

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer le concentrateur VPN 3000](#)

[Configurer le contrôleur NG](#)

[Vérification](#)

[Vérification de la communication réseau](#)

[Afficher l'état du tunnel sur le contrôleur NG](#)

[Afficher l'état du tunnel sur le concentrateur VPN](#)

[Dépannage](#)

[Récapitulation de réseau](#)

[Débogues pour Checkpoint NG](#)

[Débogues pour le concentrateur VPN](#)

[Informations connexes](#)

Introduction

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

Conditions préalables

Conditions requises

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

divisé en cinq étapes, dont deux phases IKE (Internet Key Exchange). 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 les homologues authentifiés, un tunnel sécurisé est créé avec l'Association de sécurité Internet et le protocole ISAKMP (Key Management Protocol). Dans IKE Phase 2, les homologues IPSec utilisent le tunnel authentifié et sécurisé afin de négocier les transformations de SA IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi. Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformation IPSec. Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

Components Used

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

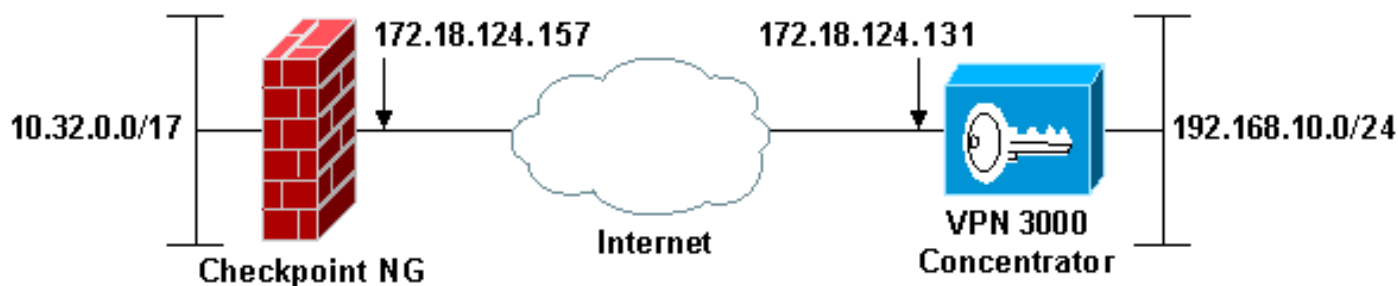
- Concentrateur de la gamme VPN 3000 3.5.2
- Pare-feu GN Checkpoint

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 :



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

Configurations

Configurer le concentrateur VPN 3000

Complétez ces étapes afin de configurer le concentrateur VPN 3000 :

1. Accédez à **Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN** afin de

configurer la session LAN-to-LAN. Définissez les options d'authentification et d'algorithmes IKE, de clé pré-partagée, d'adresse IP d'homologue et de paramètres de réseau local et distant. Cliquez sur Apply. Dans cette configuration, l'authentification a été définie comme ESP-MD5-HMAC et le chiffrement a été défini comme 3DES.

Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify

Modify an IPSec LAN-to-LAN connection.

Name	<input type="text" value="Checkpoint"/>	Enter the name for this LAN-to-LAN connection.
Interface	<input type="text" value="Ethernet 2 (Public) (172.18.124.131)"/>	Select the interface to put this LAN-to-LAN connection on.
Peer	<input type="text" value="172.18.124.157"/>	Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate	<input type="text" value="None (Use Preshared Keys)"/>	Select the Digital Certificate to use.
Certificate Transmission	<input type="radio"/> Entire certificate chain <input checked="" type="radio"/> Identity certificate only	Choose how to send the digital certificate to the IKE peer.
Preshared Key	<input type="text" value="ciscortprules"/>	Enter the preshared key for this LAN-to-LAN connection.
Authentication	<input type="text" value="ESP/MD5/HMAC-128"/>	Specify the packet authentication mechanism to use.
Encryption	<input type="text" value="3DES-168"/>	Specify the encryption mechanism to use.
IKE Proposal	<input type="text" value="IKE-3DES-MD5"/>	Select the IKE Proposal to use for this LAN-to-LAN connection.
Routing	<input type="text" value="None"/>	Choose the routing mechanism to use. Parameters below are ignored if Network Autodiscovery is chosen.

Local Network

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the local network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text" value="192.168.10.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text" value="0.0.0.255"/>	

Remote Network

Network List	<input type="text" value="Use IP Address/Wildcard-mask below"/>	Specify the remote network address list or the IP address and wildcard mask for this LAN-to-LAN connection.
IP Address	<input type="text" value="10.32.0.0"/>	Note: Enter a <i>wildcard</i> mask, which is the reverse of a subnet mask. A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
Wildcard Mask	<input type="text" value="0.0.127.255"/>	

- Accédez à **Configuration > System > Tunneling Protocols > IPSec > IKE Propositions** et définissez les paramètres requis. Sélectionnez la proposition IKE IKE-3DES-MD5 et vérifiez les paramètres sélectionnés pour la proposition. Cliquez sur **Apply** afin de configurer la session LAN à LAN. Voici les paramètres de cette configuration :

Configuration | System | Tunneling Protocols | IPSec | IKE Proposals | Modify

Modify a configured IKE Proposal.

Proposal Name	<input type="text" value="IKE-3DES-MD5"/>	Specify the name of this IKE Proposal.
Authentication Mode	<input type="text" value="Preshared Keys"/>	Select the authentication mode to use.
Authentication Algorithm	<input type="text" value="MD5/HMAC-128"/>	Select the packet authentication algorithm to use.
Encryption Algorithm	<input type="text" value="3DES-168"/>	Select the encryption algorithm to use.
Diffie-Hellman Group	<input type="text" value="Group 2 (1024-bits)"/>	Select the Diffie Hellman Group to use.
Lifetime Measurement	<input type="text" value="Time"/>	Select the lifetime measurement of the IKE keys.
Data Lifetime	<input type="text" value="10000"/>	Specify the data lifetime in kilobytes (KB).
Time Lifetime	<input type="text" value="86400"/>	Specify the time lifetime in seconds.

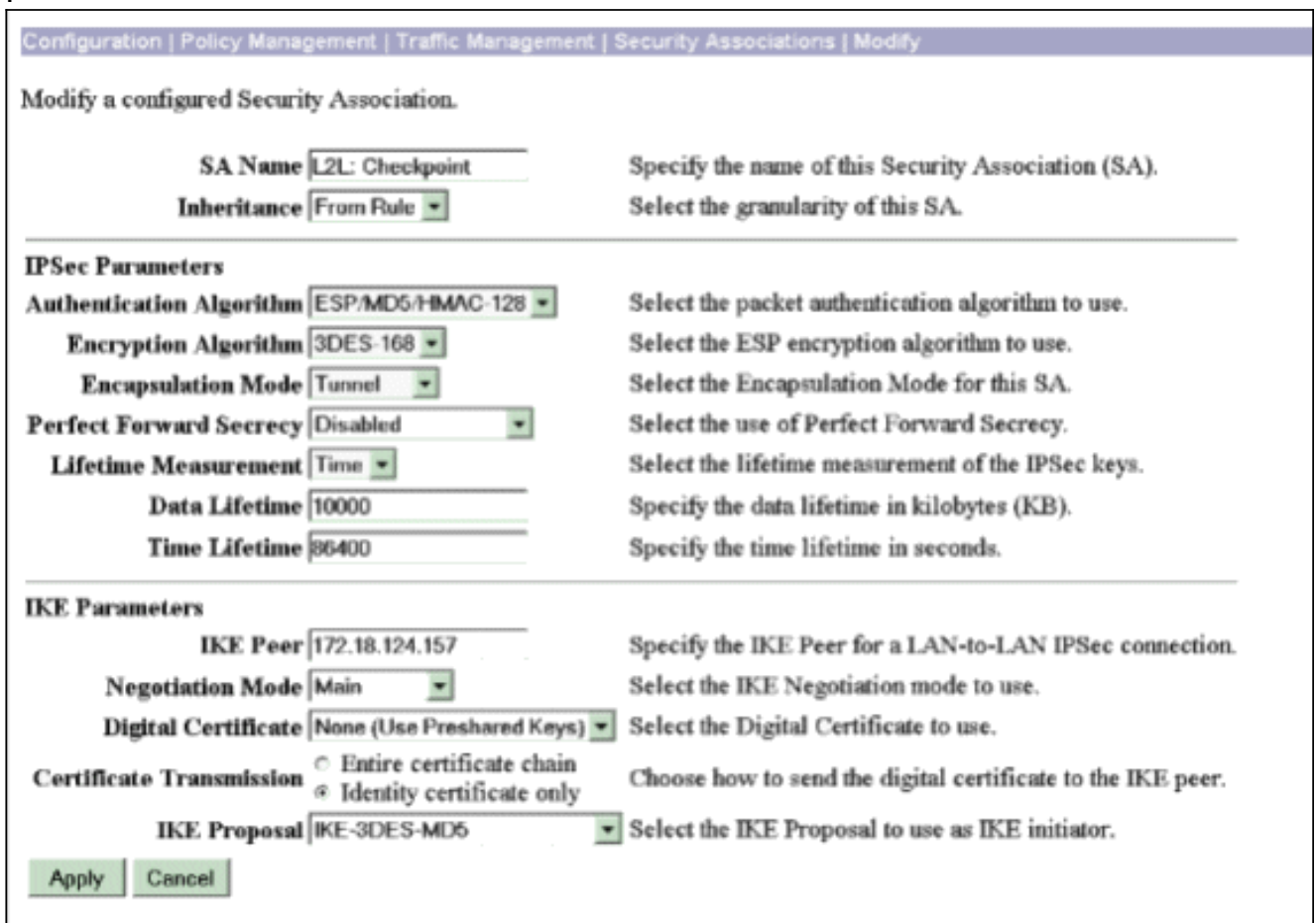
3. Accédez à **Configuration > Policy Management > Traffic Management > Security Associations**, sélectionnez l'association de sécurité IPSec créée pour la session et vérifiez les paramètres de l'association de sécurité IPSec sélectionnés pour la session LAN à LAN. Dans cette configuration, le nom de la session LAN à LAN était « Checkpoint », de sorte que la SA IPSec a été créée automatiquement en tant que « L2L : Point de contrôle.

»



Voici les paramètres de cette SA

:



[Configurer le contrôleur NG](#)

Les objets et les règles réseau sont définis sur le contrôleur NG afin de définir la stratégie relative à la configuration VPN à configurer. Cette stratégie est ensuite installée avec l'Éditeur de stratégie de GN Checkpoint pour compléter le côté GN Checkpoint de la configuration.

1. Créez les deux objets réseau pour le réseau Checkpoint NG et le réseau de concentrateur VPN qui chiffreront le trafic intéressant. afin de créer des objets, sélectionnez **Gérer > Objets réseau**, puis sélectionnez **Nouveau > Réseau**. Saisissez les informations réseau appropriées, puis cliquez sur OK. Ces exemples montrent la configuration d'objets réseau appelés CP_inside (le réseau interne du contrôleur NG) et CONC_INSIDE (le réseau interne 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

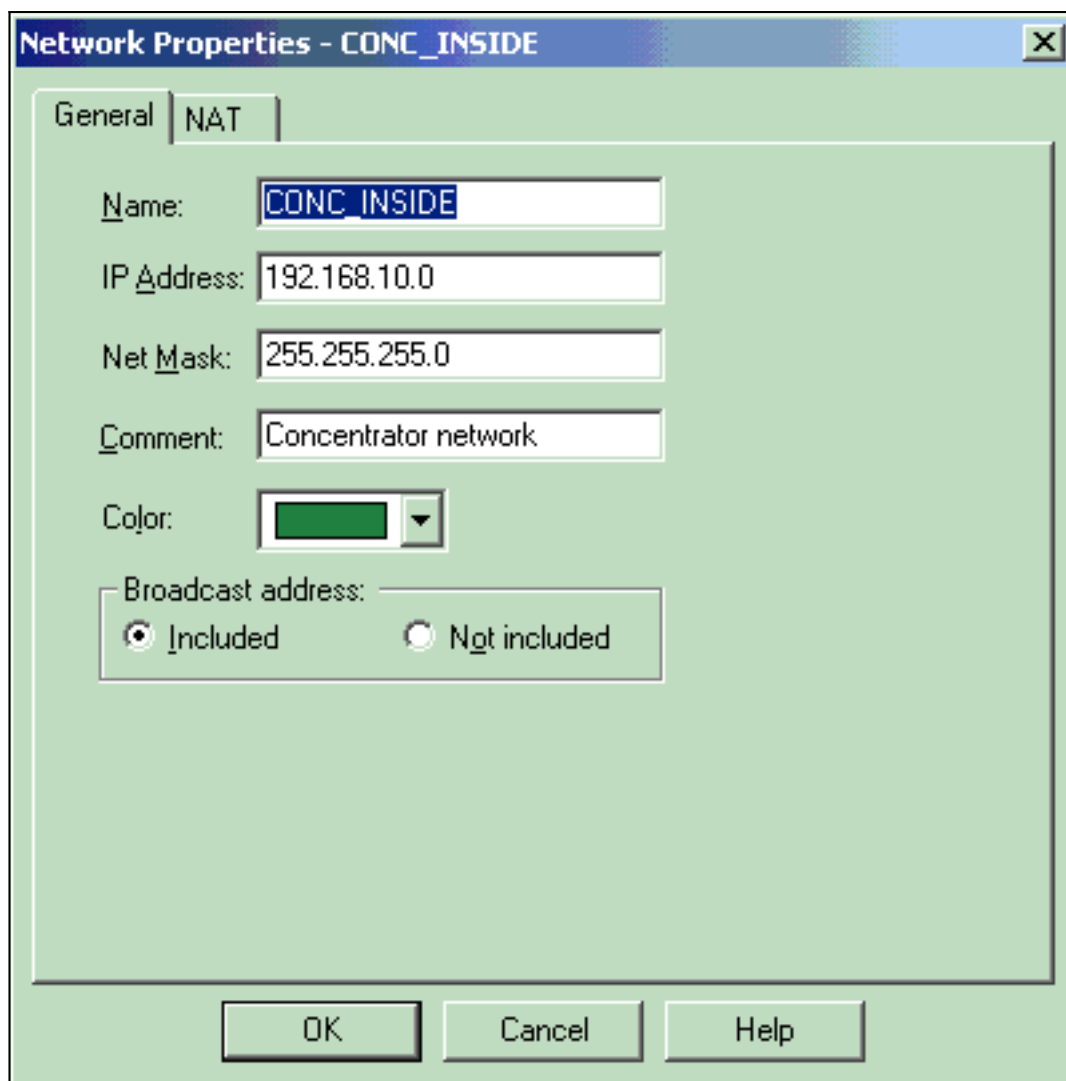
Color: [Blue]

Broadcast address:

Included Not included

OK Cancel Help

VPN).



2. Accédez à **Manage > Network Objects** et sélectionnez **New > Workstation** afin de créer des objets de station de travail pour les périphériques VPN, Checkpoint NG et le concentrateur VPN. **Remarque** : Vous pouvez utiliser l'objet de station de travail Checkpoint NG créé lors de la configuration initiale de Checkpoint NG. Sélectionnez les options pour définir la station de travail en tant que passerelle et périphérique VPN interopérable, puis cliquez sur **OK**. Ces exemples montrent la configuration d'objets appelés ciscocp (Checkpoint NG) et CISCO_CONC (concentrateur VPN 3000)

:

- General
- Topology
- NAT
- VPN
- Authentication
- Management
- Advanced

General

Name:

IP Address:

Comment:

Color:

Type: Host Gateway

Check Point Products _____

Check Point products installed: Version

- VPN-1 & FireWall-1
- FloodGate-1
- Policy Server
- Primary Management Station

Object Management _____

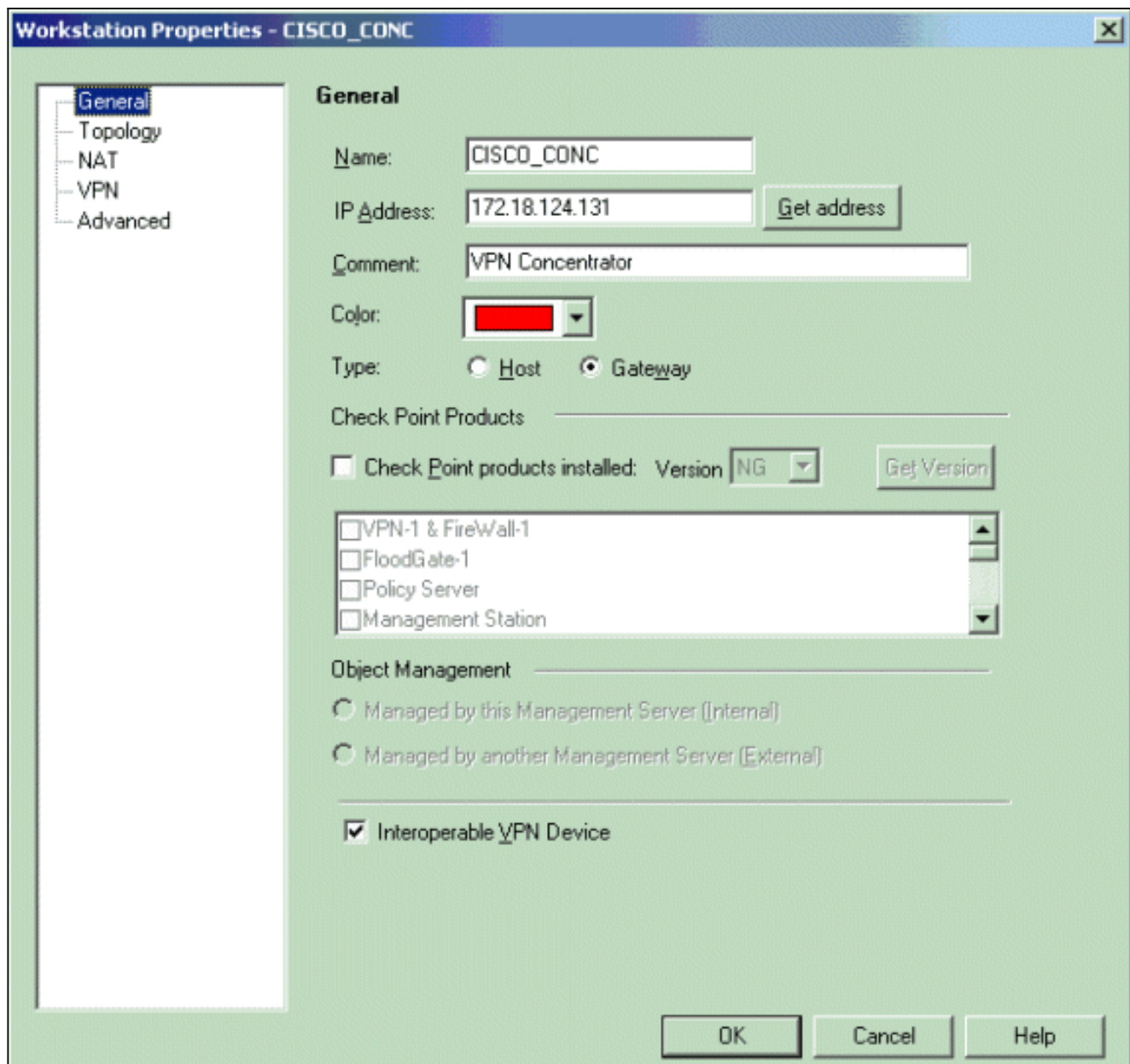
Managed by this Management Server (Internal)

Managed by another Management Server (External)

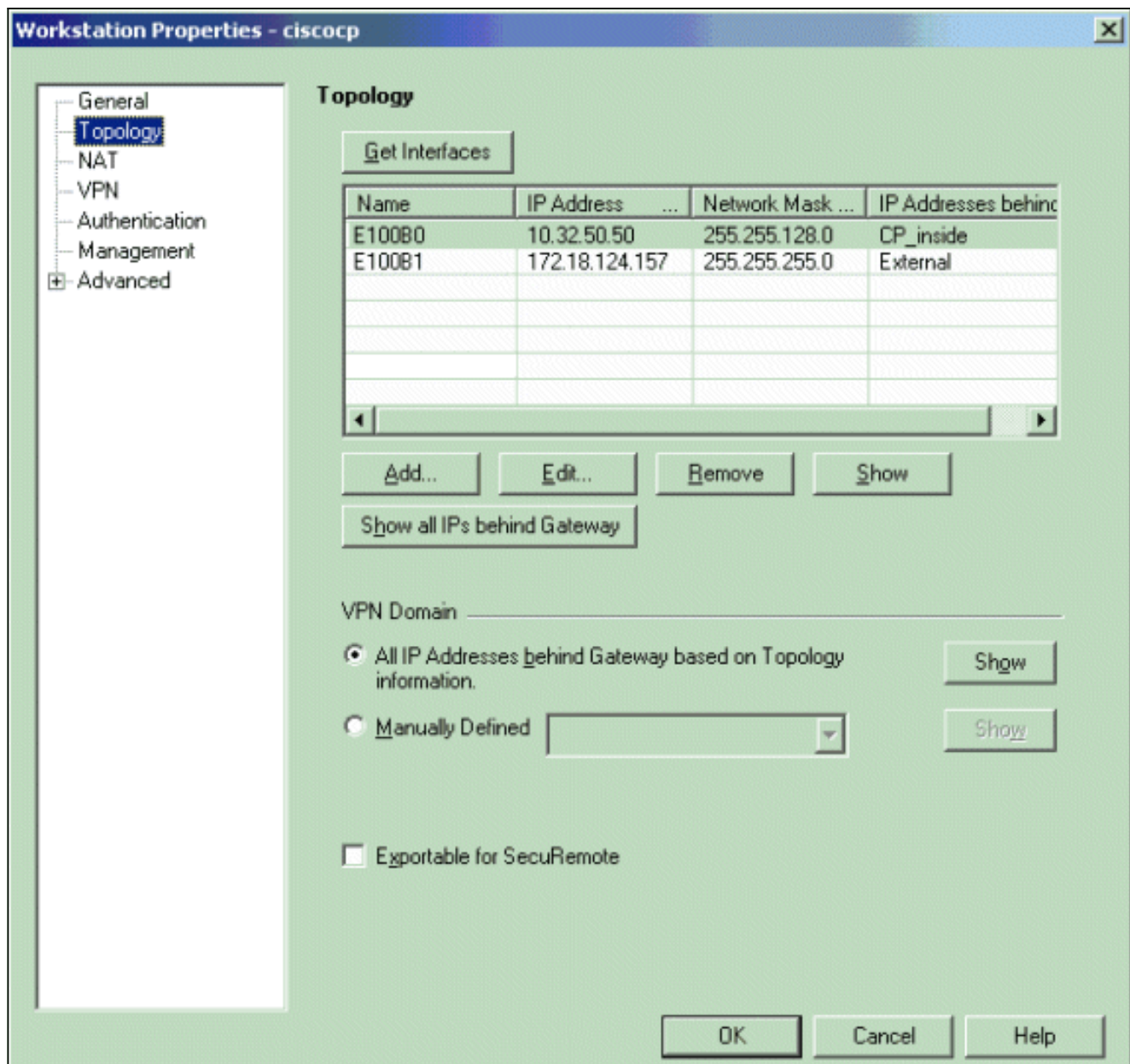
Secure Internal Communication _____

DN:

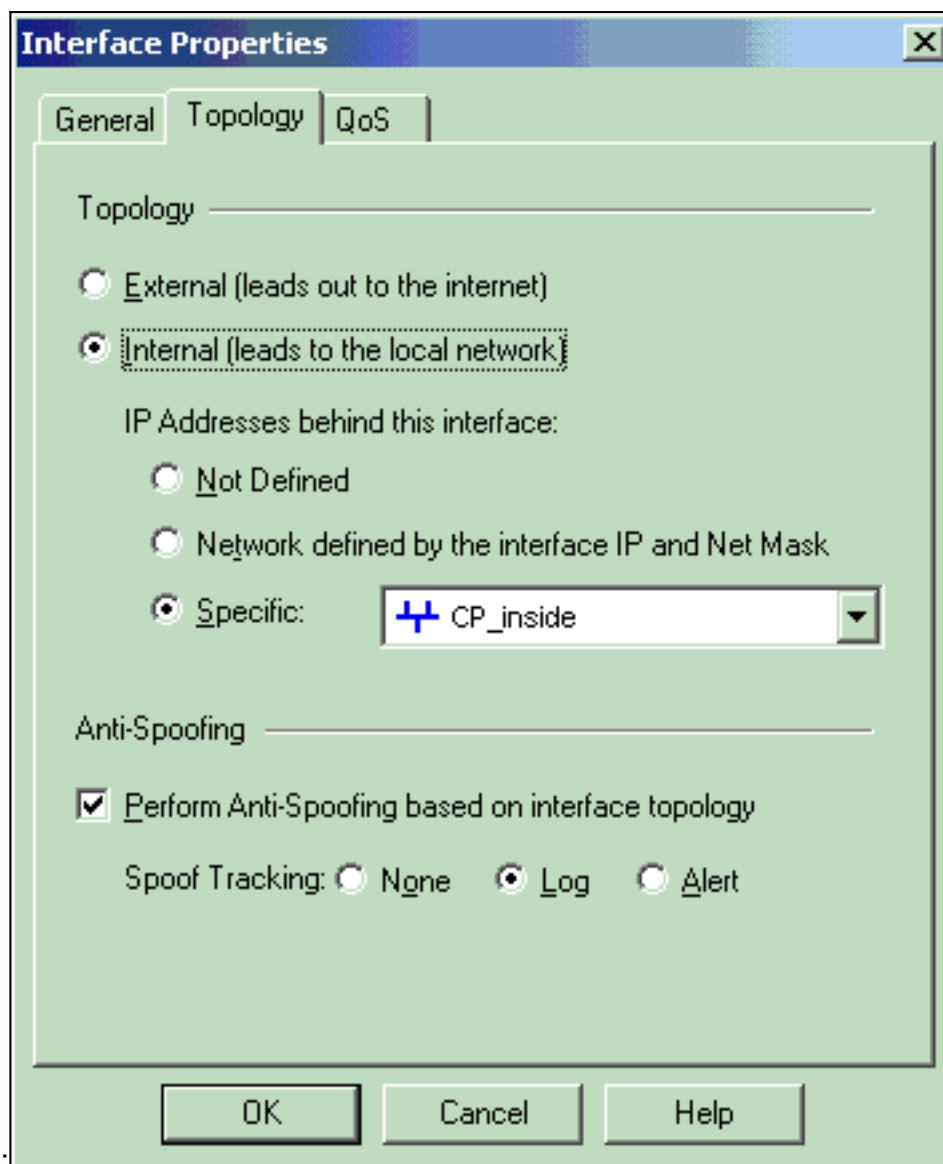
Interoperable VPN Device



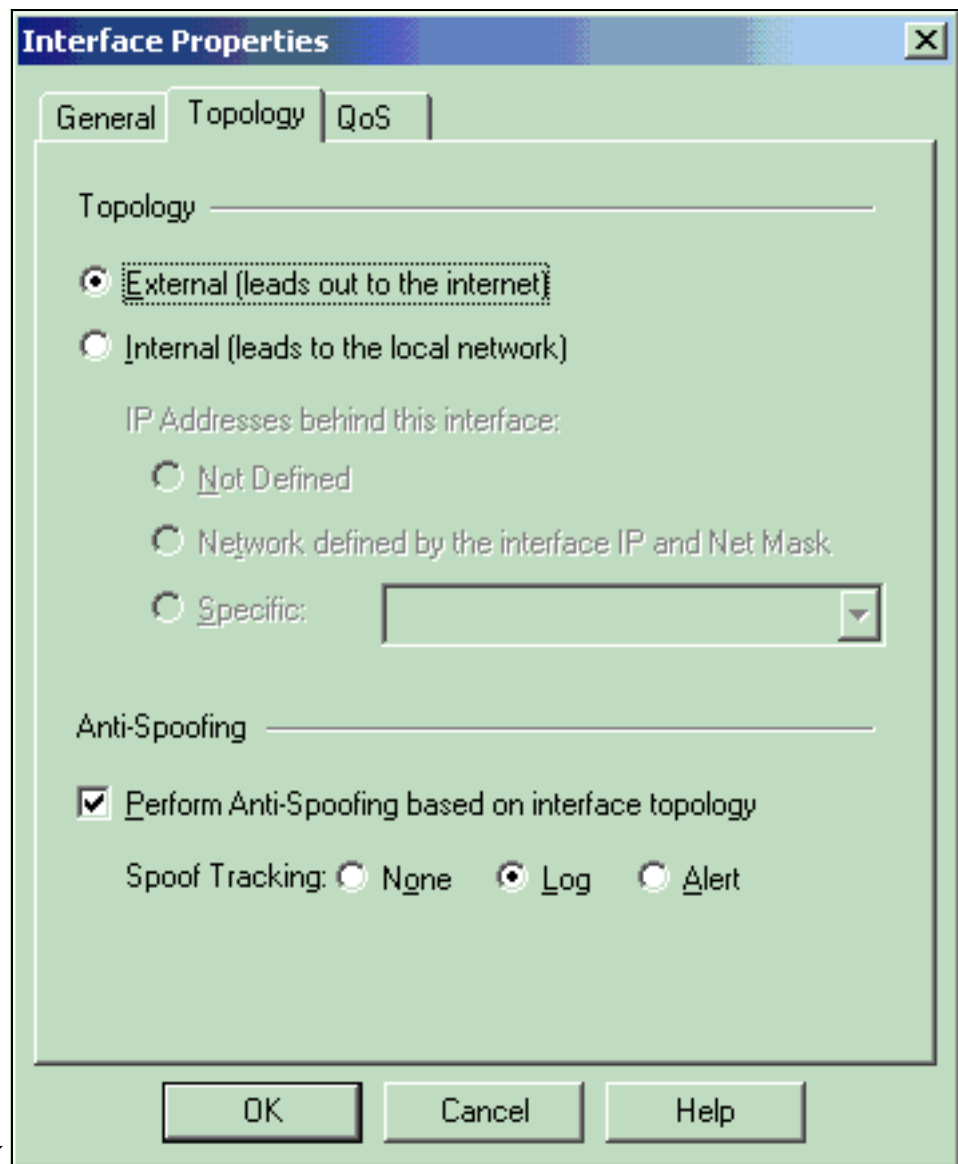
3. Accédez à **Manage > Network Objects > Edit** afin d'ouvrir la fenêtre Workstation Properties pour Checkpoint NG workstation (ciscocp dans cet exemple). Sélectionnez **Topologie** dans les choix situés à gauche de la fenêtre, puis sélectionnez le réseau à chiffrer. Cliquez sur **Edit** afin de définir les propriétés de l'interface. Dans cet exemple, CP_inside est le réseau interne du contrôleur NG.



4. Dans la fenêtre Propriétés de l'interface, sélectionnez l'option permettant de désigner la station de travail comme interne, puis spécifiez l'adresse IP appropriée. Click OK. Les sélections de topologie affichées désignent la station de travail comme interne et spécifient les adresses IP derrière l'interface CP_inside

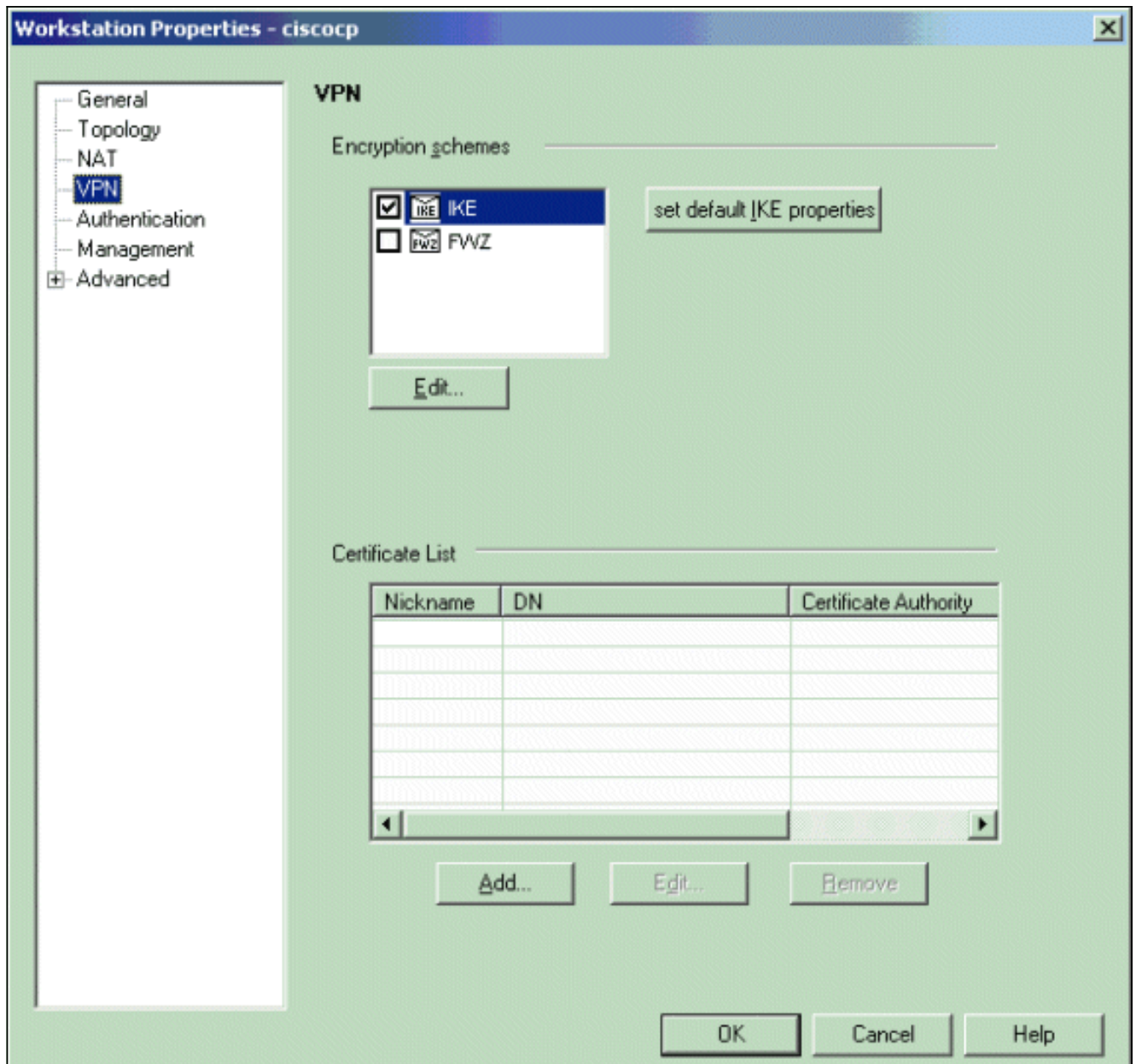


5. Dans la fenêtre Propriétés de la station de travail, sélectionnez l'interface externe sur l'indicateur Checkpoint NG qui mène à Internet, puis cliquez sur **Modifier** afin de définir les propriétés de l'interface. Sélectionnez l'option pour désigner la topologie comme externe,

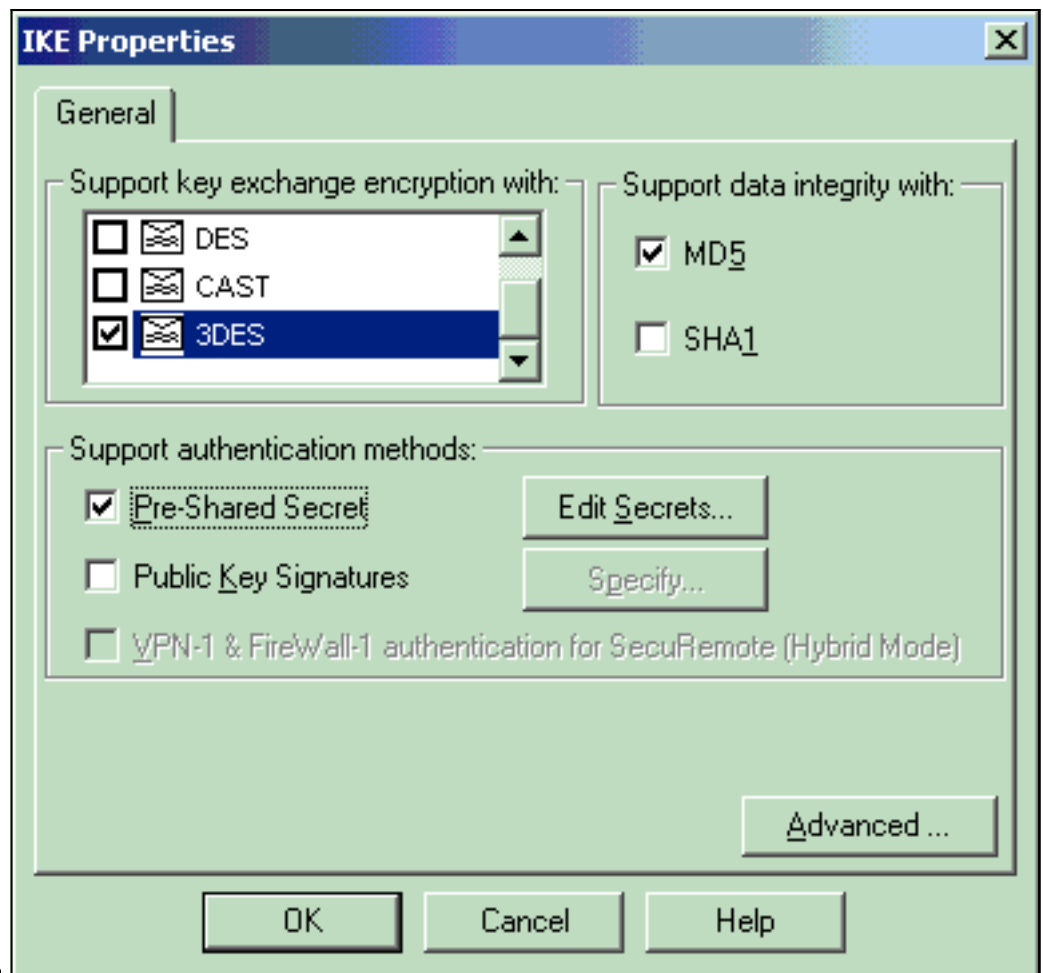


puis cliquez sur **OK**.

6. Dans la fenêtre Propriétés de la station de travail sur Checkpoint NG, sélectionnez **VPN** dans les choix à gauche de la fenêtre, puis sélectionnez les paramètres IKE pour les algorithmes de chiffrement et d'authentification. Cliquez sur **Edit** afin de configurer les propriétés IKE.

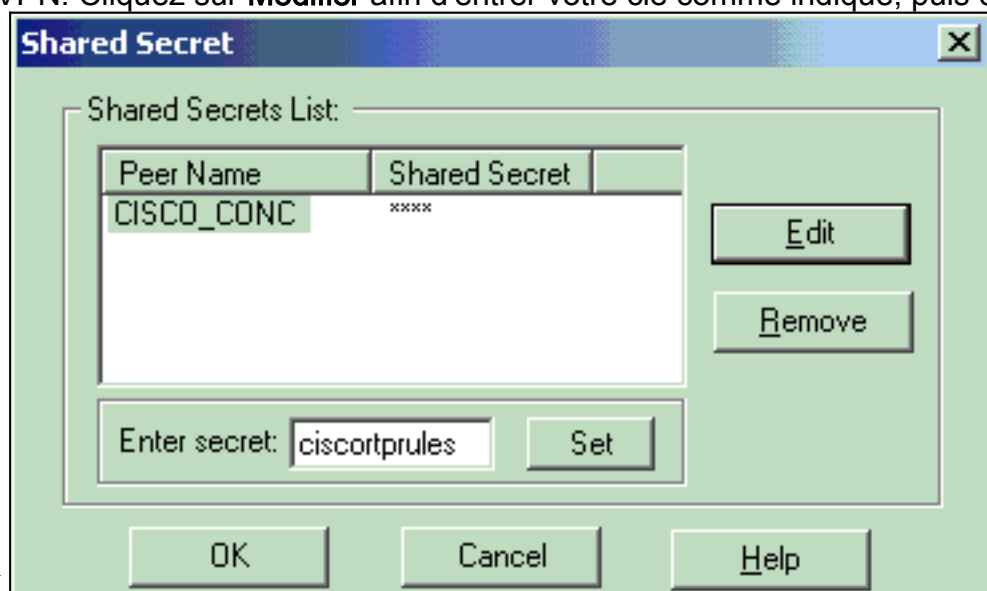


7. Définissez les propriétés IKE pour qu'elles correspondent aux propriétés du concentrateur VPN. Dans cet exemple, sélectionnez l'option de chiffrement pour **3DES** et l'option de



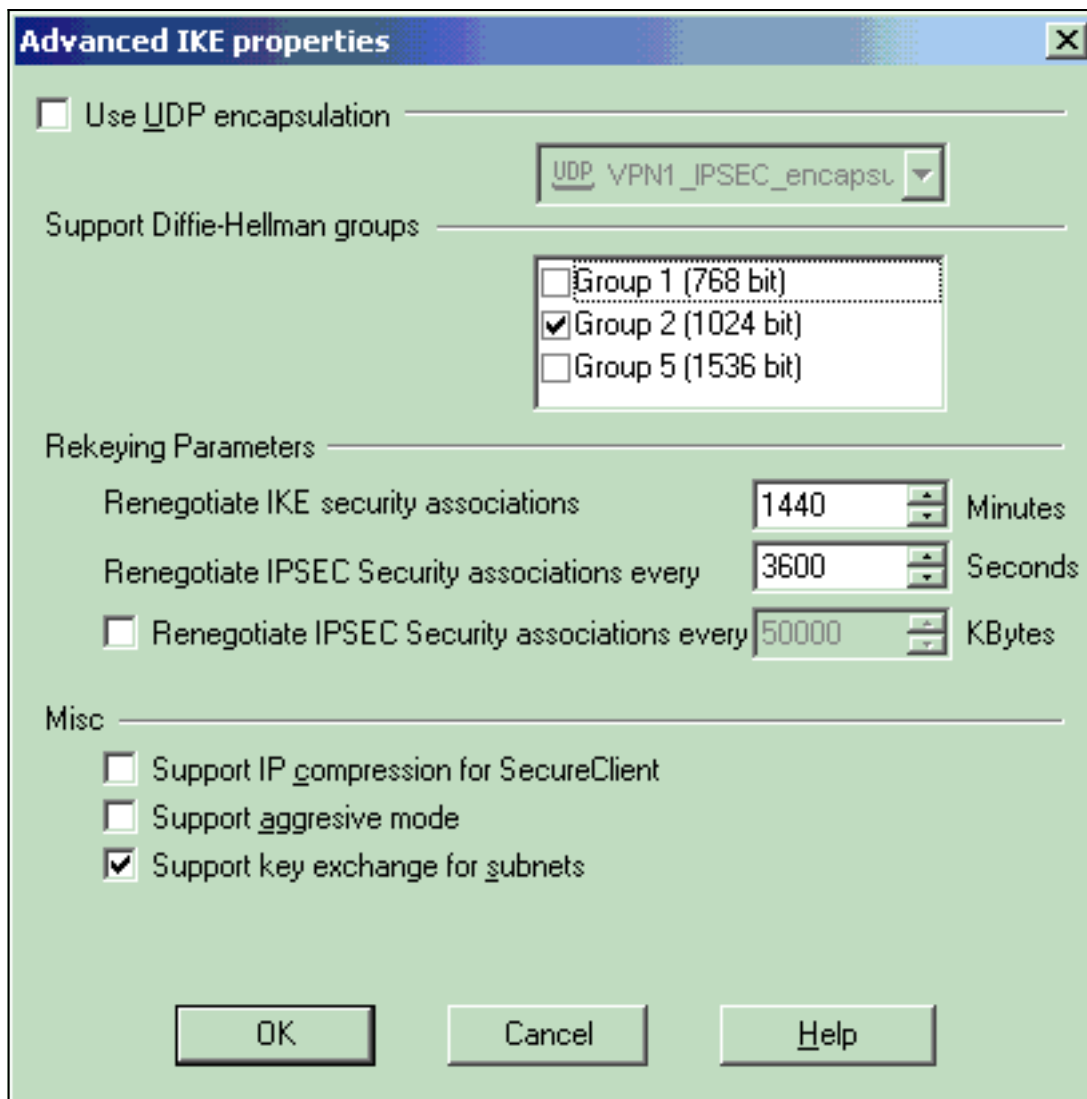
hachage pour MD5.

- Sélectionnez l'option d'authentification pour **Secrets pré-partagés**, puis cliquez sur **Modifier les secrets** pour définir la clé pré-partagée comme compatible avec la clé pré-partagée sur le concentrateur VPN. Cliquez sur **Modifier** afin d'entrer votre clé comme indiqué, puis cliquez



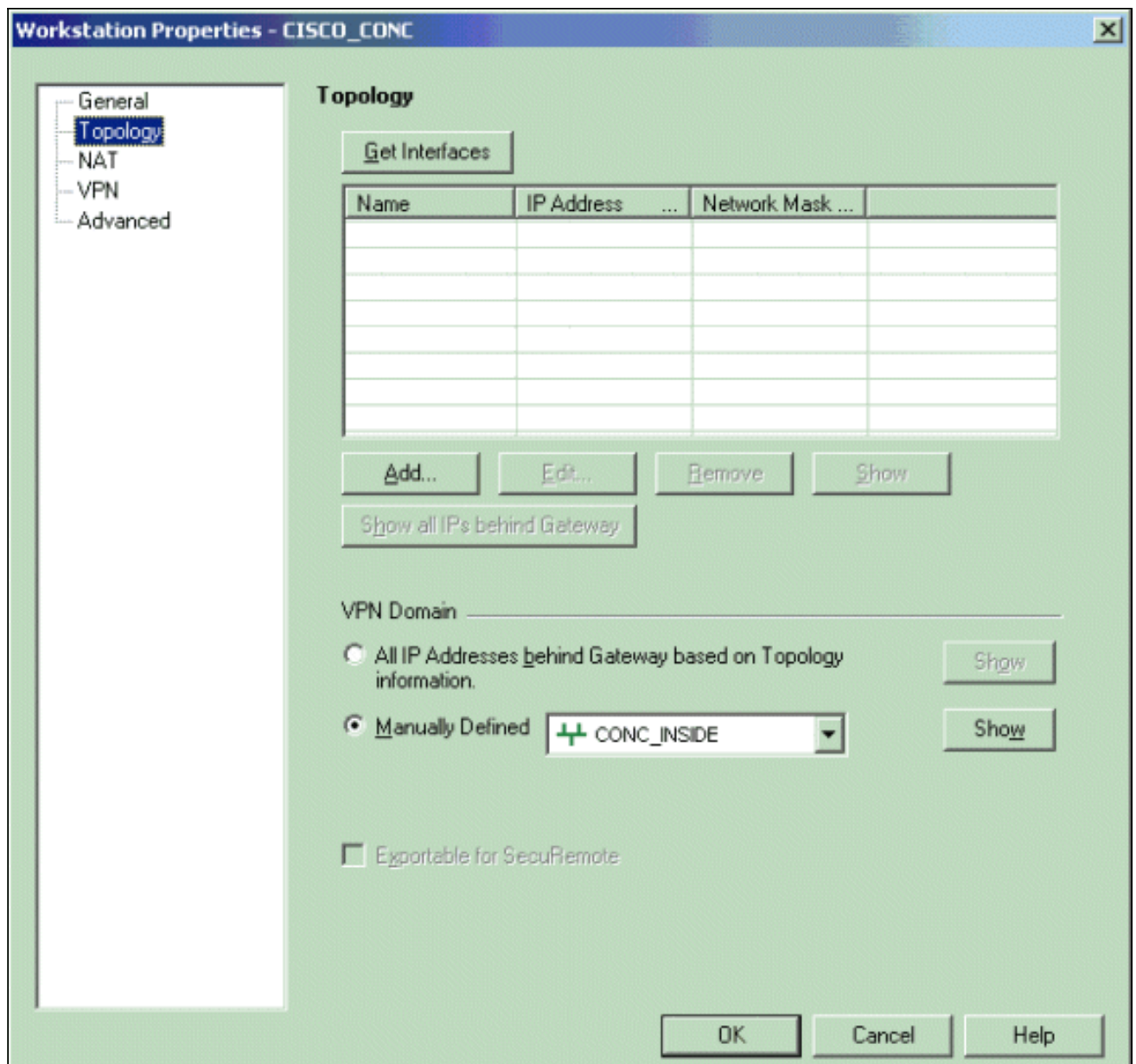
sur **Définir**, OK.

- Dans la fenêtre des propriétés IKE, cliquez sur **Avancé...** et modifiez ces paramètres : Désélectionnez l'option **Support agressif mode**. Sélectionnez l'option d'**échange de clés de support pour les sous-réseaux**. Lorsque vous avez terminé, cliquez sur **OK**,

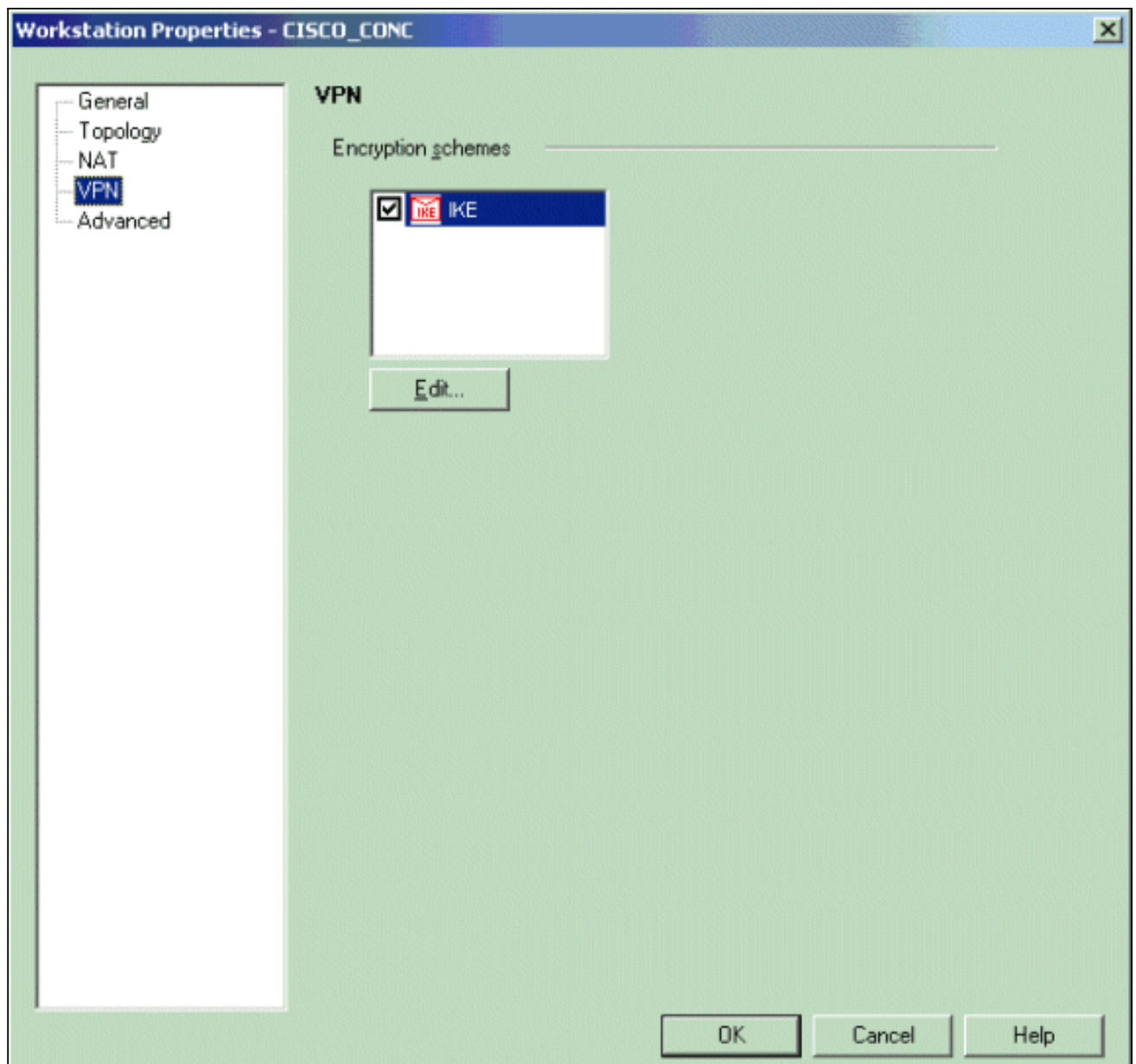


OK.

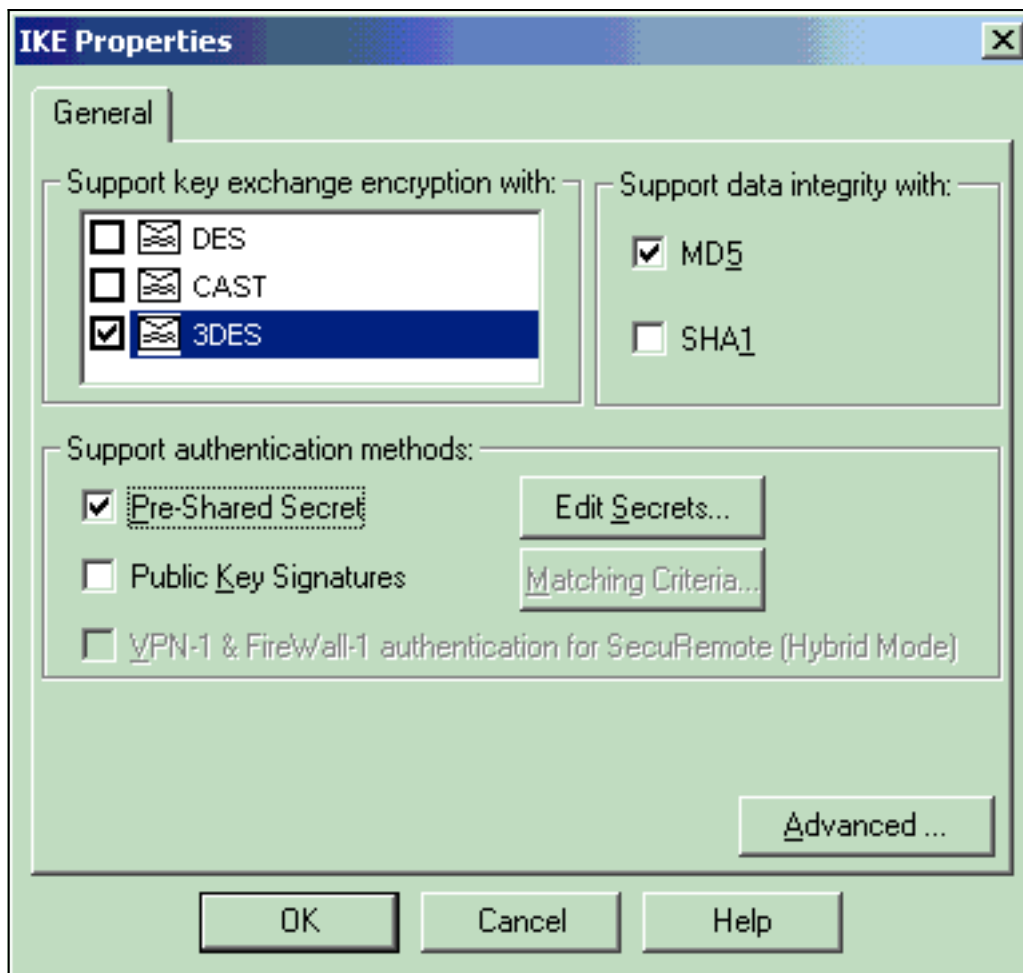
10. Accédez à **Manage > Network Objects > Edit** afin d'ouvrir la fenêtre Workstation Properties pour le concentrateur VPN. Sélectionnez **Topologie** dans les choix situés à gauche de la fenêtre afin de définir manuellement le domaine VPN. Dans cet exemple, CONC_INSIDE (le réseau interne du concentrateur VPN) est défini comme domaine VPN.



11. Sélectionnez **VPN** dans les choix situés à gauche de la fenêtre, puis sélectionnez **IKE** comme schéma de cryptage. Cliquez sur **Edit** afin de configurer les propriétés IKE.

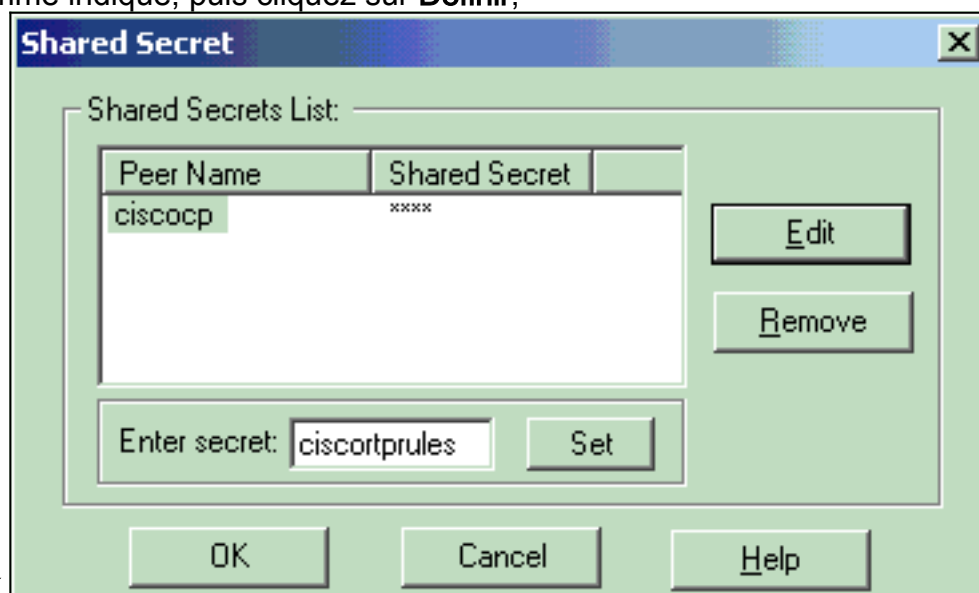


12. Définissez les propriétés IKE pour refléter la configuration actuelle sur le concentrateur VPN. Dans cet exemple, définissez l'option de chiffrement pour **3DES** et l'option de hachage



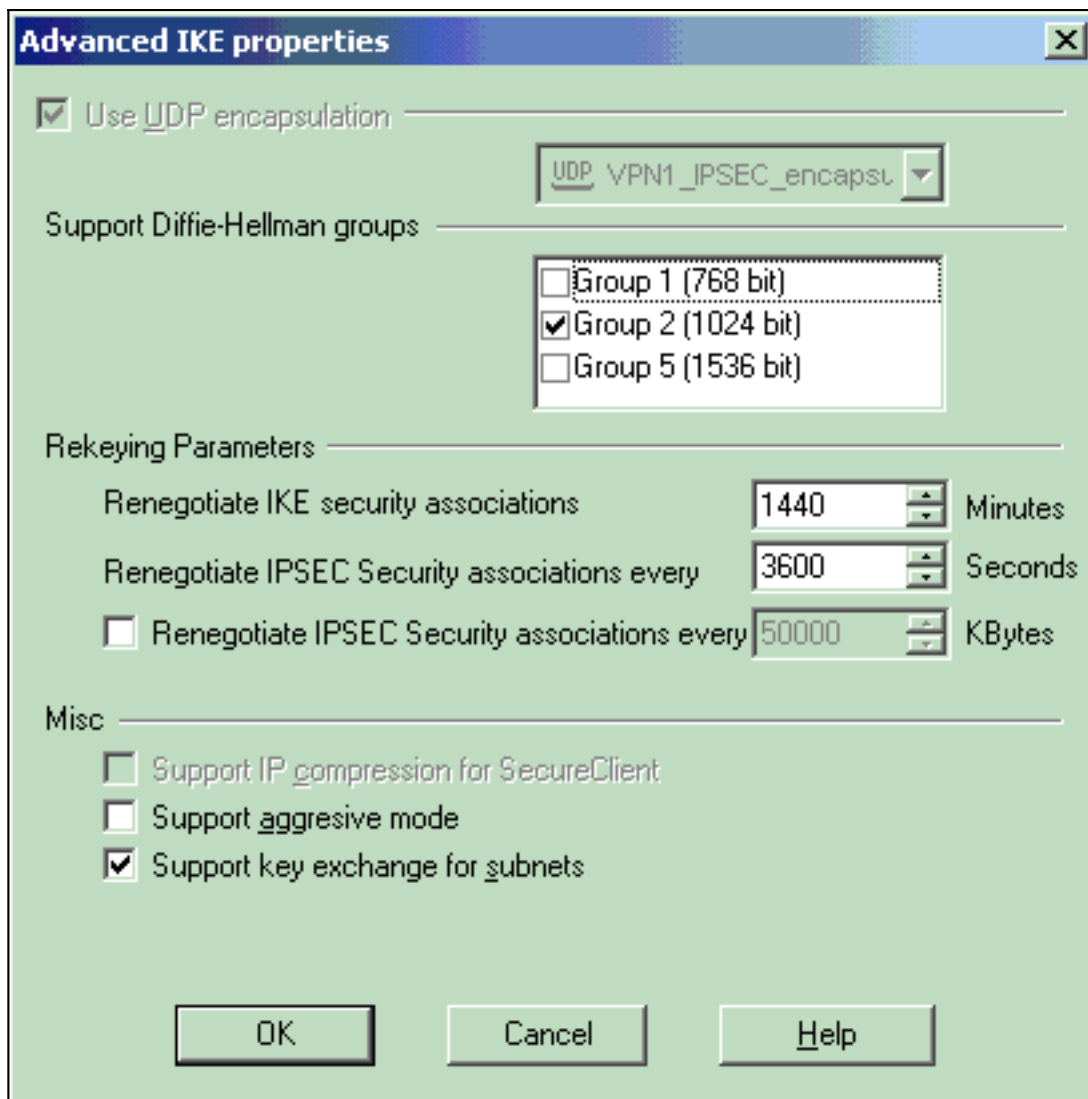
pour MD5.

13. Sélectionnez l'option d'authentification pour **Secrets pré-partagés**, puis cliquez sur **Modifier les secrets** afin de définir la clé pré-partagée. Cliquez sur **Modifier** afin d'entrer votre clé comme indiqué, puis cliquez sur **Définir**,



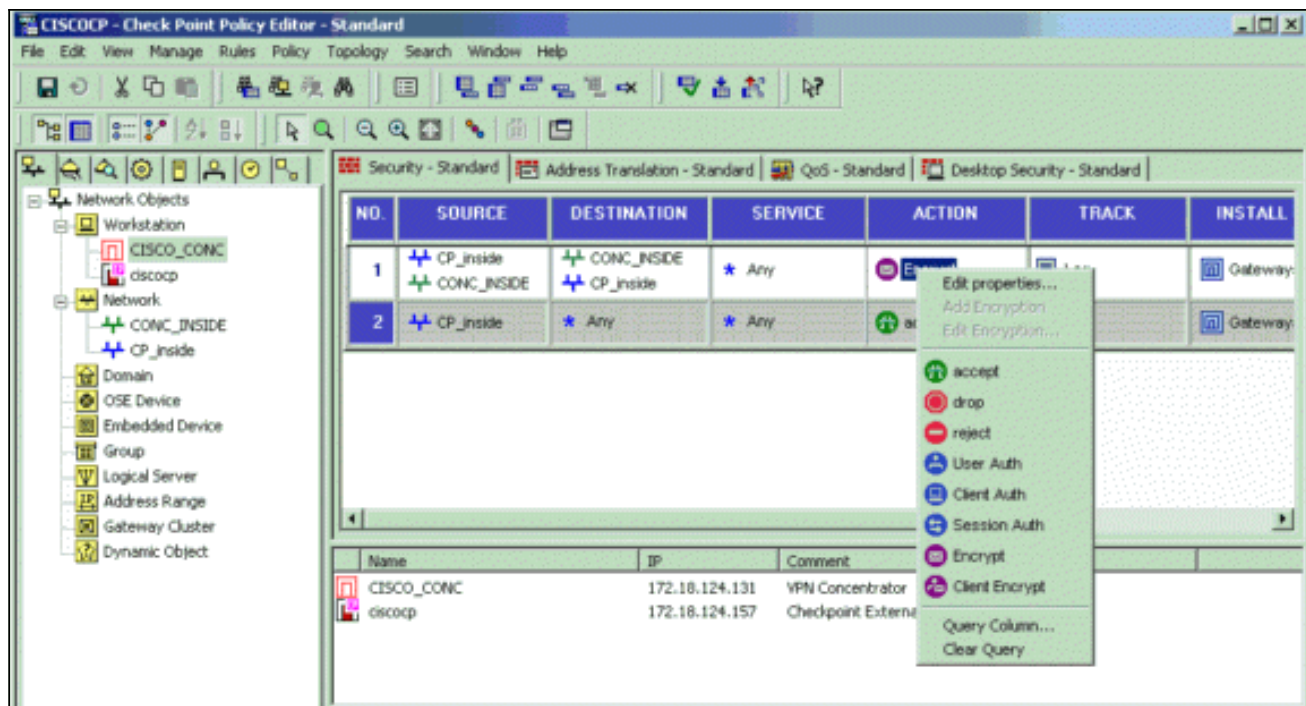
OK.

14. Dans la fenêtre des propriétés IKE, cliquez sur **Avancé...** et modifiez ces paramètres :Sélectionnez le groupe Diffie-Hellman approprié aux propriétés IKE.Désélectionnez l'option **Support agressif mode**.Sélectionnez l'option d'échange de clés de support pour les sous-réseaux.Lorsque vous avez terminé, cliquez sur **OK**,

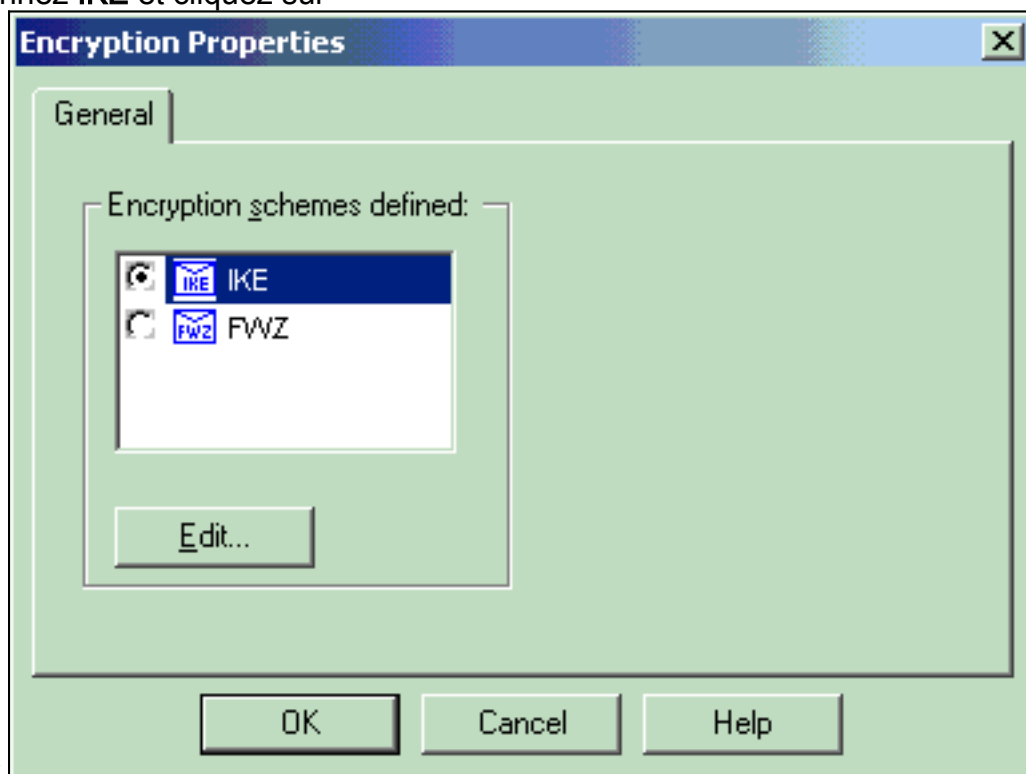


OK.

15. Sélectionnez **Règles > Ajouter des règles > Haut** afin de configurer les règles de chiffrement pour la stratégie. Dans la fenêtre Éditeur de stratégie, insérez une règle avec la source comme CP_inside (réseau interne du contrôleur NG) et la destination comme CONC_INSIDE (réseau interne du concentrateur VPN). Définissez des valeurs pour **Service = Any**, **Action = Encrypt** et **Track = Log**. Lorsque vous avez ajouté la section Action de chiffrement de la règle, cliquez avec le bouton droit sur **Action** et sélectionnez **Modifier les propriétés**.

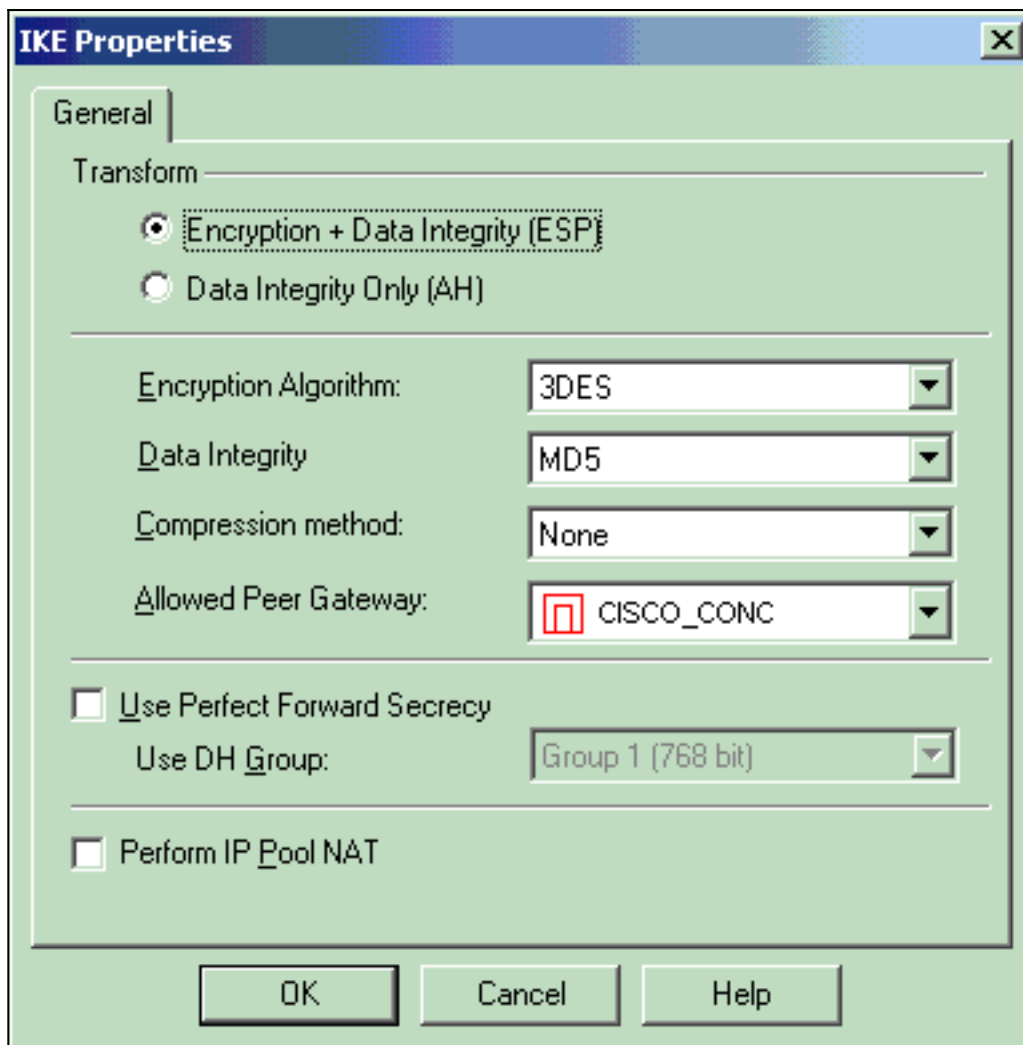


16. Sélectionnez **IKE** et cliquez sur



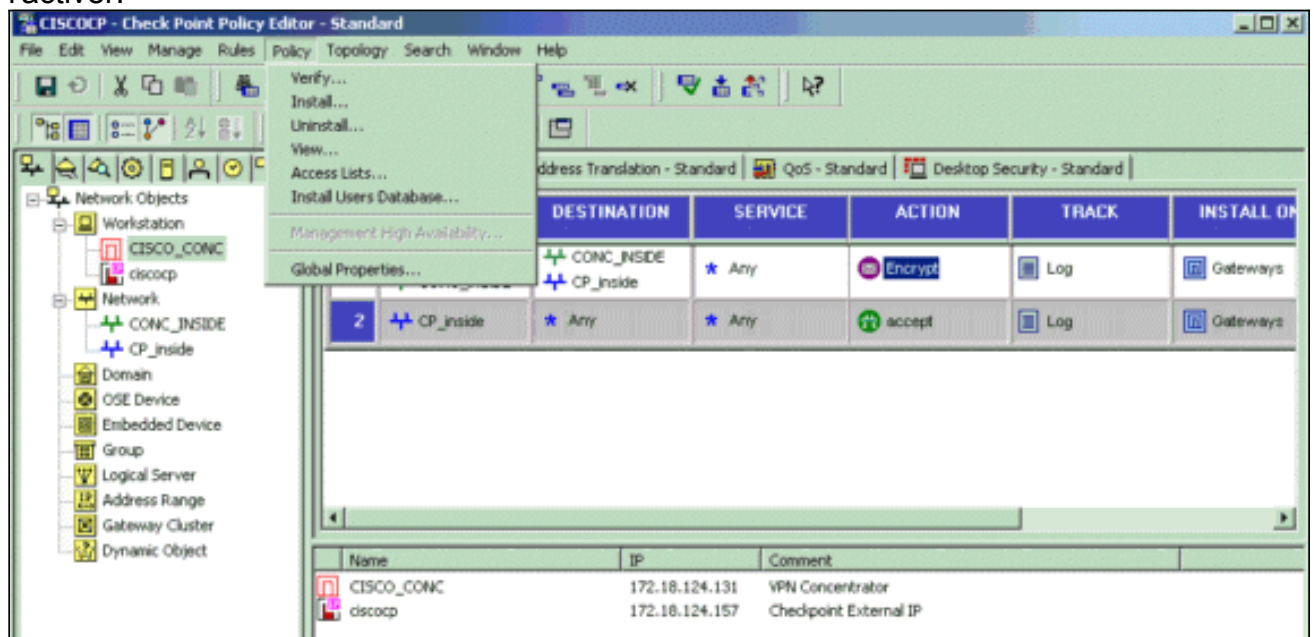
Modifier.

17. Dans la fenêtre Propriétés IKE, modifiez les propriétés pour les mettre en accord avec la transformation du concentrateur VPN. Définissez l'option Transform sur **Encryption + Data Integrity (ESP)**. Définissez l'algorithme de chiffrement sur **3DES**. Définissez l'intégrité des données sur **MD5**. Configurez la passerelle d'homologue autorisée pour qu'elle corresponde au concentrateur VPN (CISCO_CONC). Lorsque vous avez terminé, cliquez sur

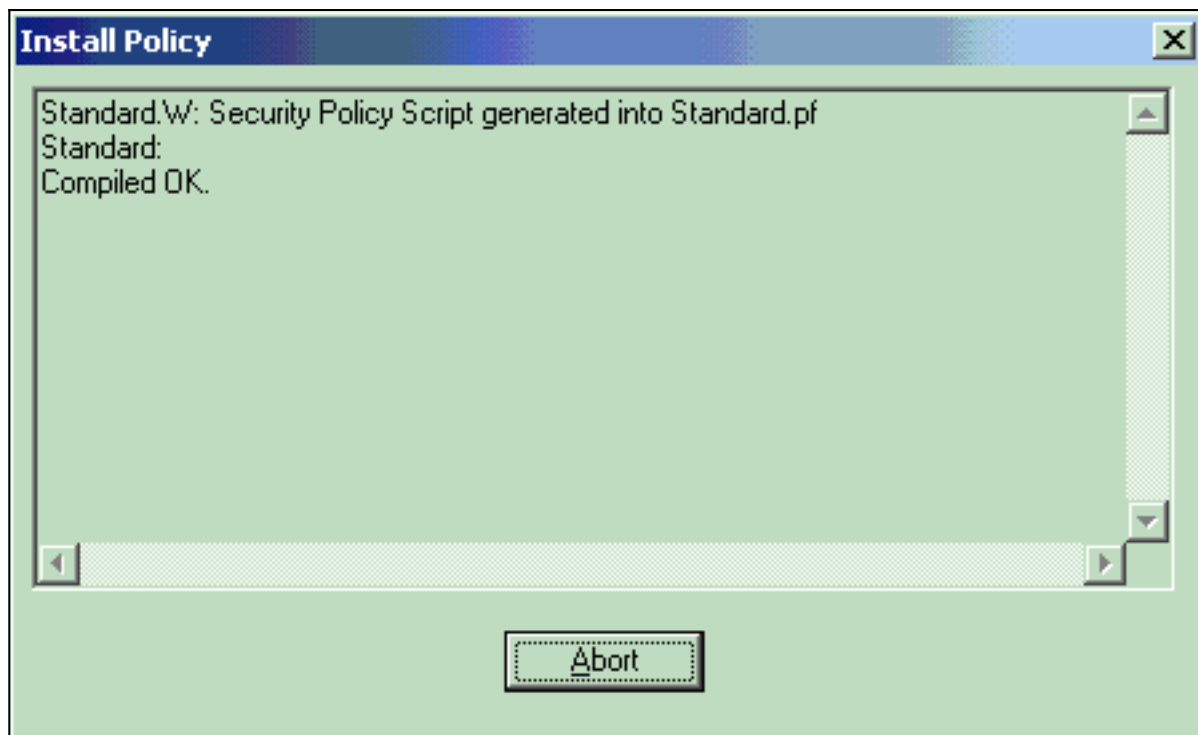


OK.

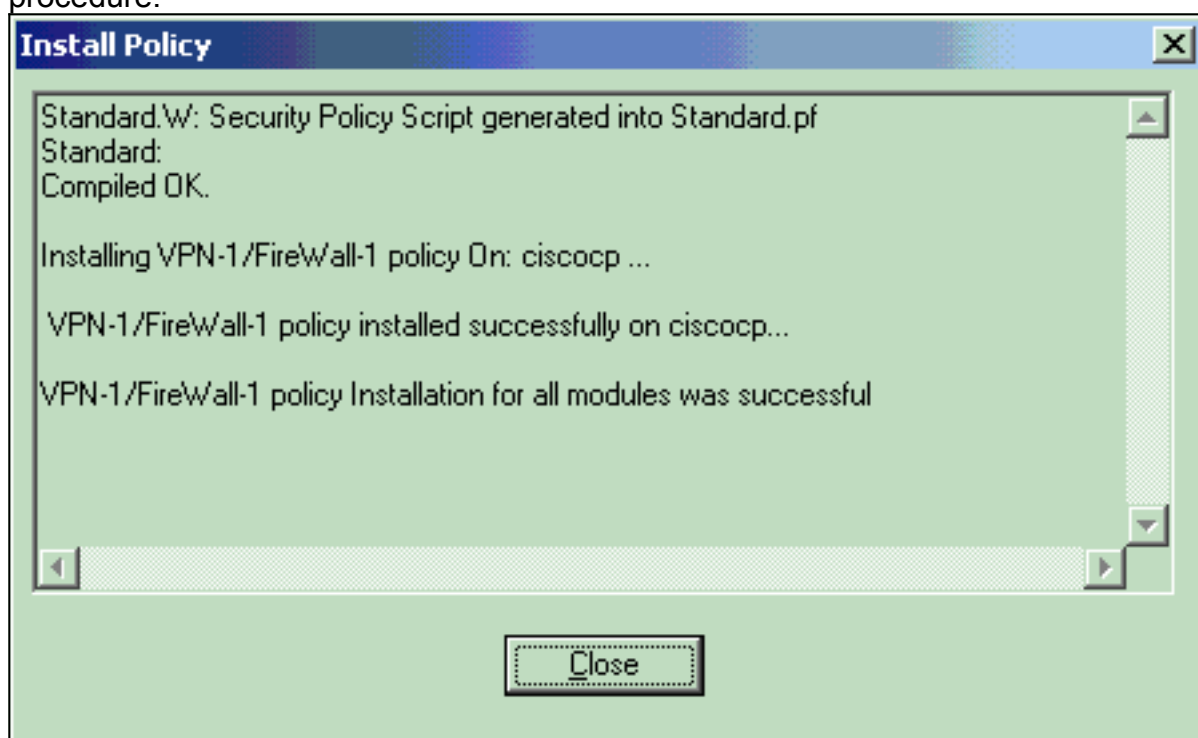
18. Une fois que Checkpoint NG est configuré, enregistrez la stratégie et sélectionnez **Policy > Install** afin de l'activer.



La fenêtre d'installation affiche les notes de progression lors de la compilation de la stratégie.



Lorsqu
e la fenêtre d'installation indique que l'installation de la stratégie est terminée, cliquez sur **Fermer** pour terminer la procédure.



Vérification

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

Vérification de la communication réseau

Afin de tester la communication entre les deux réseaux privés, vous pouvez lancer une requête ping de l'un des réseaux privés vers l'autre réseau privé. Dans cette configuration, une requête ping a été envoyée du côté de Checkpoint NG (10.32.50.51) au réseau du concentrateur VPN

(192.168.10.2).

```
C:\WINNT\System32\cmd.exe
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

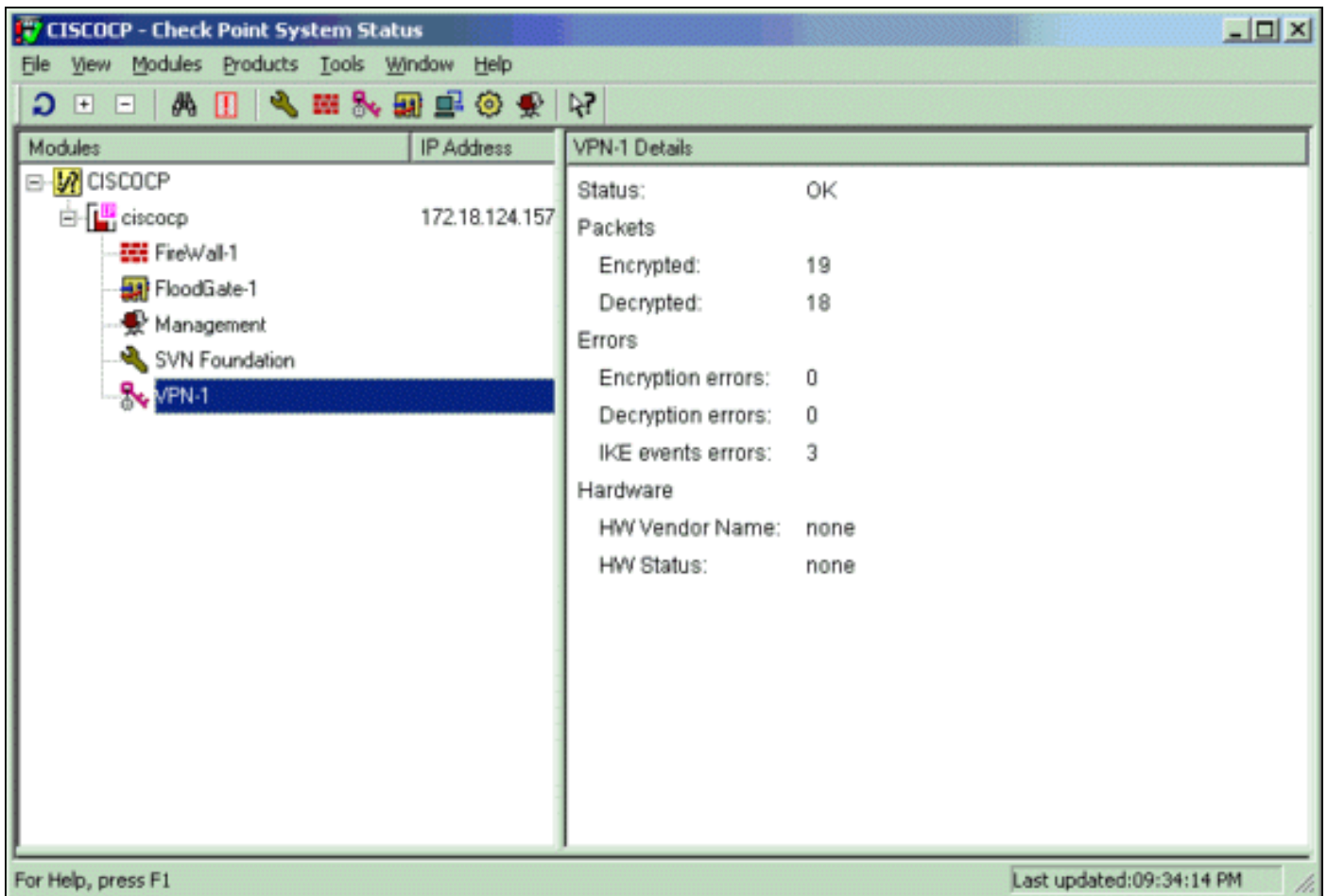
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time=10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253
Reply from 192.168.10.2: bytes=32 time<10ms TTL=253

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 5ms

C:\>
C:\>
C:\>
C:\>
```

[Afficher l'état du tunnel sur le contrôleur NG](#)

Pour afficher l'état du tunnel, accédez à l'Éditeur de stratégie et sélectionnez **Fenêtre > État du système**.



[Afficher l'état du tunnel sur le concentrateur VPN](#)

Afin de vérifier l'état du tunnel sur le concentrateur VPN, accédez à **Administration > Administrer Sessions**.

Administration | Administer Sessions Wednesday, 11 September 2002 20:37:01
Reset Refresh

This screen shows statistics for sessions. To refresh the statistics, click **Refresh**. Select a **Group** to filter the sessions. For more information on a session, click on that session's name. To log out a session, click **Logout** in the table below. To test the network connection to a session, click **Ping**.

Group:

Logout All: [PPTP User](#) | [L2TP User](#) | [IPSec User](#) | [L2TP/IPSec User](#) | [IPSec/UDP User](#) | [IPSec/TCP User](#) | [IPSec LAN-to-LAN](#)

Session Summary

Active LAN-to-LAN Sessions	Active Remote Access Sessions	Active Management Sessions	Total Active Sessions	Peak Concurrent Sessions	Concurrent Sessions Limit	Total Cumulative Sessions
1	0	3	4	4	1500	17

LAN-to-LAN Sessions [[Remote Access Sessions](#) | [Management Sessions](#)]

Connection Name	IP Address	Protocol	Encryption	Login Time	Duration	Actions
Checkpoint	172.18.124.157	IPSec/LAN-to-LAN	3DES-168	Sep 11 20:36:03	0:00:57	[Logout Ping]

Sous Sessions LAN à LAN, sélectionnez le nom de connexion du point de contrôle pour afficher les détails sur les SA créées et le nombre de paquets transmis/reçus.

[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

Dépannage

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

Remarque : le trafic ne doit pas être PATed sur le tunnel IPSec à l'aide de l'adresse IP publique du concentrateur VPN (interface externe). Sinon, le tunnel échoue. Ainsi, l'adresse IP utilisée pour PATing doit être une adresse autre que l'adresse configurée sur l'interface externe.

Récapitulation de réseau

Lorsque plusieurs réseaux internes adjacents sont configurés dans le domaine de chiffrement sur le point de contrôle, le périphérique peut automatiquement résumer les réseaux en fonction du trafic intéressant. Si le concentrateur VPN n'est pas configuré pour correspondre, le tunnel risque d'échouer. Par exemple, si les réseaux internes 10.0.0.0 /24 et 10.0.1.0 /24 sont configurés pour être inclus dans le tunnel, ces réseaux peuvent être résumés sur 10.0.0.0 /23.

Débogues pour Checkpoint NG

Pour afficher les journaux, sélectionnez **Fenêtre > Visionneuse de journaux**.

..	Date	Time	Product	Inter.	Orig..	Type	Action	Source	Destinati..	Pr..	Rule	S_Port	SrcKeyID	DstKeyID
1	13Aug2002	21:32	VPN-1 & FireV...	dae...	cisco	log	key install	cisco	CISCO_CONC					
2	13Aug2002	21:32	VPN-1 & FireV...	dae...	cisco	log	key install	cisco	CISCO_CONC				0x5879f30d	0xf1351129

Débogues pour le concentrateur VPN

Afin d'activer les débogages sur le concentrateur VPN, accédez à **Configuration > System > Events > Classes**. Activez AUTH, AUTHDBG, IKE, IKEDBG, IPSEC et IPSECDBG pour la gravité à enregistrer en tant que 1 - 13. Afin d'afficher les débogages, sélectionnez **Monitoring > Filterable Event Log**.

```
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 constructing 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: FilterIpssecAddIkeSa 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](#)