur VPN 3000)
:

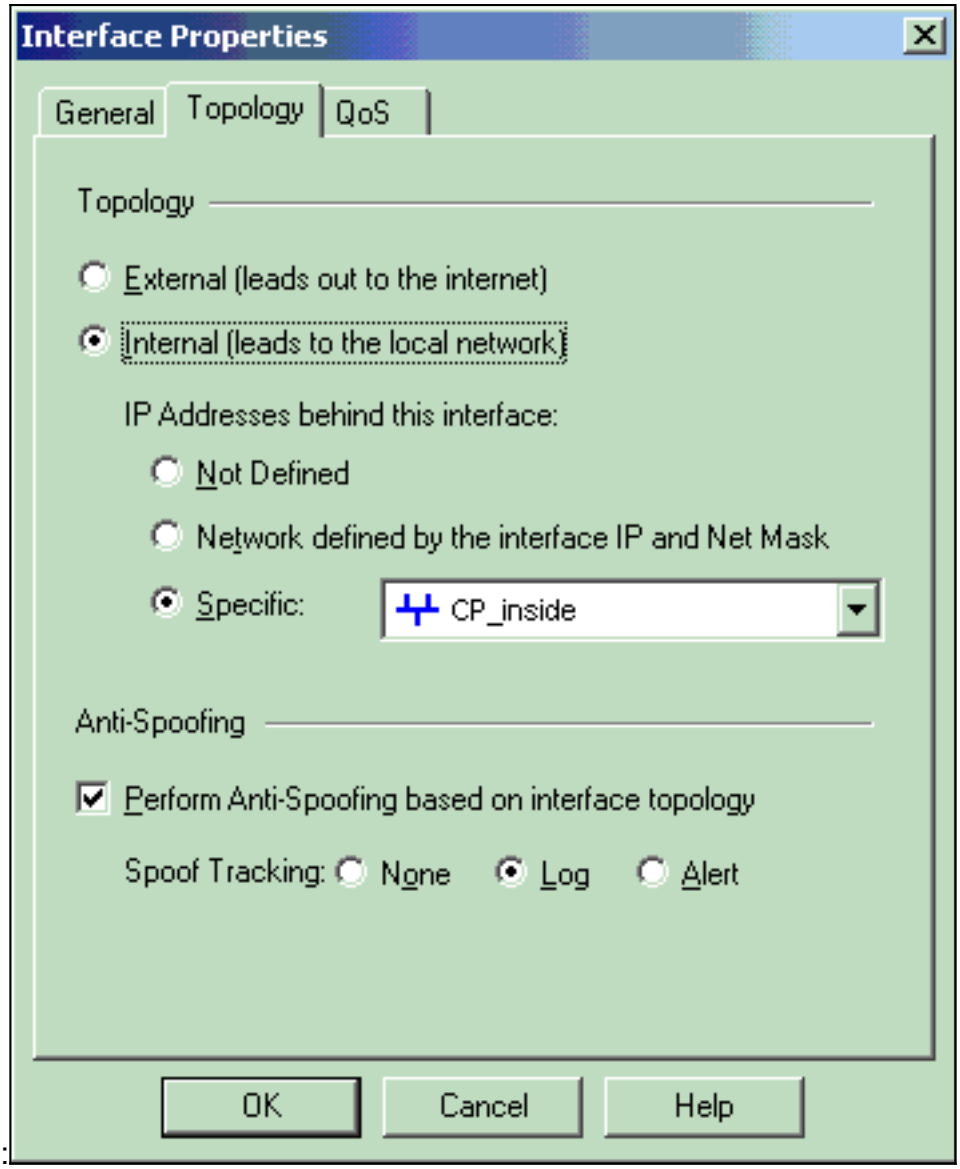

Workstation Properties - ciscocp
General
Topology
NAT
VPN
Authentication
Management
Advanced
General
Name:
ciscocp
IP Address:
172.18.124.157
Get address
Comment:
Checkpoint External IP
Color:
Type:
Host
Gateway
Check Point Products
Check Point products installed:
Version
NG
Get Version
VPN-1 & FireWall-1
FloodGate-1
Policy Server
Primary Management Station
Object Management
Managed by this Management Server (Internal)
Managed by another Management Server (External)
Secure Internal Communication
Communication...
DN:
cn=cp_mgmt,o=ciscocp..pvzfoa
Interoperable VPN Device
OK
Cancel
Help



3. Allez **gérer > des objets de réseau > éditent** afin d'ouvrir la fenêtre de Properties de poste de travail pour le poste de travail de Checkpoint NG (ciscocp dans cet exemple). **La topologie** choisie des choix du côté gauche de la fenêtre, sélectionnent alors le réseau à chiffrer. Cliquez sur Edit afin de placer les propriétés d'interface.Dans cet exemple, CP_inside est le réseau intérieur de Checkpoint
NG.

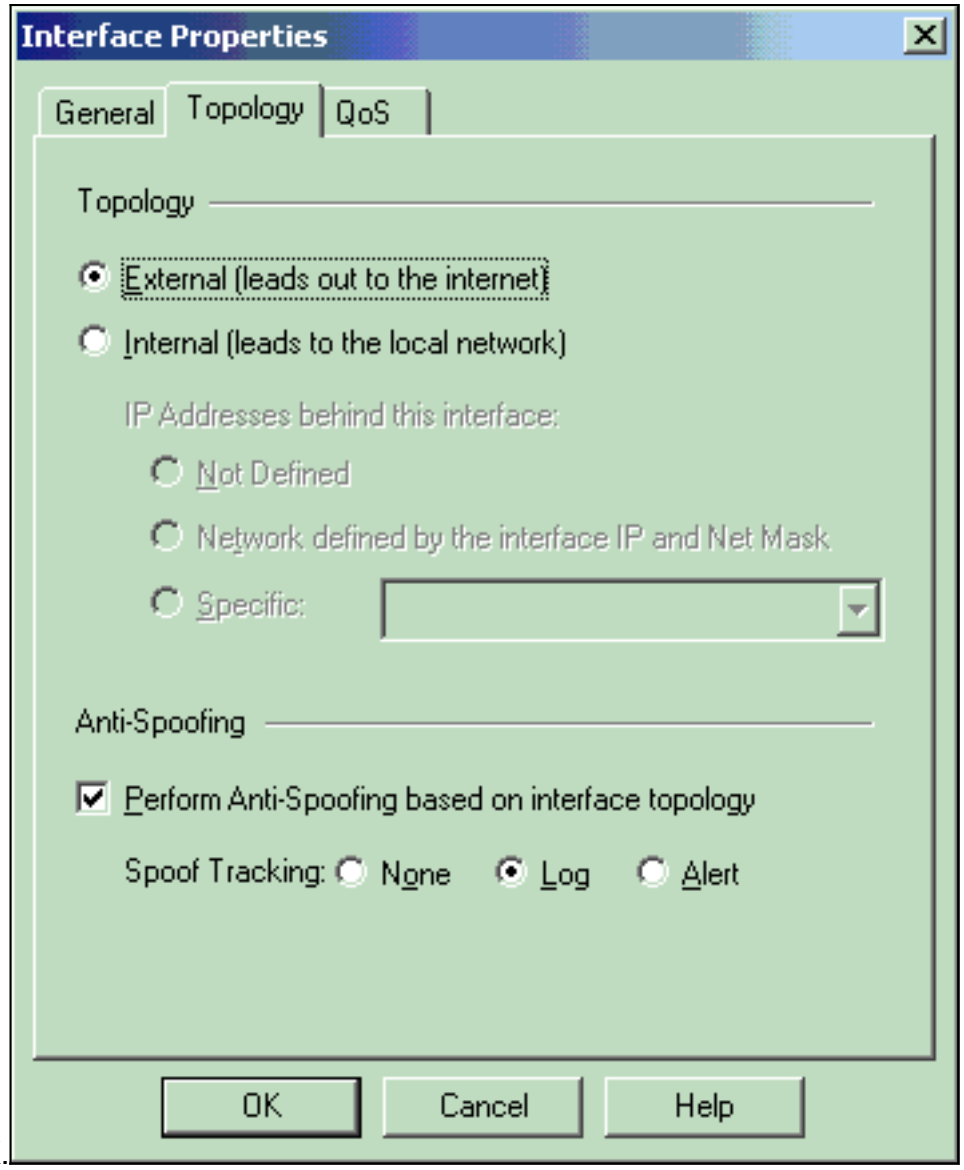


4. Sur la fenêtre de Properties d'interface, sélectionnez l'option d'indiquer le poste de travail comme interne, puis spécifiez l'adresse IP appropriée. Cliquez sur **OK**.Les sélections de topologie affichées indiquent le poste de travail en tant qu'interne et spécifient des adresses IP derrière l'interface de CP_inside



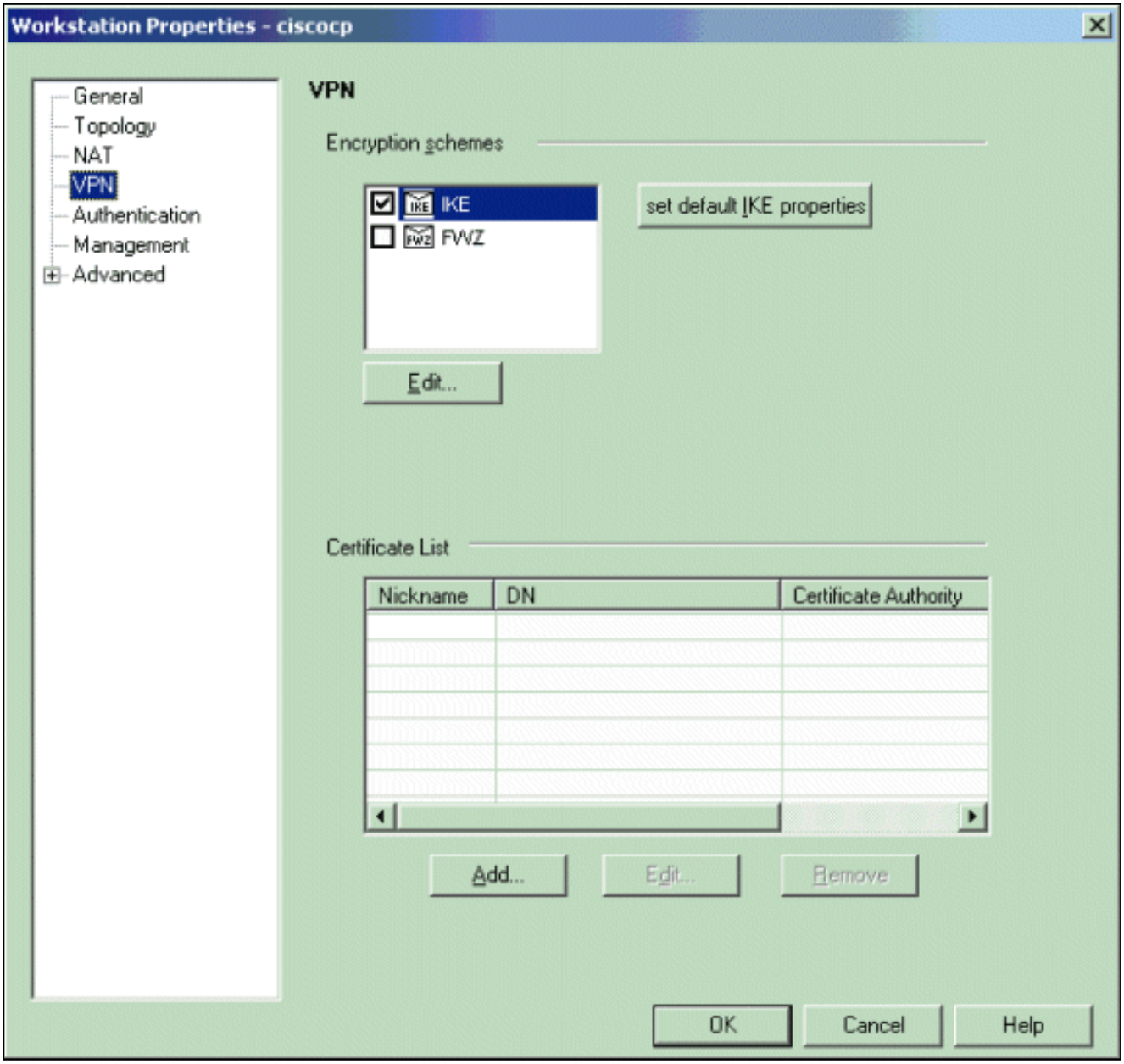
:

5. De la fenêtre de Properties de poste de travail, sélectionnez l'interface extérieure sur Checkpoint NG que cela mène à l'Internet, puis cliquez sur Edit afin de placer les propriétés d'interface. Sélectionnez l'option d'indiquer la topologie comme externe, puis cliquez sur

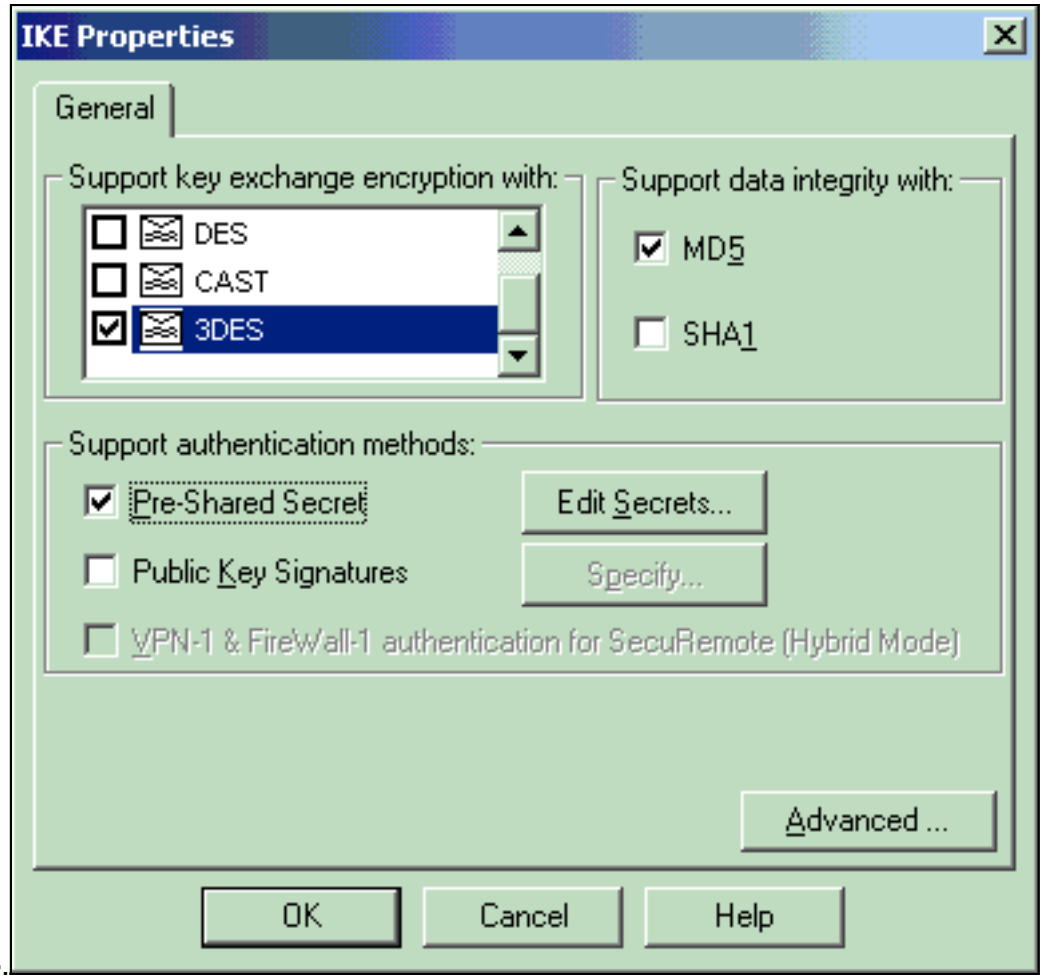


OK.

6. De la fenêtre de Properties de poste de travail sur Checkpoint NG, le **VPN** choisi des choix du côté gauche de la fenêtre, sélectionnent alors les paramètres d'IKE pour des algorithmes de cryptage et d'authentification. Cliquez sur Edit afin de configurer les propriétés IKE.

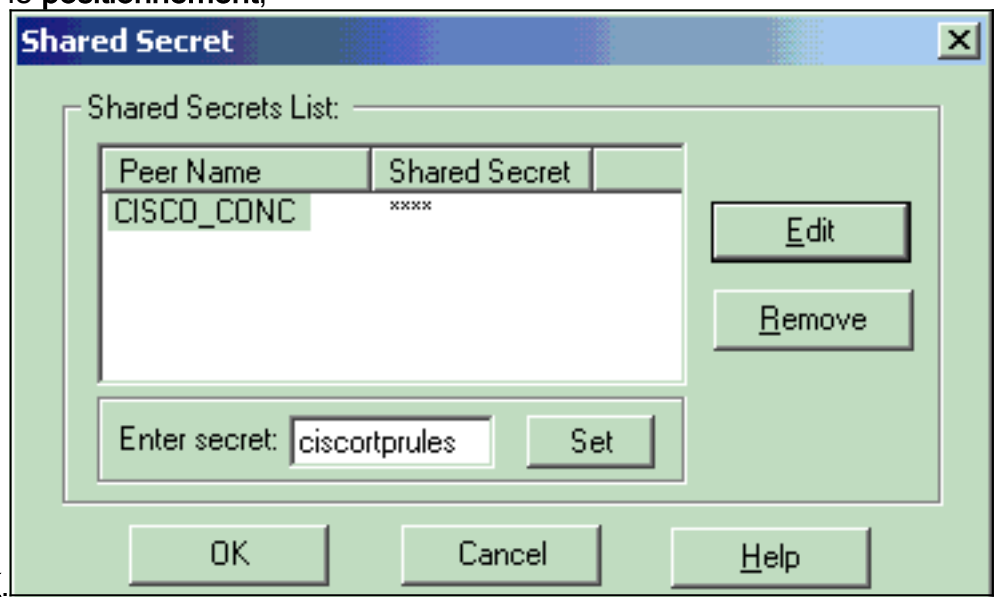


7. Placez les propriétés IKE pour apparier les propriétés sur le concentrateur VPN.Dans cet exemple, sélectionnez l'option de chiffrement pour **3DES** et l'option de hachage pour le



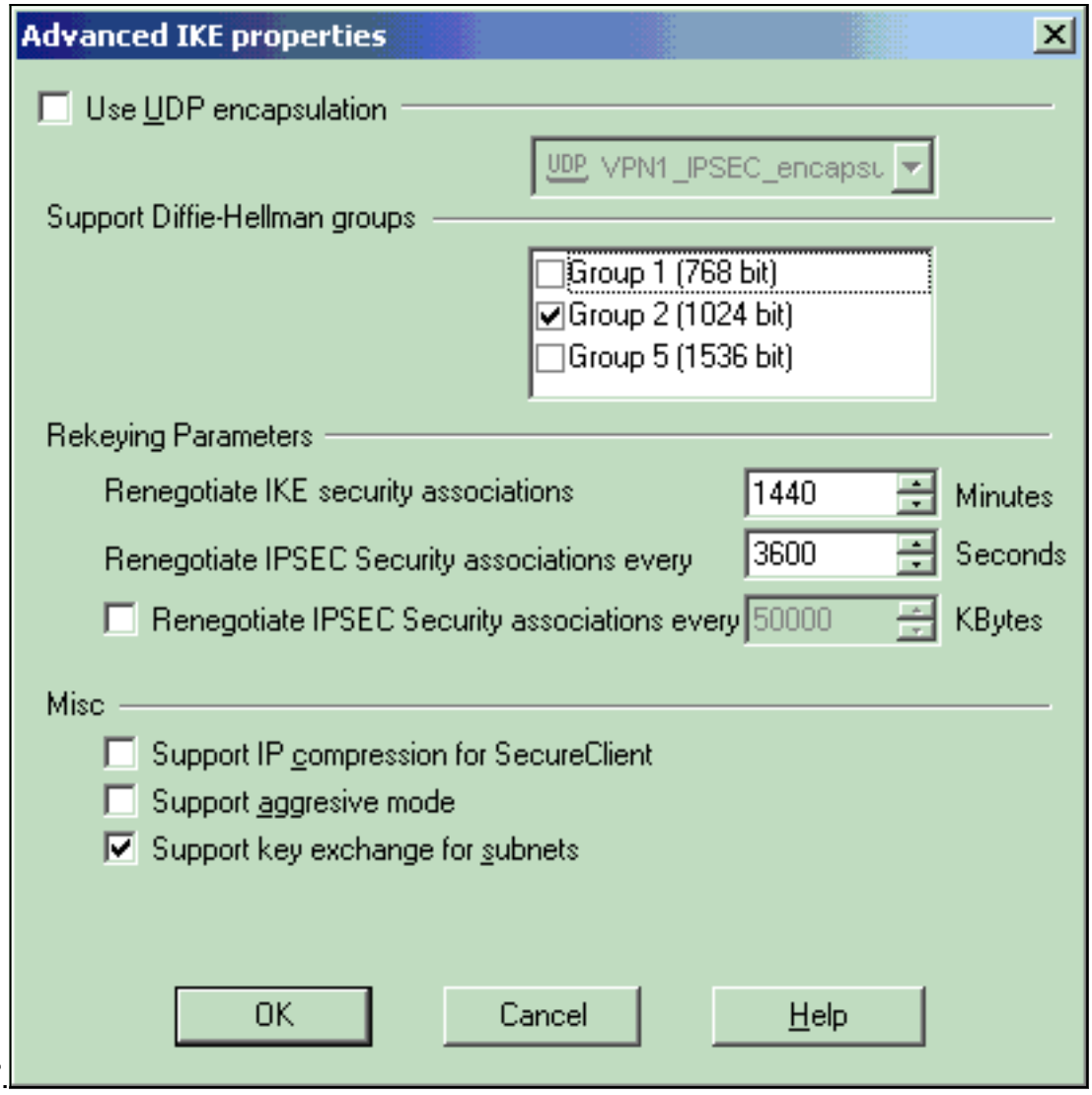
MD5.

8. Sélectionnez l'option d'authentification pour des **secrets pré-partagés**, puis cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être compatible avec la clé pré-partagée sur le concentrateur VPN. Cliquez sur Edit afin d'introduire votre clé comme affiché, puis cliquez sur le **positionnement**,



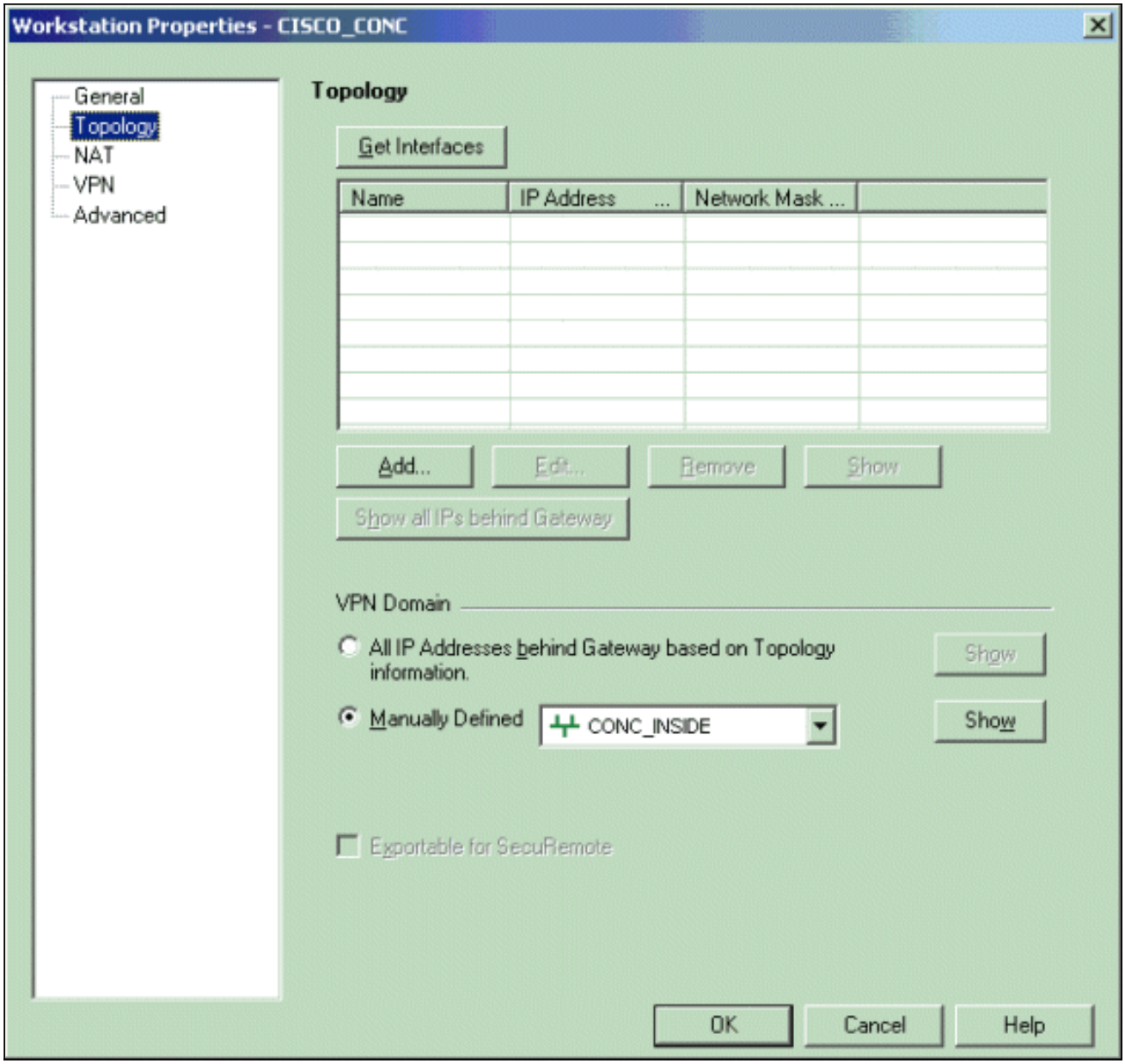
OK.

9. De la fenêtre de propriétés IKE, cliquez sur **avancé…** et changez ces configurations :Désélectionnez l'option pour le **mode agressif de support**.Sélectionnez l'option pour l'**échange de clé de support pour des sous-réseaux**.Quand vous êtes de finition, cliquez sur OK,

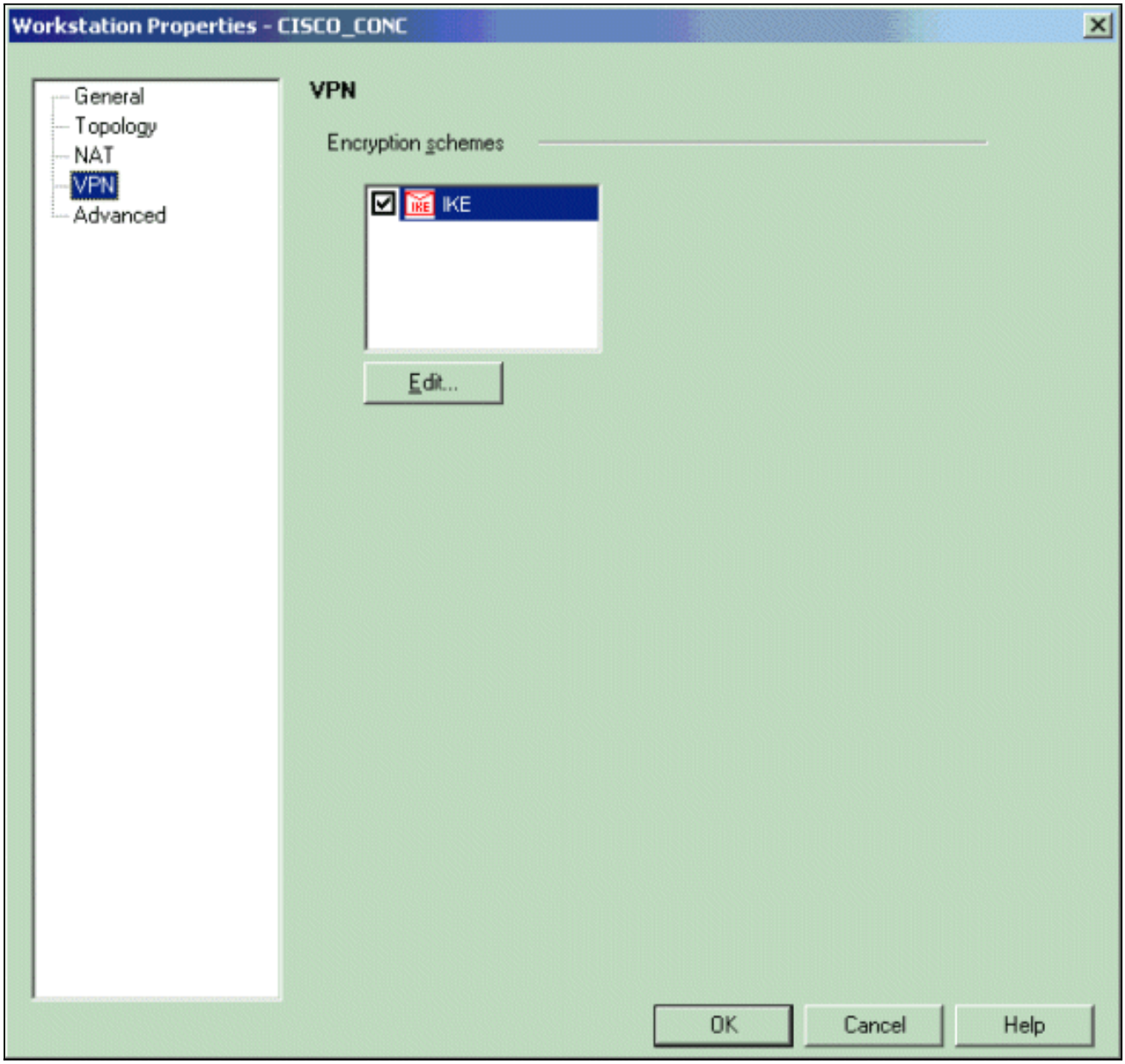


CORRECT.

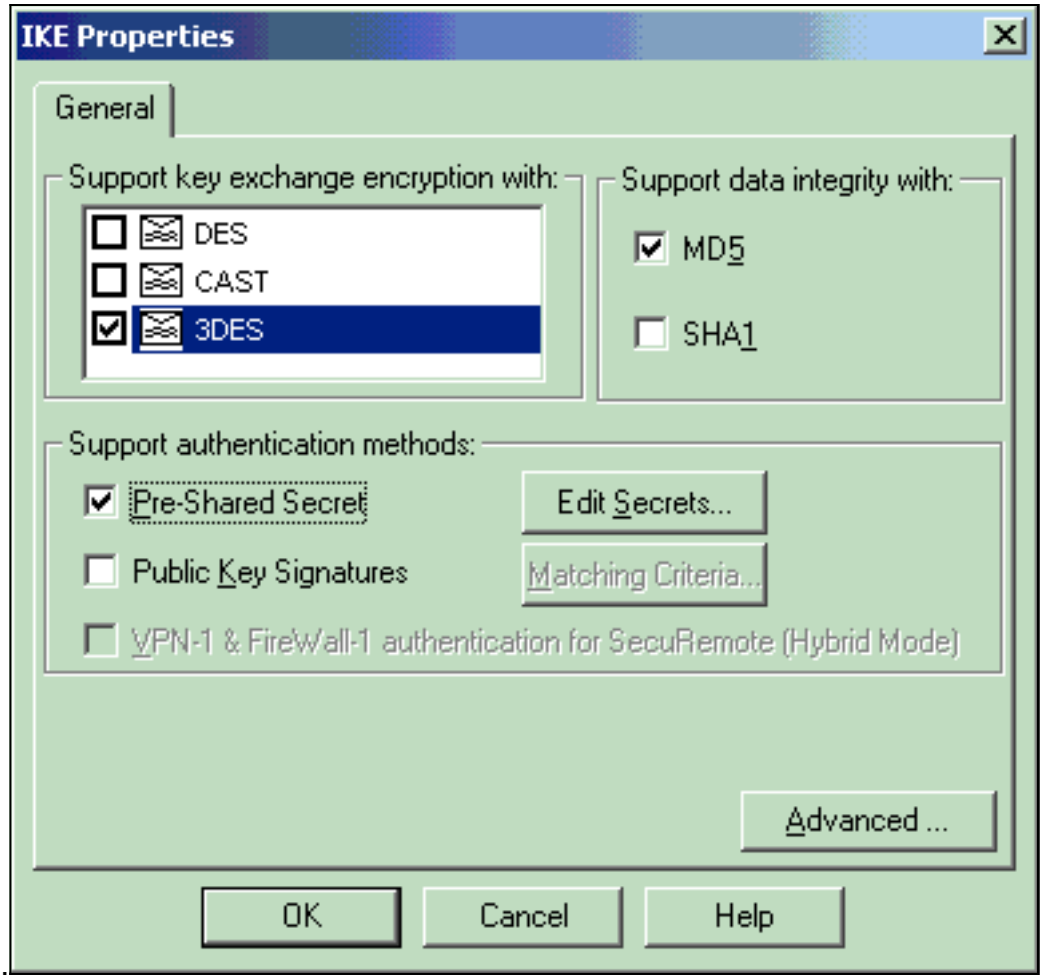
10. Allez **gérer > des objets de réseau > éditent** afin d'ouvrir la fenêtre de Properties de poste de travail pour le concentrateur VPN. **Topologie** choisie des choix du côté gauche de la fenêtre afin de définir manuellement le domaine VPN.Dans cet exemple, CONC_INSIDE (le réseau intérieur du concentrateur VPN) est défini comme domaine VPN.



11. **Le VPN** choisi des choix du côté gauche de la fenêtre, sélectionnent alors l'**IKE** comme structure de chiffrement. Cliquez sur Edit afin de configurer les propriétés IKE.

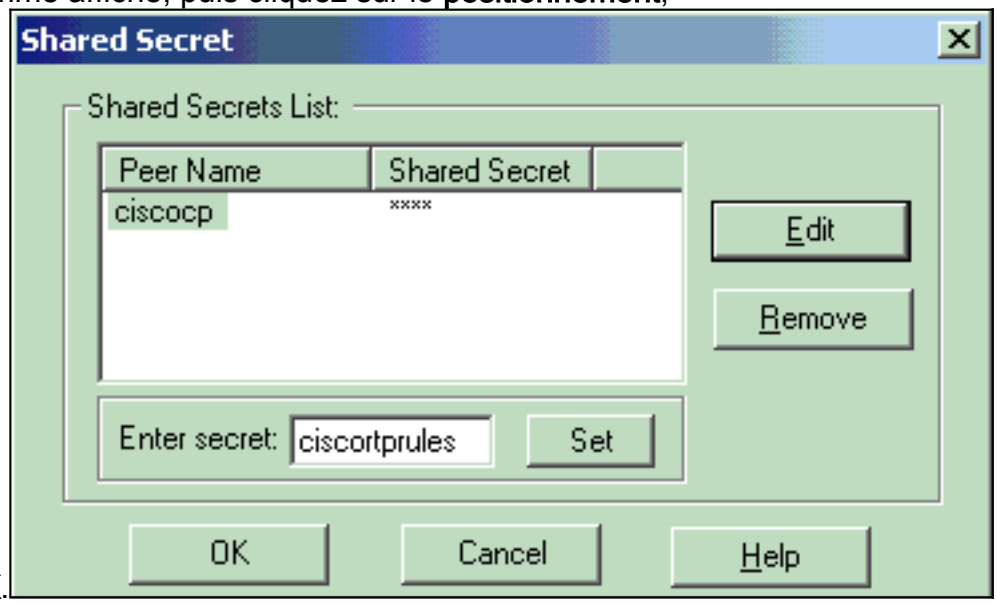


12. Placez les propriétés IKE pour refléter la configuration en cours sur le concentrateur VPN.Dans cet exemple, placez l'option de chiffrement pour **3DES** et l'option de hachage



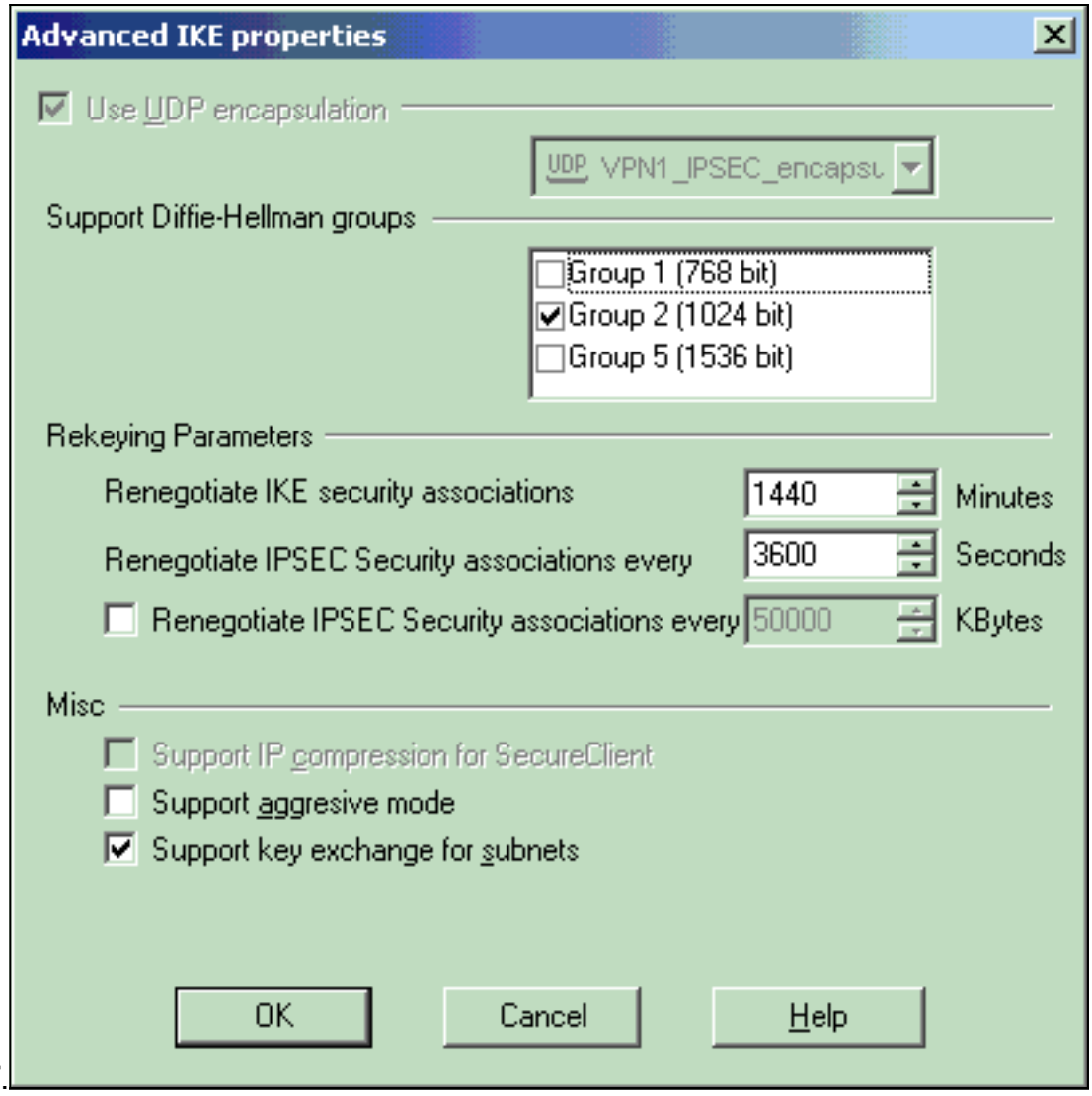
pour le **MD5**.

13. Sélectionnez l'option d'authentification pour des **secrets pré-partagés**, puis cliquez sur Edit les **secrets** afin de placer la clé pré-partagée. Cliquez sur Edit afin d'introduire votre clé comme affiché, puis cliquez sur le **positionnement**,



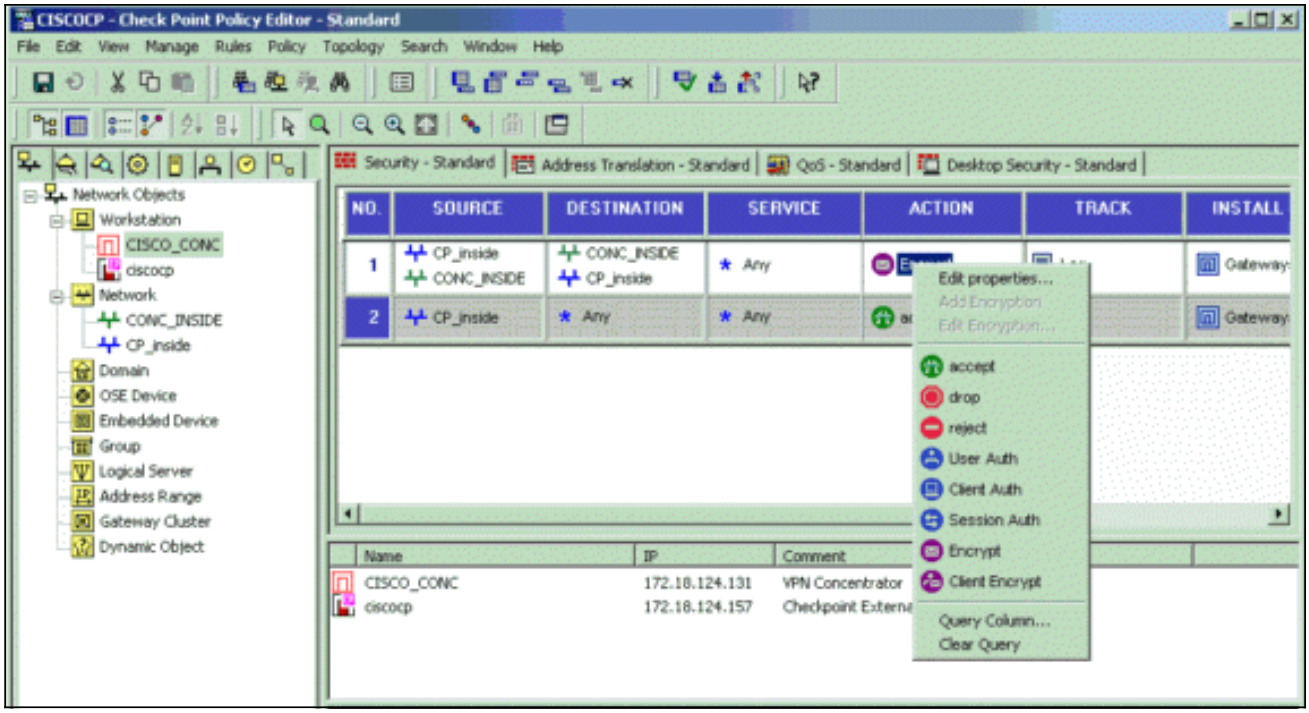
OK.

14. De la fenêtre de propriétés IKE, cliquez sur **avancé…** et changez ces configurations :Sélectionnez le groupe de Diffie-Hellman approprié pour les propriétés IKE.Désélectionnez l'option pour le **mode agressif de support**.Sélectionnez l'option pour l'**échange de clé de support pour des sous-réseaux**.Quand vous êtes de finition, cliquez sur OK,

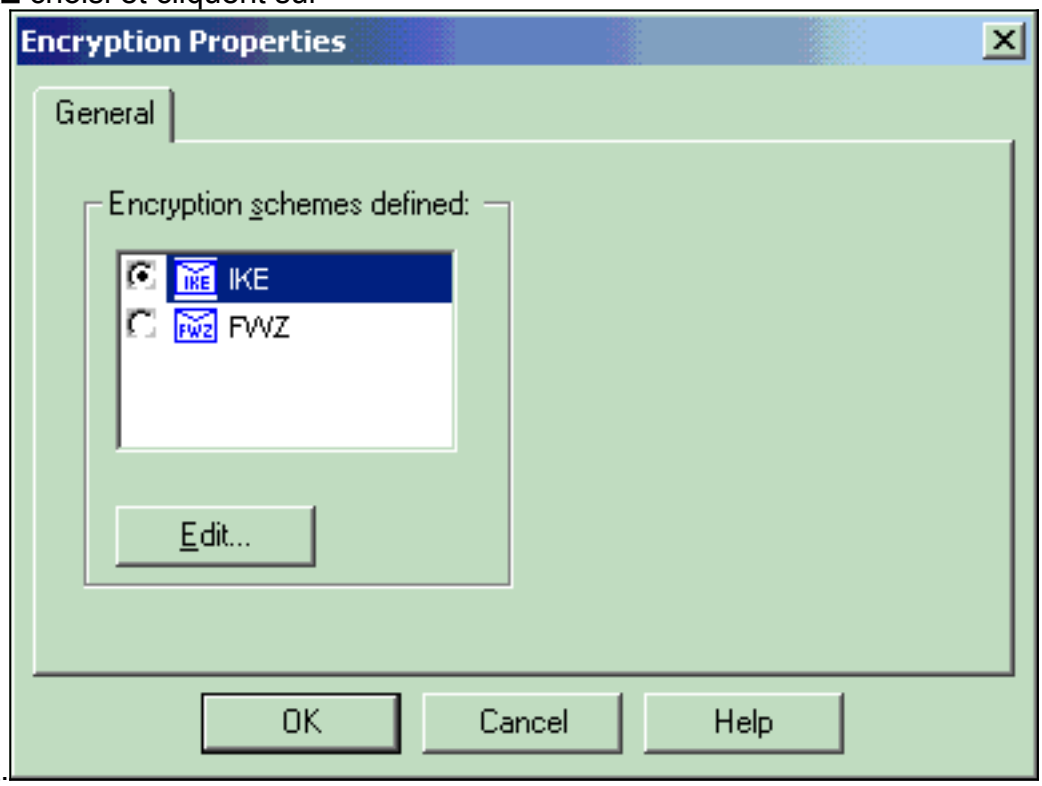


CORRECT.

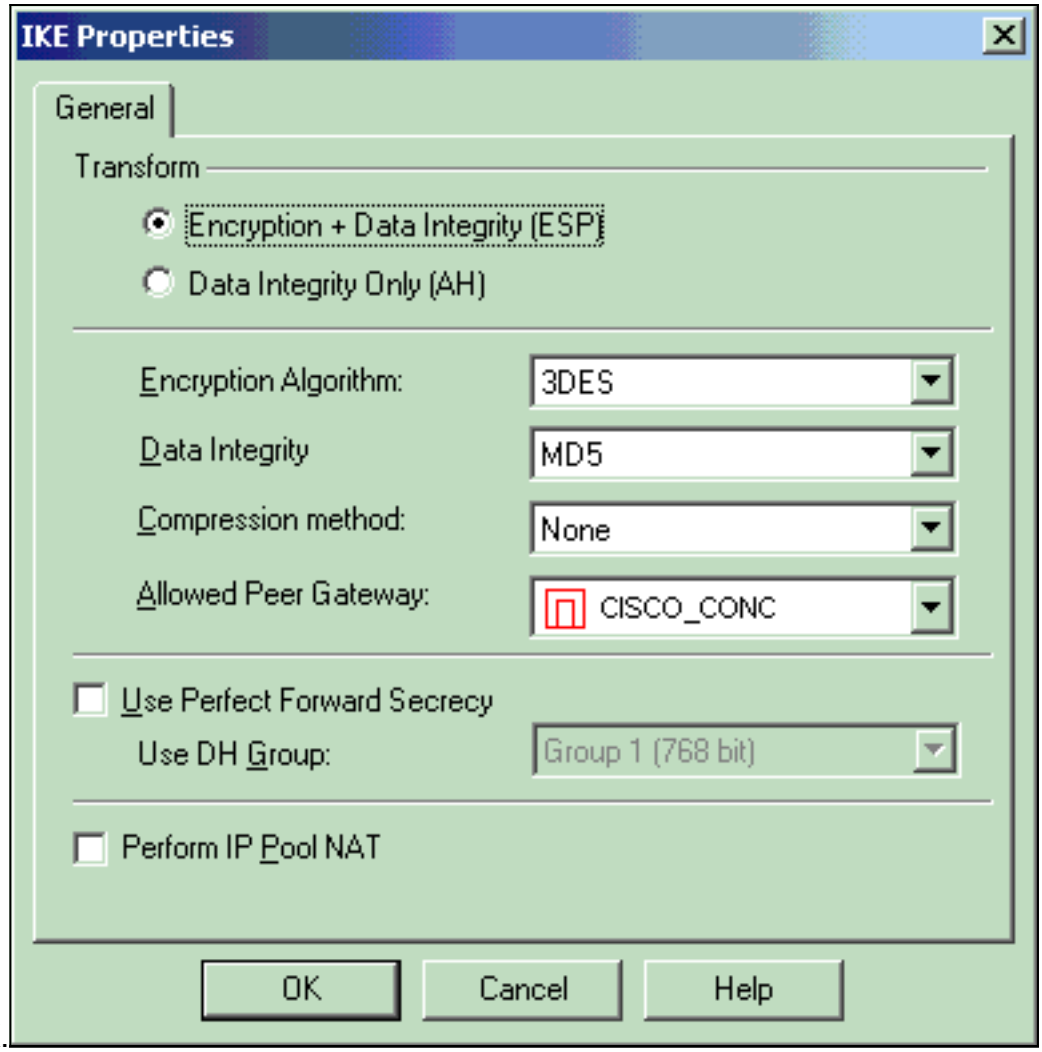
15. **Les règles** choisies **> ajoutent les règles > le dessus** afin de configurer les règles de cryptage pour la stratégie. Dans la fenêtre de l'éditeur de stratégie, insérez une règle avec la source comme CP_inside (réseau d'intérieur de Checkpoint NG) et la destination comme CONC_INSIDE (réseau d'intérieur du concentrateur VPN). Placez les valeurs pour le **service =**, l'**action = chiffrent**, et **piste = log**. Quand vous avez ajouté la section d'action de chiffrer de la règle, cliquez avec le bouton droit l'**action** et choisi **éditez Properties**.



16. **L'IKE** choisi et cliquent sur Edit.

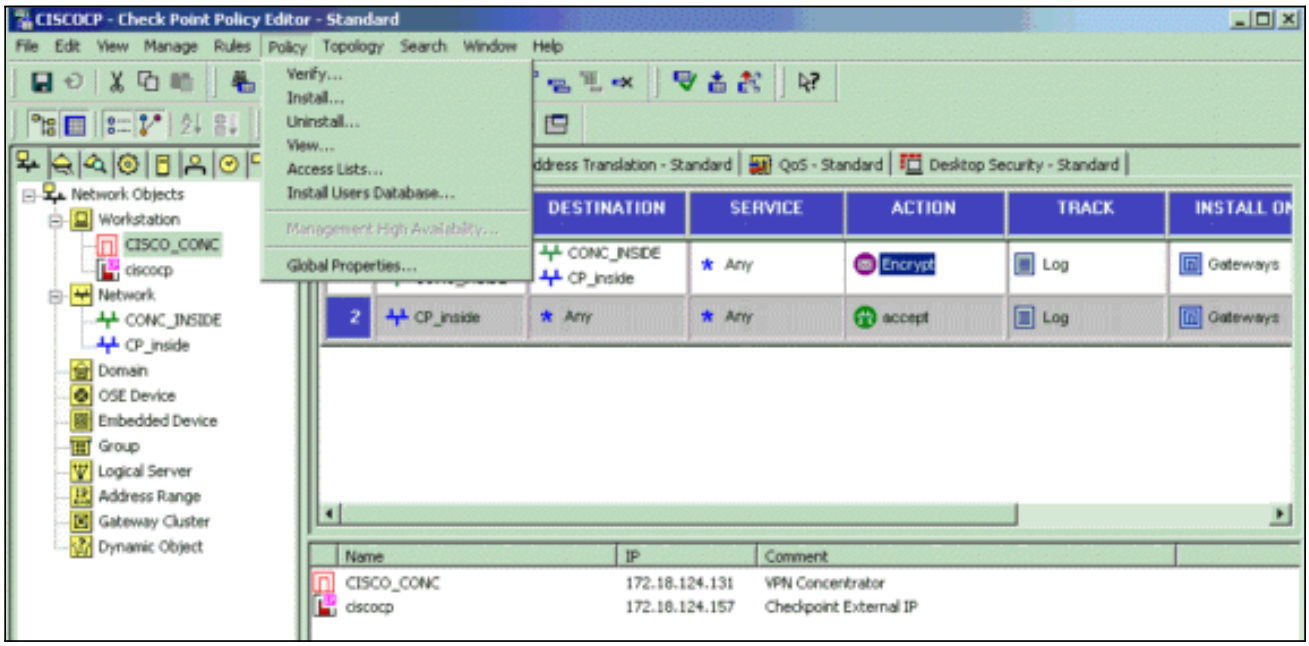


17. Sur la fenêtre de propriétés IKE, changez les propriétés pour être d'accord avec le concentrateur VPN transforment.Placez l'option de transformation au **cryptage + à l'intégrité des données (ESP)**.Placez l'algorithme de chiffrement à **3DES**.Fixez l'intégrité des données au **MD5**.Placez la passerelle homologue permise pour apparier le concentrateur VPN (CISCO_CONC).Quand vous êtes de finition, cliquez sur

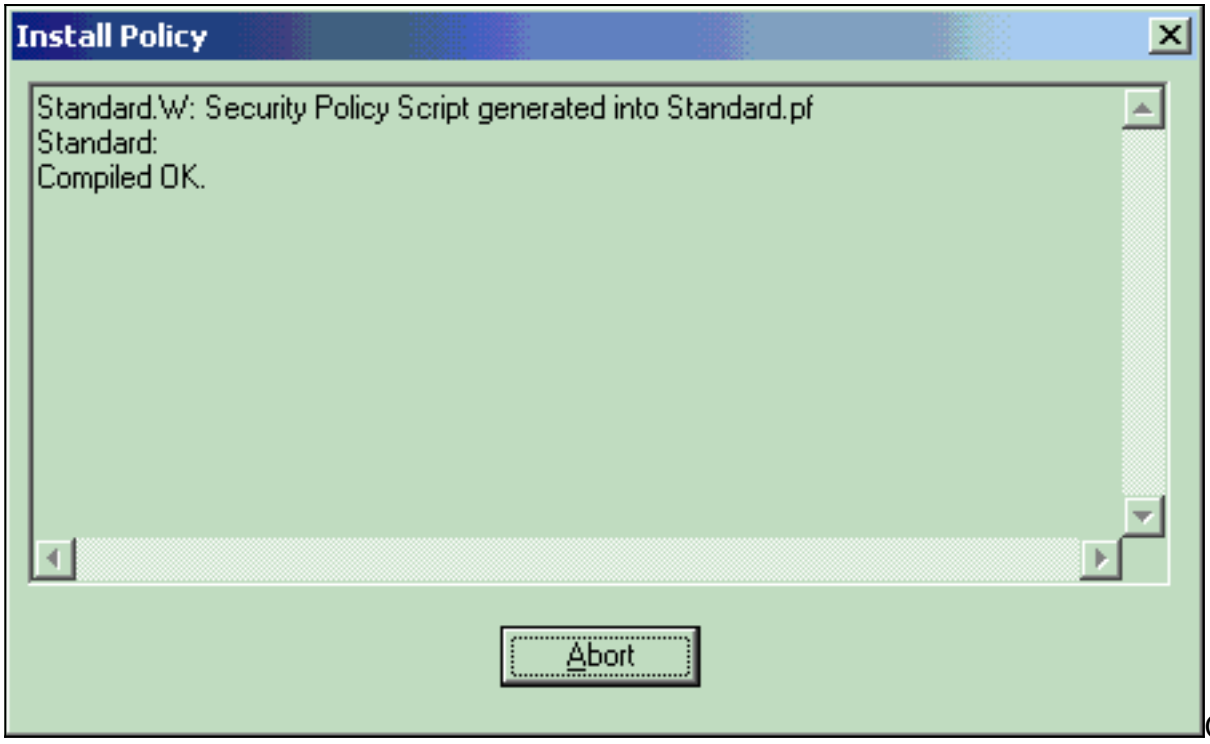


OK.

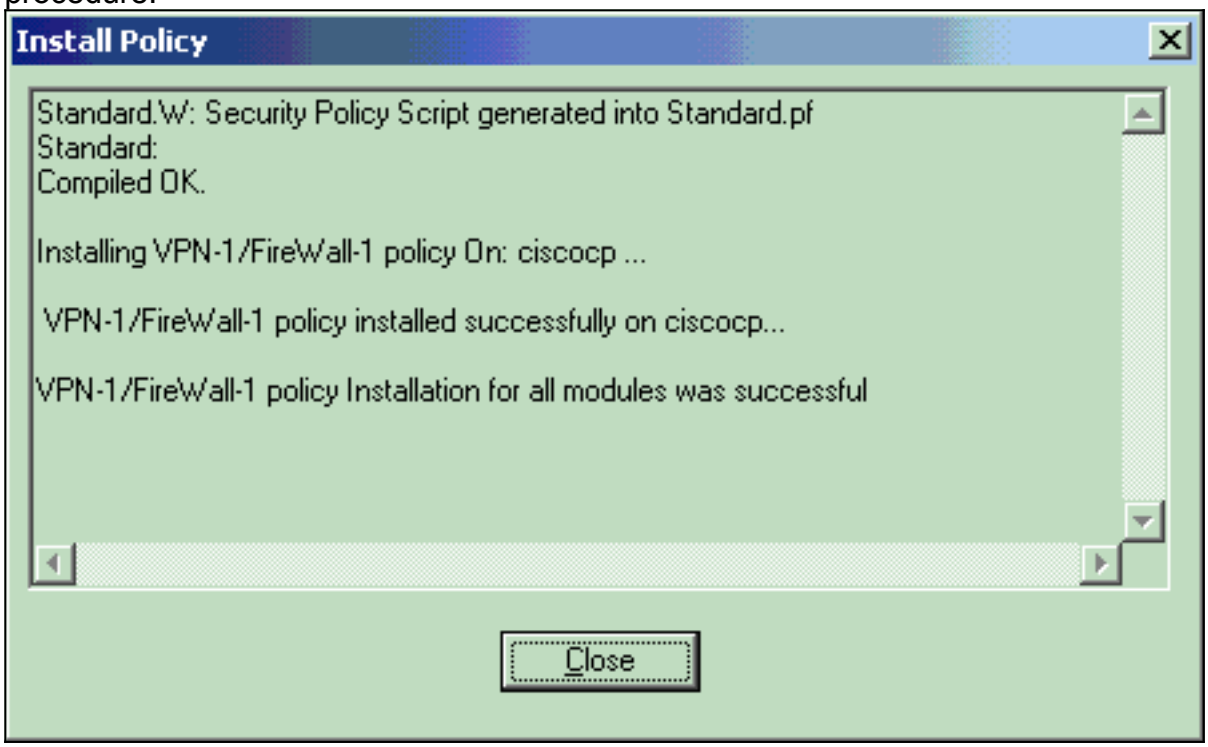
18. Après que Checkpoint NG soit configuré, sauvegardez la stratégie et la **stratégie** choisie **> installent** afin de l'activer.



La fenêtre d'installation affiche des notes en progression pendant que la stratégie est compilée.



Quand la fenêtre d'installation indique que l'installation de stratégie est complète, clic **étroit** afin de terminer la
procédure.

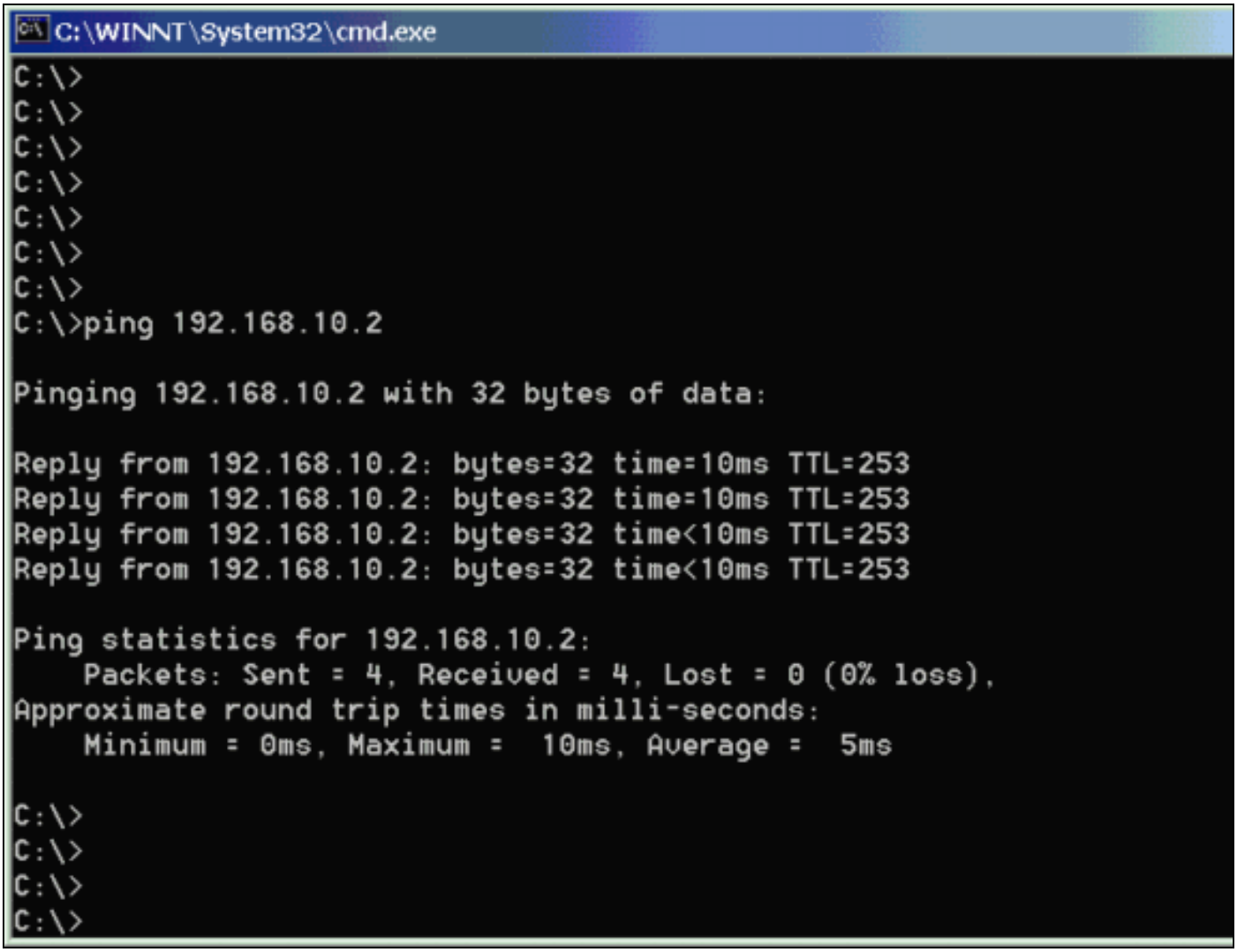


Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

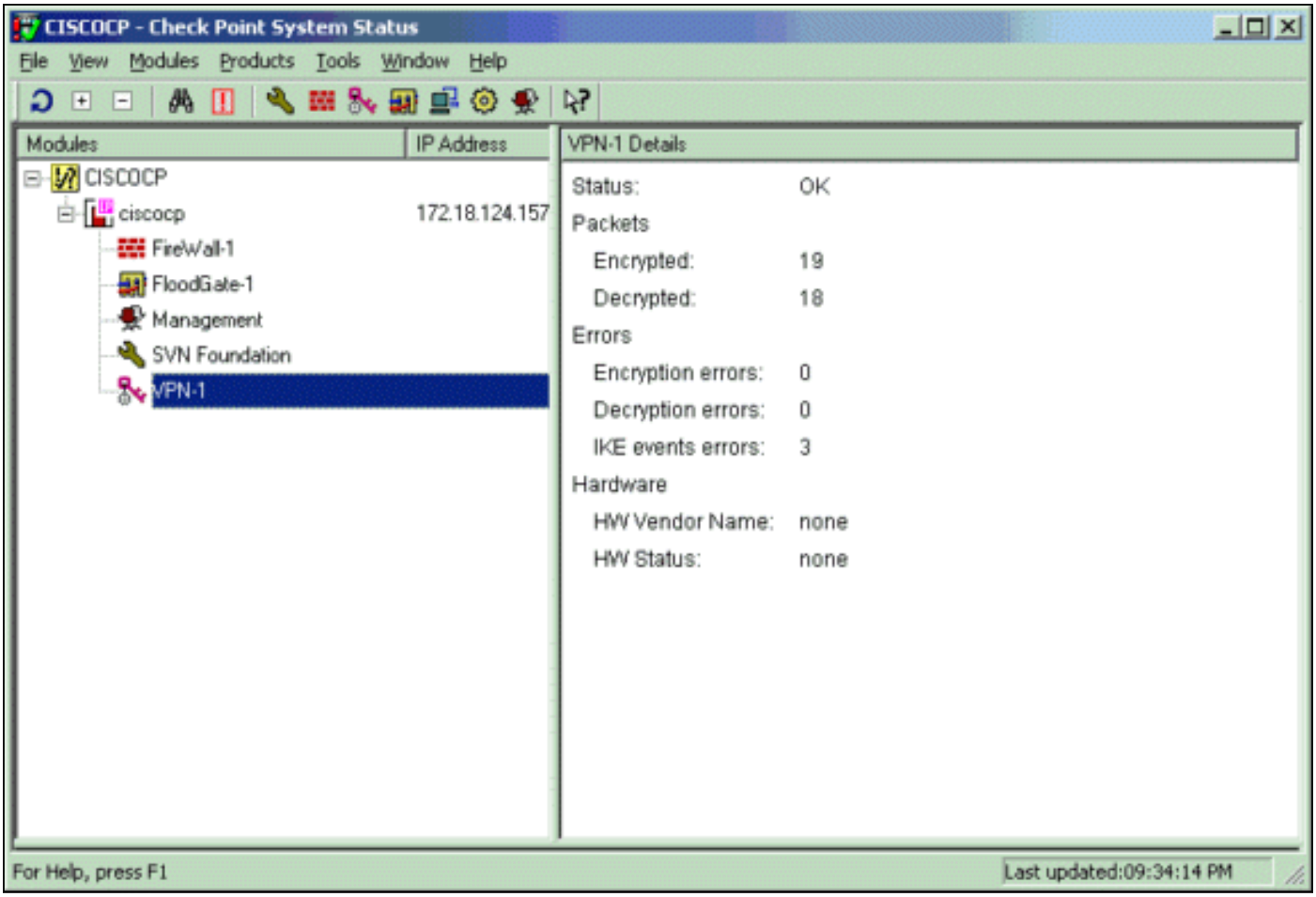
Vérifiez la communication réseau

Afin de tester la transmission entre les deux réseaux privés, vous pouvez initier un ping d'un des réseaux privés à l'autre réseau privé. Dans cette configuration, un ping a été envoyé du côté de Checkpoint NG (10.32.50.51) au réseau de concentrateur VPN (192.168.10.2).



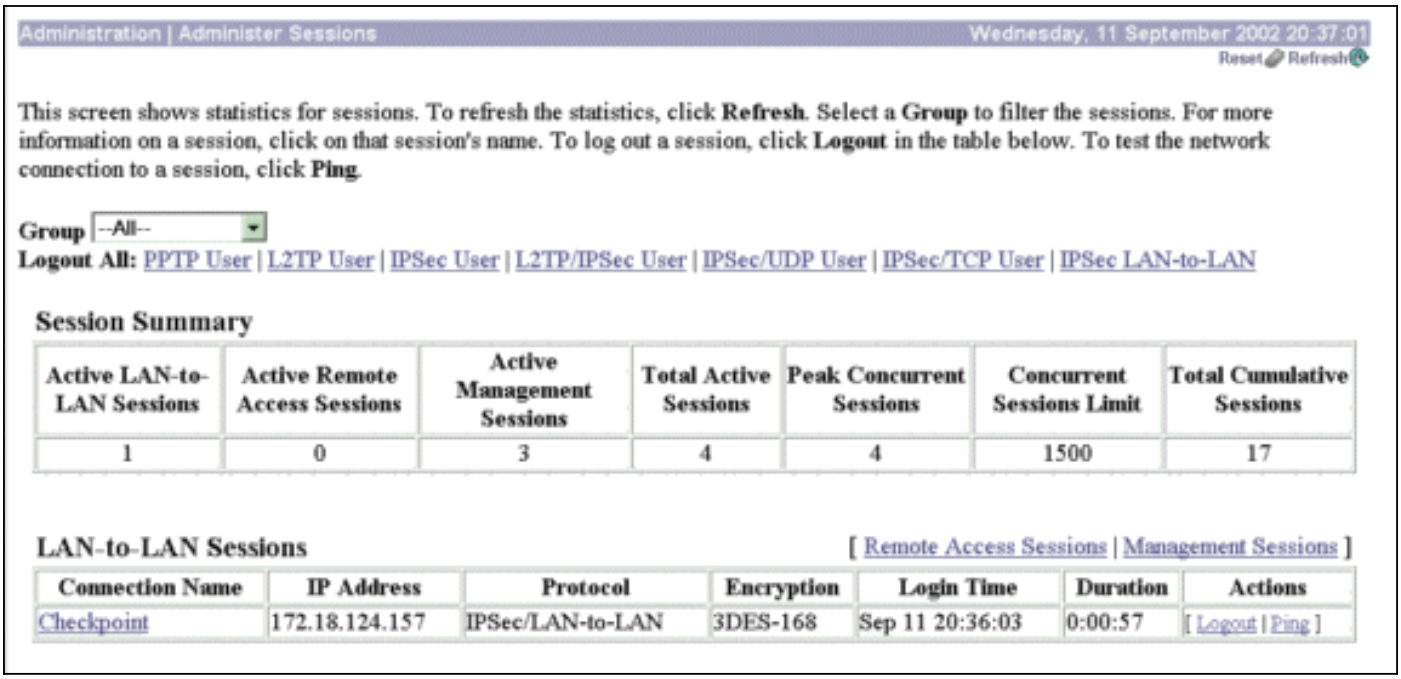
État de tunnel de vue sur Checkpoint NG

Afin de visualiser l'état de tunnel, allez à l'éditeur de stratégie et sélectionnez la **fenêtre > l'état du système**.



État de tunnel de vue sur le concentrateur VPN

Afin de vérifier l'état de tunnel sur le concentrateur VPN, allez à la **gestion > gèrent des sessions**.



Sous des sessions entre réseaux locaux, sélectionnez le nom de la connexion pour que le point de reprise visualise des détails sur SAS créée et le nombre de paquets transmis/reçus.

Administration | Administer Sessions | Detail — Wednesday, 11 September 2002 20:37:59
Reset Refresh

Back to Sessions

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Bytes Tx	Bytes Rx
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:01:55	256	256

IKE Sessions: 1
IPSec Sessions: 1

IKE Session			
Session ID	1	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**Diffie-Hellman Group**	Group 2 (1024-bit)
Authentication Mode	Pre-Shared Keys	**IKE Negotiation Mode**	Main
Rekey Time Interval	86400 seconds		
IPSec Session			
Session ID	2	**Remote Address**	10.32.0.0/0.0.127.255
Local Address	192.168.10.0/0.0.0.255	**Encryption Algorithm**	3DES-168
Hashing Algorithm	MD5	**SEP**	1
Encapsulation Mode	Tunnel	**Rekey Time Interval**	28800 seconds
Bytes Received	256	**Bytes Transmitted**	256

Dépannez

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

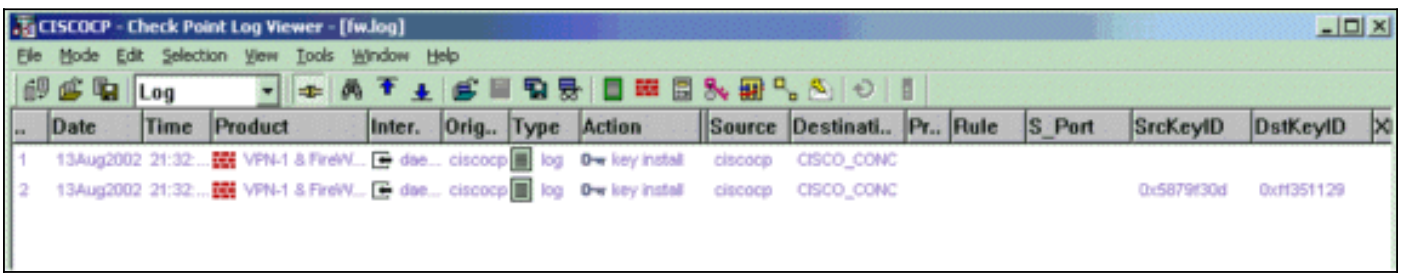
Note: Le trafic ne doit pas être PATed à travers le tunnel d'IPSec utilisant l'adresse IP publique de concentrateur VPN (interface d'extérieur). Autrement, le tunnel échoue. Ainsi, l'adresse IP utilisée pour PATing doit être une adresse autre que l'adresse configurée sur l'interface extérieure.

Récapitulation de réseau

Quand le multiple adjacent, les réseaux intérieurs sont configurés dans le domaine de cryptage sur le point de reprise, le périphérique peut automatiquement récapituler les réseaux en ce qui concerne le trafic intéressant. Si le concentrateur VPN n'est pas configuré pour s'assortir, le tunnel est susceptible d'échouer. Par exemple, si les réseaux intérieurs de 10.0.0.0 /24 et de 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ces réseaux peuvent être récapitulés à 10.0.0.0 /23.

Debugs pour Checkpoint NG

Afin de visualiser les logs, **fenêtre > visualiseur** choisis de **log**.



Debugs pour le concentrateur VPN

Afin d'activer met au point sur le concentrateur VPN, vont à la **configuration > au système > aux événements > aux classes**. Activez AUTHENTIQUE, AUTHDBG, IKE, IKEDBG, IPSEC, et IPSECDBG pour la sévérité pour se connecter en tant que 1 - 13. Afin de visualiser met au point, **surveillance > journal d'événements filtrables** choisis.

```
1 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=506 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + SA (1) + VENDOR (13) + NONE (0) ... total length : 128

3 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=507 172.18.124.157
processing SA payload

4 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=508
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

10 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=509
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

13 09/11/2002 20:36:03.610 SEV=7 IKEDBG/0 RPT=510 172.18.124.157
Oakley proposal is acceptable

14 09/11/2002 20:36:03.610 SEV=9 IKEDBG/47 RPT=9 172.18.124.157
processing VID payload

15 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=511 172.18.124.157
processing IKE SA

16 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=512
Proposal # 1, Transform # 1, Type ISAKMP, Id IKE
Parsing received transform:
Phase 1 failure against global IKE proposal # 1:
Mismatched attr types for class Auth Method:
Rcv'd: Preshared Key
Cfg'd: XAUTH with Preshared Key (Initiator authenticated)

22 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=513
Phase 1 failure against global IKE proposal # 2:
Mismatched attr types for class DH Group:
Rcv'd: Oakley Group 2
Cfg'd: Oakley Group 1

25 09/11/2002 20:36:03.610 SEV=7 IKEDBG/28 RPT=9 172.18.124.157
IKE SA Proposal # 1, Transform # 1 acceptable
Matches global IKE entry # 3

26 09/11/2002 20:36:03.610 SEV=9 IKEDBG/0 RPT=514 172.18.124.157
constructing ISA_SA for isakmp

27 09/11/2002 20:36:03.610 SEV=8 IKEDBG/0 RPT=515 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 84

29 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=516 172.18.124.157
```

```
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

31 09/11/2002 20:36:03.630 SEV=8 IKEDBG/0 RPT=517 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 184

33 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=518 172.18.124.157
processing ke payload

34 09/11/2002 20:36:03.630 SEV=9 IKEDBG/0 RPT=519 172.18.124.157
processing ISA_KE

35 09/11/2002 20:36:03.630 SEV=9 IKEDBG/1 RPT=91 172.18.124.157
processing nonce payload

36 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=520 172.18.124.157
constructing ke payload

37 09/11/2002 20:36:03.660 SEV=9 IKEDBG/1 RPT=92 172.18.124.157
constructing nonce payload

38 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=37 172.18.124.157
constructing Cisco Unity VID payload

39 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=38 172.18.124.157
constructing xauth V6 VID payload

40 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=19 172.18.124.157
Send IOS VID

41 09/11/2002 20:36:03.660 SEV=9 IKEDBG/38 RPT=10 172.18.124.157
Constructing VPN 3000 spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)

43 09/11/2002 20:36:03.660 SEV=9 IKEDBG/46 RPT=39 172.18.124.157
constructing VID payload

44 09/11/2002 20:36:03.660 SEV=9 IKEDBG/48 RPT=20 172.18.124.157
Send Altiga GW VID

45 09/11/2002 20:36:03.660 SEV=9 IKEDBG/0 RPT=521 172.18.124.157
Generating keys for Responder...

46 09/11/2002 20:36:03.670 SEV=8 IKEDBG/0 RPT=522 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) ... total length : 256

48 09/11/2002 20:36:03.690 SEV=8 IKEDBG/0 RPT=523 172.18.124.157
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) + NONE (0) ... total length : 60

50 09/11/2002 20:36:03.690 SEV=9 IKEDBG/1 RPT=93 172.18.124.157
Group [172.18.124.157]
Processing ID

51 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=524 172.18.124.157
Group [172.18.124.157]
processing hash

52 09/11/2002 20:36:03.690 SEV=9 IKEDBG/0 RPT=525 172.18.124.157
Group [172.18.124.157]
computing hash
```

```
53 09/11/2002 20:36:03.690 SEV=9 IKEDBG/23 RPT=10 172.18.124.157
Group [172.18.124.157]
Starting group lookup for peer 172.18.124.157

54 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/1 RPT=10
AUTH_Open() returns 9

55 09/11/2002 20:36:03.690 SEV=7 AUTH/12 RPT=10
Authentication session opened: handle = 9

56 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/3 RPT=10
AUTH_PutAttrTable(9, 748174)

57 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/6 RPT=10
AUTH_GroupAuthenticate(9, 2f1b19c, 49c648)

58 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/59 RPT=10
AUTH_BindServer(51a6b48, 0, 0)

59 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/69 RPT=10
Auth Server e054d4 has been bound to ACB 51a6b48, sessions = 1

60 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/65 RPT=10
AUTH_CreateTimer(51a6b48, 0, 0)

61 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/72 RPT=10
Reply timer created: handle = 4B0018

62 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/61 RPT=10
AUTH_BuildMsg(51a6b48, 0, 0)

63 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/64 RPT=10
AUTH_StartTimer(51a6b48, 0, 0)

64 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/73 RPT=10
Reply timer started: handle = 4B0018, timestamp = 1163319,
timeout = 30000

65 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/62 RPT=10
AUTH_SndRequest(51a6b48, 0, 0)

66 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/50 RPT=19
IntDB_Decode(3825300, 156)

67 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=19
IntDB_Xmt(51a6b48)

68 09/11/2002 20:36:03.690 SEV=9 AUTHDBG/71 RPT=10
xmit_cnt = 1

69 09/11/2002 20:36:03.690 SEV=8 AUTHDBG/47 RPT=20
IntDB_Xmt(51a6b48)

70 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/49 RPT=10
IntDB_Match(51a6b48, 3eb7ab0)

71 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/63 RPT=10
AUTH_RcvReply(51a6b48, 0, 0)

72 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/50 RPT=20
IntDB_Decode(3eb7ab0, 298)

73 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/48 RPT=10
IntDB_Rcv(51a6b48)
```

```
74 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/66 RPT=10
AUTH_DeleteTimer(51a6b48, 0, 0)

75 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/74 RPT=10
Reply timer stopped: handle = 4B0018, timestamp = 1163329

76 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/58 RPT=10
AUTH_Callback(51a6b48, 0, 0)

77 09/11/2002 20:36:03.790 SEV=6 AUTH/41 RPT=10 172.18.124.157
Authentication successful: handle = 9, server = Internal,
group = 172.18.124.157

78 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=526 172.18.124.157
Group [172.18.124.157]
Found Phase 1 Group (172.18.124.157)

79 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/4 RPT=10
AUTH_GetAttrTable(9, 748420)

80 09/11/2002 20:36:03.790 SEV=7 IKEDBG/14 RPT=10 172.18.124.157
Group [172.18.124.157]
Authentication configured for Internal

81 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=19 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: IP Compression = disabled

82 09/11/2002 20:36:03.790 SEV=9 IKEDBG/19 RPT=20 172.18.124.157
Group [172.18.124.157]
IKEGetUserAttributes: Split Tunneling Policy = Disabled

83 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/2 RPT=10
AUTH_Close(9)

84 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=94 172.18.124.157
Group [172.18.124.157]
constructing ID

85 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=527
Group [172.18.124.157]
construct hash payload

86 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=528 172.18.124.157
Group [172.18.124.157]
computing hash

87 09/11/2002 20:36:03.790 SEV=9 IKEDBG/46 RPT=40 172.18.124.157
Group [172.18.124.157]
constructing dpd vid payload

88 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=529 172.18.124.157
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + HASH (8) ... total length : 80

90 09/11/2002 20:36:03.790 SEV=4 IKE/119 RPT=10 172.18.124.157
Group [172.18.124.157]
PHASE 1 COMPLETED

91 09/11/2002 20:36:03.790 SEV=6 IKE/121 RPT=10 172.18.124.157
Keep-alive type for this connection: None

92 09/11/2002 20:36:03.790 SEV=6 IKE/122 RPT=10 172.18.124.157
```

```
Keep-alives configured on but peer does not
support keep-alives (type = None)

93 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=530 172.18.124.157
Group [172.18.124.157]
Starting phase 1 rekey timer: 64800000 (ms)

94 09/11/2002 20:36:03.790 SEV=4 AUTH/22 RPT=16
User 172.18.124.157 connected

95 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/60 RPT=10
AUTH_UnbindServer(51a6b48, 0, 0)

96 09/11/2002 20:36:03.790 SEV=9 AUTHDBG/70 RPT=10
Auth Server e054d4 has been unbound from ACB 51a6b48, sessions = 0

97 09/11/2002 20:36:03.790 SEV=8 AUTHDBG/10 RPT=10
AUTH_Int_FreeAuthCB(51a6b48)

98 09/11/2002 20:36:03.790 SEV=7 AUTH/13 RPT=10
Authentication session closed: handle = 9

99 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=531 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

102 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=532 172.18.124.157
Group [172.18.124.157]
processing hash

103 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=533 172.18.124.157
Group [172.18.124.157]
processing SA payload

104 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=95 172.18.124.157
Group [172.18.124.157]
processing nonce payload

105 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=96 172.18.124.157
Group [172.18.124.157]
Processing ID

106 09/11/2002 20:36:03.790 SEV=5 IKE/35 RPT=6 172.18.124.157
Group [172.18.124.157]
Received remote IP Proxy Subnet data in ID Payload:
Address 10.32.0.0, Mask 255.255.128.0, Protocol 0, Port 0

109 09/11/2002 20:36:03.790 SEV=9 IKEDBG/1 RPT=97 172.18.124.157
Group [172.18.124.157]
Processing ID

110 09/11/2002 20:36:03.790 SEV=5 IKE/34 RPT=6 172.18.124.157
Group [172.18.124.157]
Received local IP Proxy Subnet data in ID Payload:
Address 192.168.10.0, Mask 255.255.255.0, Protocol 0, Port 0

113 09/11/2002 20:36:03.790 SEV=8 IKEDBG/0 RPT=534
QM IsRekeyed old sa not found by addr

114 09/11/2002 20:36:03.790 SEV=5 IKE/66 RPT=8 172.18.124.157
Group [172.18.124.157]
IKE Remote Peer configured for SA: L2L: Checkpoint
```

```
115 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=535 172.18.124.157
Group [172.18.124.157]
processing IPSEC SA

116 09/11/2002 20:36:03.790 SEV=7 IKEDBG/27 RPT=8 172.18.124.157
Group [172.18.124.157]
IPSec SA Proposal # 1, Transform # 1 acceptable

117 09/11/2002 20:36:03.790 SEV=7 IKEDBG/0 RPT=536 172.18.124.157
Group [172.18.124.157]
IKE: requesting SPI!

118 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/6 RPT=39
IPSEC key message parse - msgtype 6, len 200, vers 1, pid 00000000,
seq 10, err 0, type 2, mode 0, state 32, label 0, pad 0,
spi 00000000, encrKeyLen 0, hashKeyLen 0, ivlen 0, alg 0, hmacAlg 0,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 300

122 09/11/2002 20:36:03.790 SEV=9 IPSECDBG/1 RPT=139
Processing KEY_GETSPI msg!

123 09/11/2002 20:36:03.790 SEV=7 IPSECDBG/13 RPT=10
Reserved SPI 305440147

124 09/11/2002 20:36:03.790 SEV=8 IKEDBG/6 RPT=10
IKE got SPI from key engine: SPI = 0x1234a593

125 09/11/2002 20:36:03.790 SEV=9 IKEDBG/0 RPT=537 172.18.124.157
Group [172.18.124.157]
oakley constucting quick mode

126 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=538 172.18.124.157
Group [172.18.124.157]
constructing blank hash

127 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=539 172.18.124.157
Group [172.18.124.157]
constructing ISA_SA for ipsec

128 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=98 172.18.124.157
Group [172.18.124.157]
constructing ipsec nonce payload

129 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=99 172.18.124.157
Group [172.18.124.157]
constructing proxy ID

130 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=540 172.18.124.157
Group [172.18.124.157]
Transmitting Proxy Id:
Remote subnet: 10.32.0.0 Mask 255.255.128.0 Protocol 0 Port 0
Local subnet: 192.168.10.0 mask 255.255.255.0 Protocol 0 Port 0

134 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=541 172.18.124.157
Group [172.18.124.157]
constructing qm hash

135 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=542 172.18.124.157
SENDING Message (msgid=54796f76) with payloads :
HDR + HASH (8) + SA (1) ... total length : 152

137 09/11/2002 20:36:03.800 SEV=8 IKEDBG/0 RPT=543 172.18.124.157
RECEIVED Message (msgid=54796f76) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48
```

```
139 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=544 172.18.124.157
Group [172.18.124.157]
processing hash

140 09/11/2002 20:36:03.800 SEV=9 IKEDBG/0 RPT=545 172.18.124.157
Group [172.18.124.157]
loading all IPSEC SAs

141 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=100 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

142 09/11/2002 20:36:03.800 SEV=9 IKEDBG/1 RPT=101 172.18.124.157
Group [172.18.124.157]
Generating Quick Mode Key!

143 09/11/2002 20:36:03.800 SEV=7 IKEDBG/0 RPT=546 172.18.124.157
Group [172.18.124.157]
Loading subnet:
Dst: 192.168.10.0 mask: 255.255.255.0
Src: 10.32.0.0 mask: 255.255.128.0

146 09/11/2002 20:36:03.800 SEV=4 IKE/49 RPT=7 172.18.124.157
Group [172.18.124.157]
Security negotiation complete for LAN-to-LAN Group (172.18.124.157)
Responder, Inbound SPI = 0x1234a593, Outbound SPI = 0x0df37959

149 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/6 RPT=40
IPSEC key message parse - msgtype 1, len 606, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 64, label 0, pad 0,
spi 0df37959, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

153 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=140
Processing KEY_ADD msg!

154 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=141
key_msghdr2secassoc(): Enter

155 09/11/2002 20:36:03.800 SEV=7 IPSECDBG/1 RPT=142
No USER filter configured

156 09/11/2002 20:36:03.800 SEV=9 IPSECDBG/1 RPT=143
KeyProcessAdd: Enter

157 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=144
KeyProcessAdd: Adding outbound SA

158 09/11/2002 20:36:03.800 SEV=8 IPSECDBG/1 RPT=145
KeyProcessAdd: src 192.168.10.0 mask 0.0.0.255,
dst 10.32.0.0 mask 0.0.127.255

159 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=146
KeyProcessAdd: FilterIpsecAddIkeSa success

160 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/6 RPT=41
IPSEC key message parse - msgtype 3, len 327, vers 1, pid 00000000,
seq 0, err 0, type 2, mode 1, state 32, label 0, pad 0,
spi 1234a593, encrKeyLen 24, hashKeyLen 16, ivlen 8, alg 2, hmacAlg 3,
lifetype 0, lifetime1 17248580, lifetime2 0, dsId 0

164 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=147
Processing KEY_UPDATE msg!
```

```
165 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=148
Update inbound SA addresses

166 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=149
key_msghdr2secassoc(): Enter

167 09/11/2002 20:36:03.810 SEV=7 IPSECDBG/1 RPT=150
No USER filter configured

168 09/11/2002 20:36:03.810 SEV=9 IPSECDBG/1 RPT=151
KeyProcessUpdate: Enter

169 09/11/2002 20:36:03.810 SEV=8 IPSECDBG/1 RPT=152
KeyProcessUpdate: success

170 09/11/2002 20:36:03.810 SEV=8 IKEDBG/7 RPT=7
IKE got a KEY_ADD msg for SA: SPI = 0x0df37959

171 09/11/2002 20:36:03.810 SEV=8 IKEDBG/0 RPT=547
pitcher: rcv KEY_UPDATE, spi 0x1234a593

172 09/11/2002 20:36:03.810 SEV=4 IKE/120 RPT=7 172.18.124.157
Group [172.18.124.157]
PHASE 2 COMPLETED (msgid=54796f76)
```

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du Client VPN 3000 Series Cisco
- Page d'assistance IPsec
- Support technique - Cisco Systems