Configuration d'un tunnel IPsec – entre un concentrateur Cisco VPN 5000 et un pare-feu Checkpoint 4.1

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Configurez
Diagramme du réseau
Configurations
Pare-feu Checkpoint 4.1
Vérifiez
Dépannez
Commandes de dépannage du concentrateur VPN 5000
Récapitulation de réseau
Debug de pare-feu Checkpoint 4.1
Exemple de sortie de débogage
Informations connexes

Introduction

Ce document explique comment former un tunnel d'IPsec avec des clés pré-partagées pour joindre deux réseaux privés. Il joint un réseau privé à l'intérieur du concentrateur de Cisco VPN 5000 (192.168.1.x) à un réseau privé à l'intérieur du pare-feu Checkpoint 4.1 (10.32.50.x). On le suppose que le trafic de l'intérieur du concentrateur et de l'intérieur VPN que le point de reprise à l'Internet (représenté dans ce document par les réseaux 172.18.124.x) circule avant que vous commenciez cette configuration.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur Cisco VPN 5000
- Version 5.2.19.0001 de logiciel du concentrateur de Cisco VPN 5000
- Pare-feu Checkpoint 4.1

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.

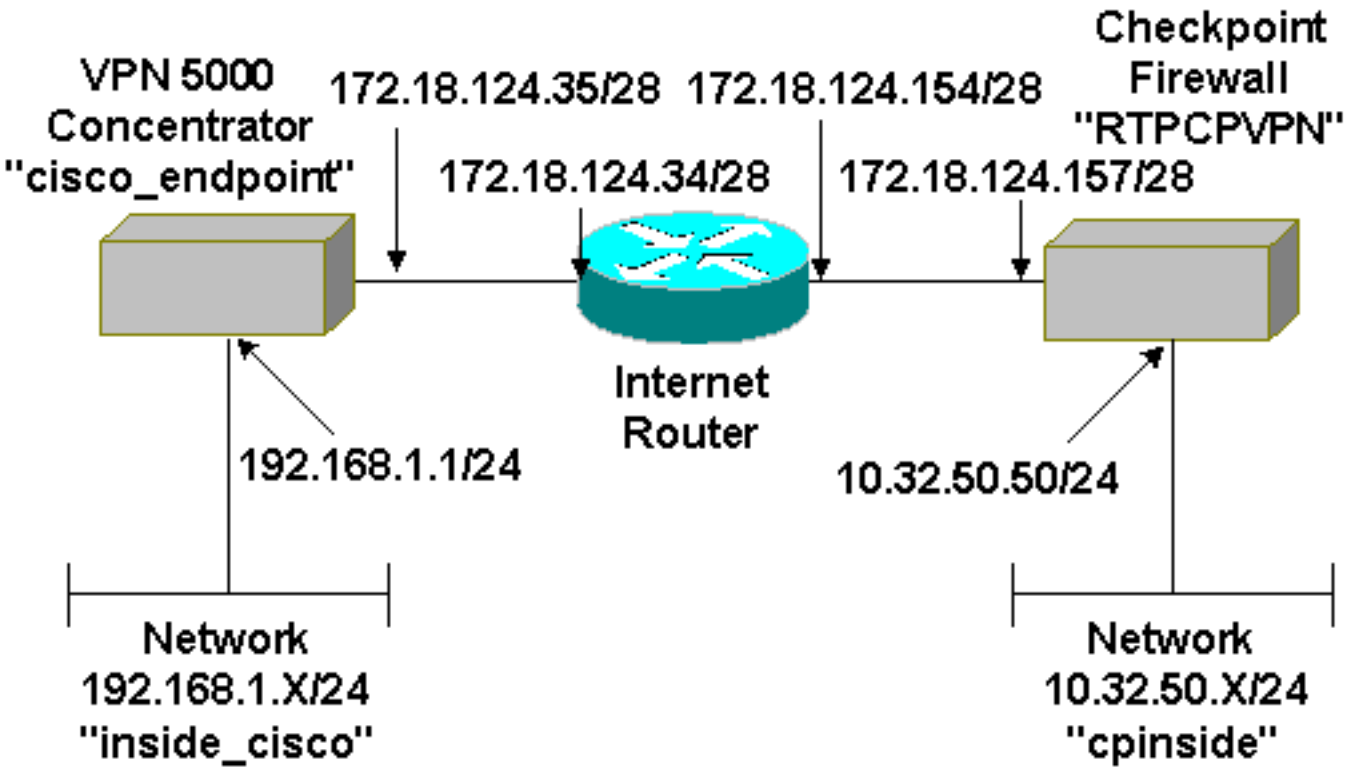
Configurez

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

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour trouver plus d'informations sur les commandes utilisées dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise cette configuration.

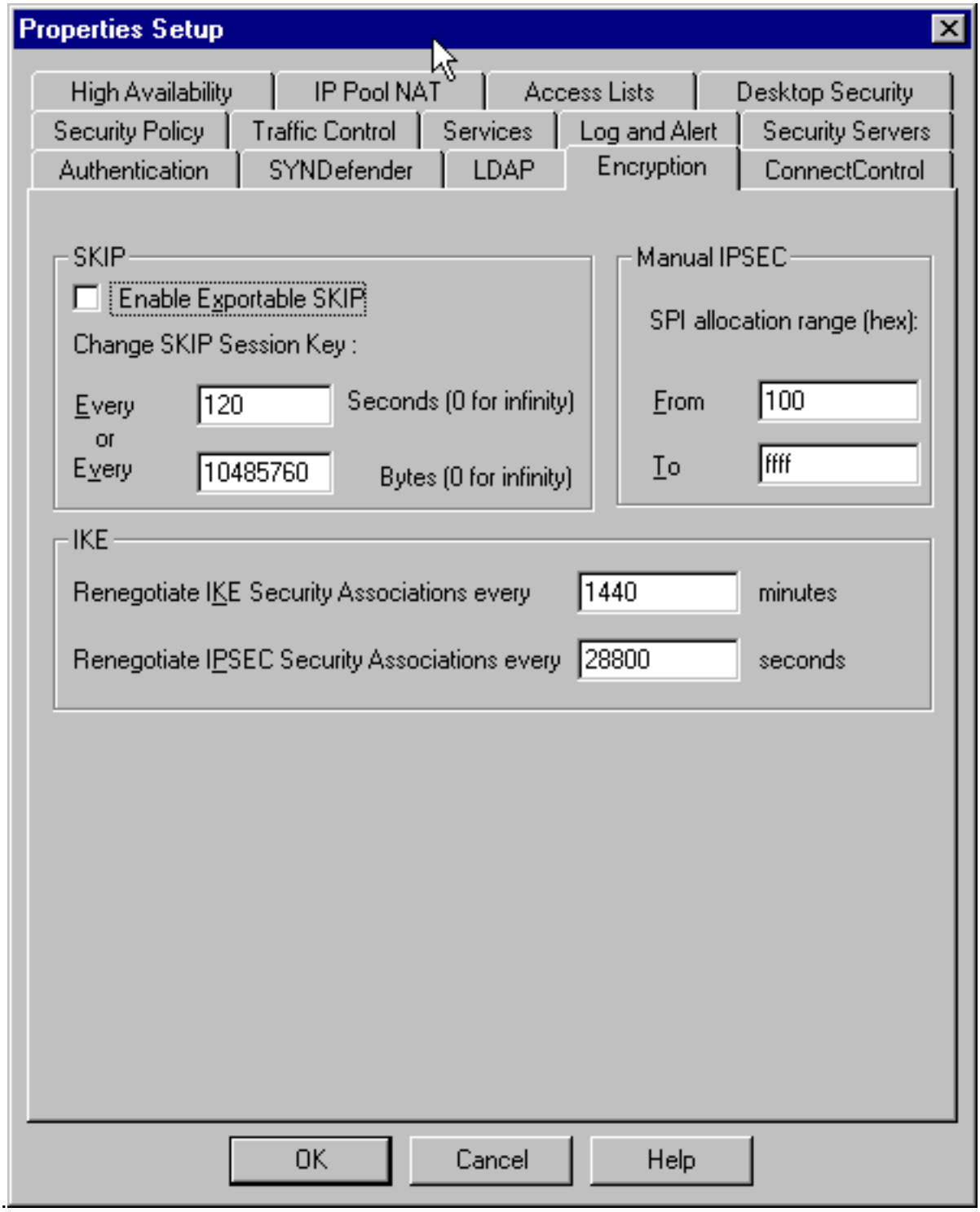
Concentrateur Cisco VPN 5000

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 192.168.1.1

[ General ]
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console
DeviceName              = "cisco_endpoint"
IPSecGateway            = 172.18.124.34

[ IKE Policy ]
Protection              = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs             = 28800
LocalAccess             = "192.168.1.0/24"
Peer                    = "10.32.50.0/24"
BindTo                  = "ethernet 1:0"
SharedKey               = "ciscorules"
KeyManage               = Auto
Transform               = esp(sha,des)
Partner                 = 172.18.124.157
Mode                    = Main

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IP Ethernet 1:0 ]
IPAddress               = 172.18.124.35
SubnetMask              = 255.255.255.240
Mode                    = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Pare-feu Checkpoint 4.1

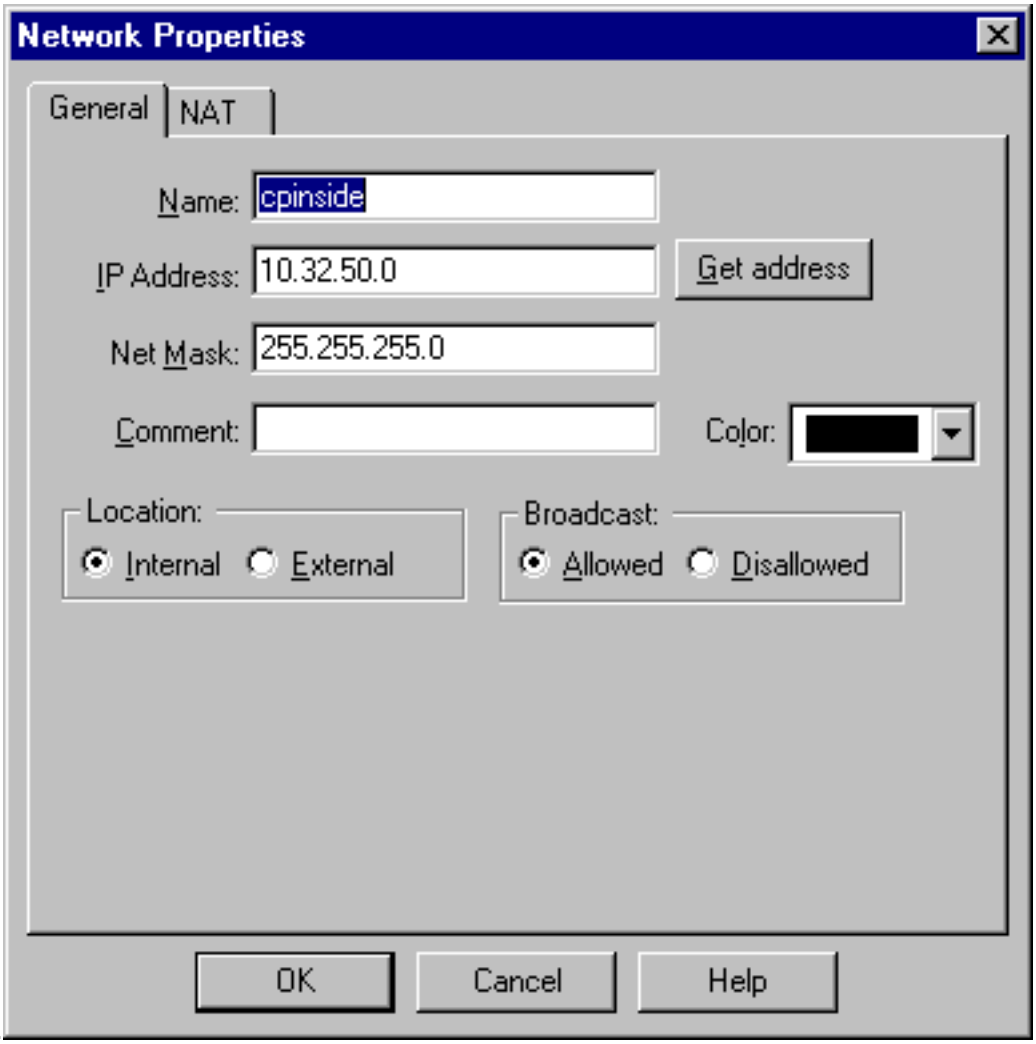
Terminez-vous ces étapes pour configurer le pare-feu Checkpoint 4.1.

1. **Properties** choisi **> cryptage** pour placer les vies d'IPsec de point de reprise pour être d'accord avec le **KeyLifeSecs =** commande de concentrateur de **28800** VPN.**Note**: Laissez les vies d'Échange de clés Internet (IKE) de point de reprise au par



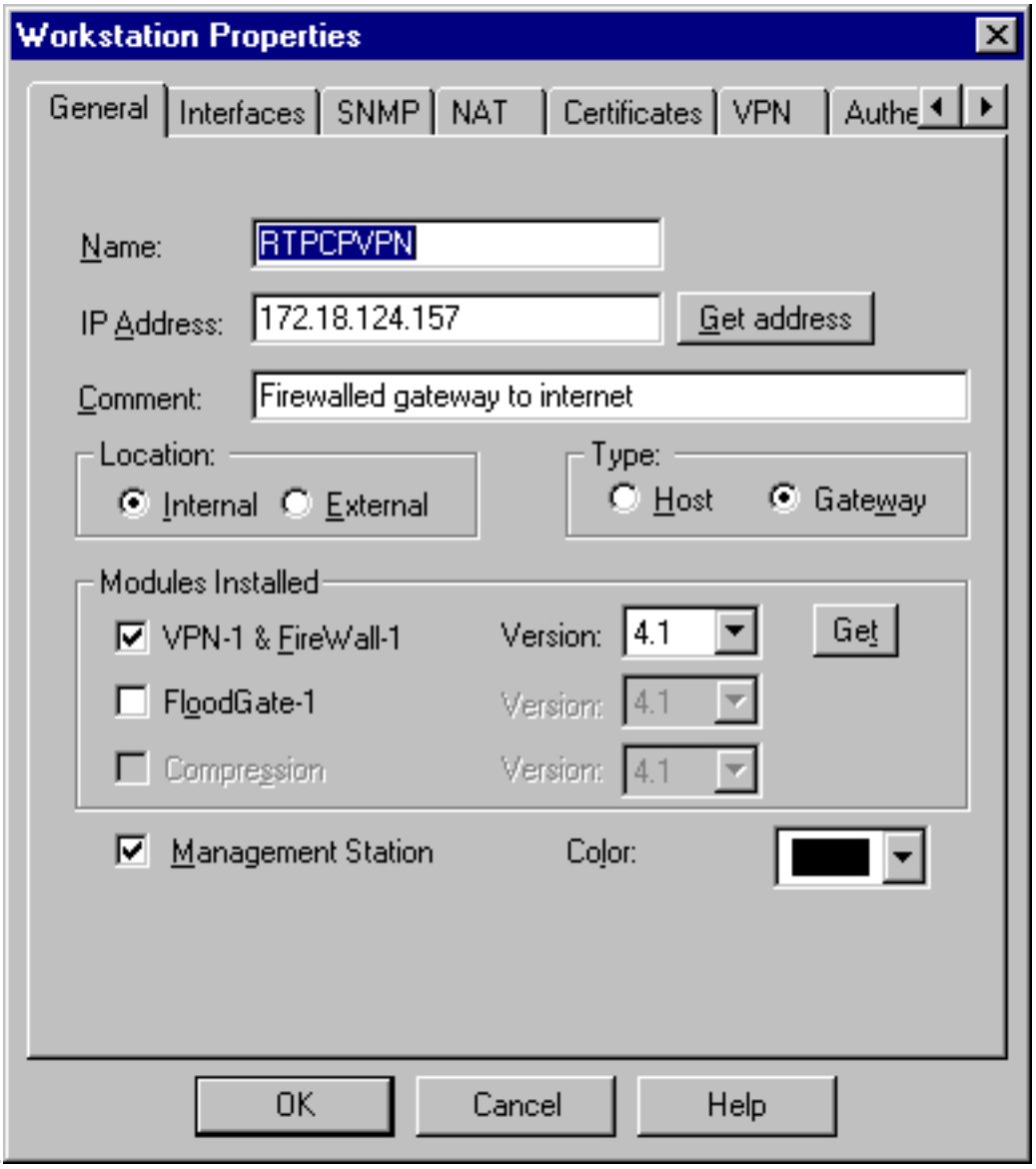
défaut.

2. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour (« cpinside ») le réseau interne derrière le point de reprise. Ceci devrait être conforme au **pair =** commande de concentrateur de **"10.32.50.0/24"**



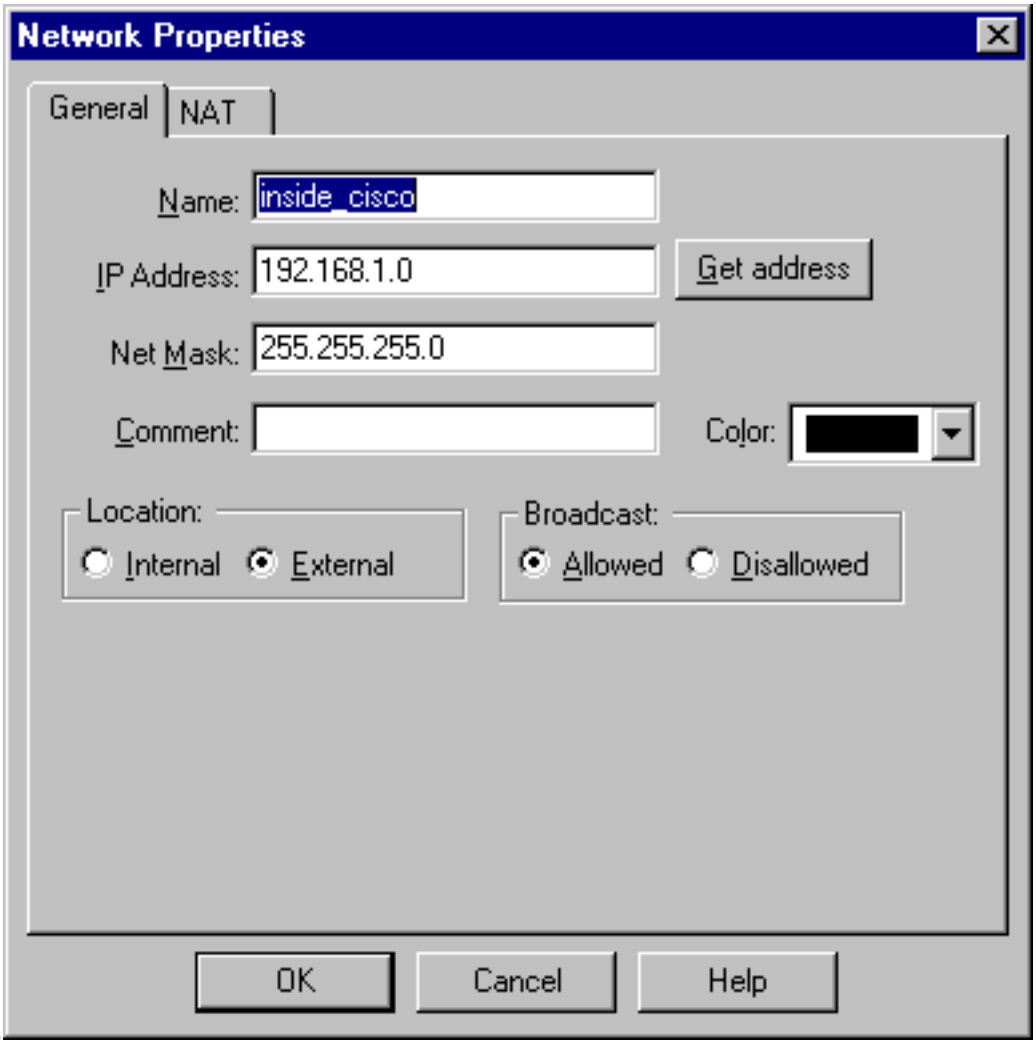
VPN.

3. Choisi **gérez > des objets de réseau > éditent** pour éditer l'objet pour point final de passerelle (point de reprise le « RTPCPVPN ») ce les points de concentrateur VPN à dans la commande de **partenaire = de <ip>**.Emplacement de dessous **interne** choisi.**Passerelle** choisie pour le type.Contrôle **VPN-1 et FireWall-1** et **station de Gestion** sous des modules



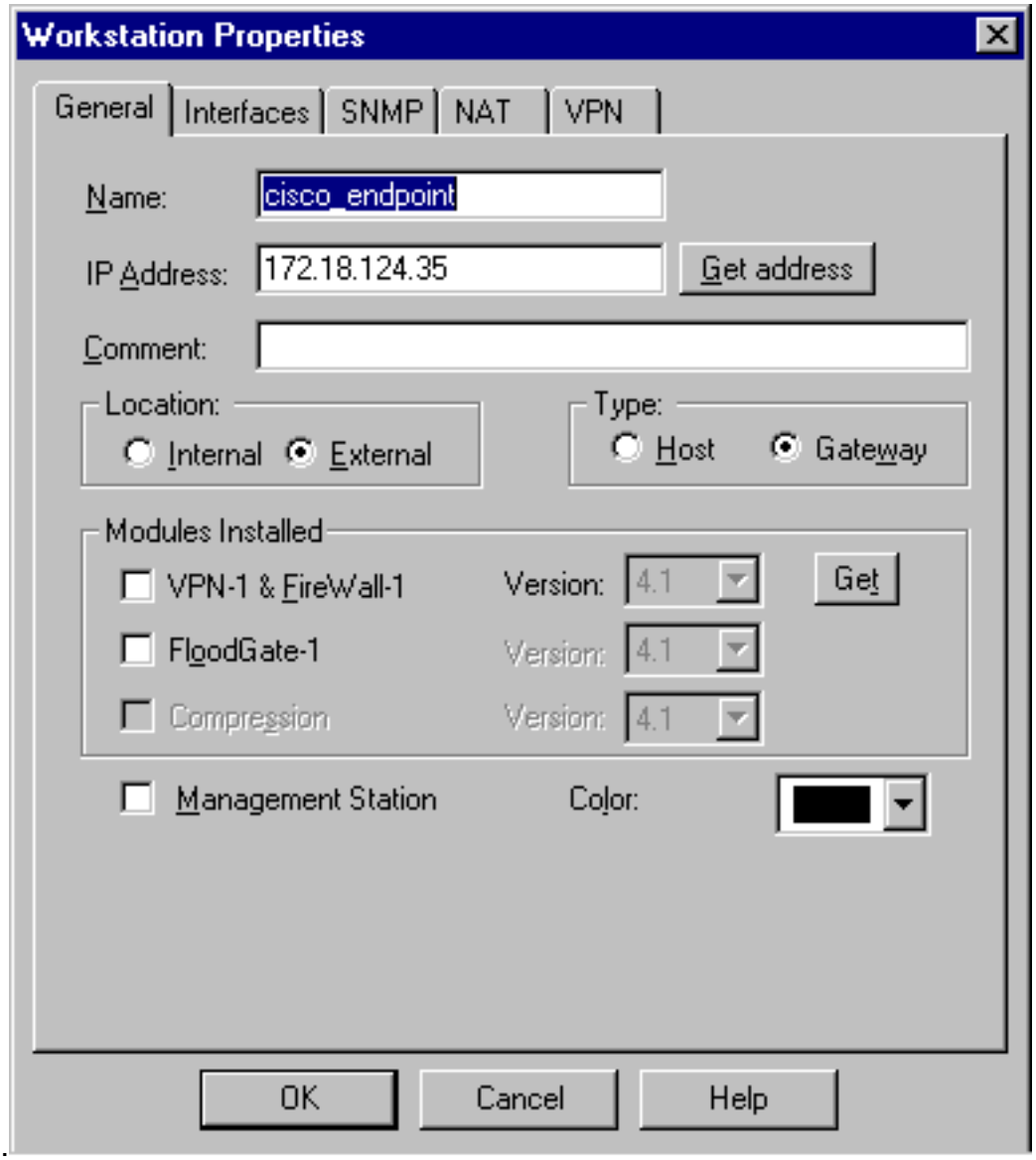
installés.

4. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour (« inside_cisco ») le réseau externe derrière le concentrateur VPN.Ceci devrait être conforme à la commande de concentrateur de **LocalAccess = <192.168.1.0/24>**

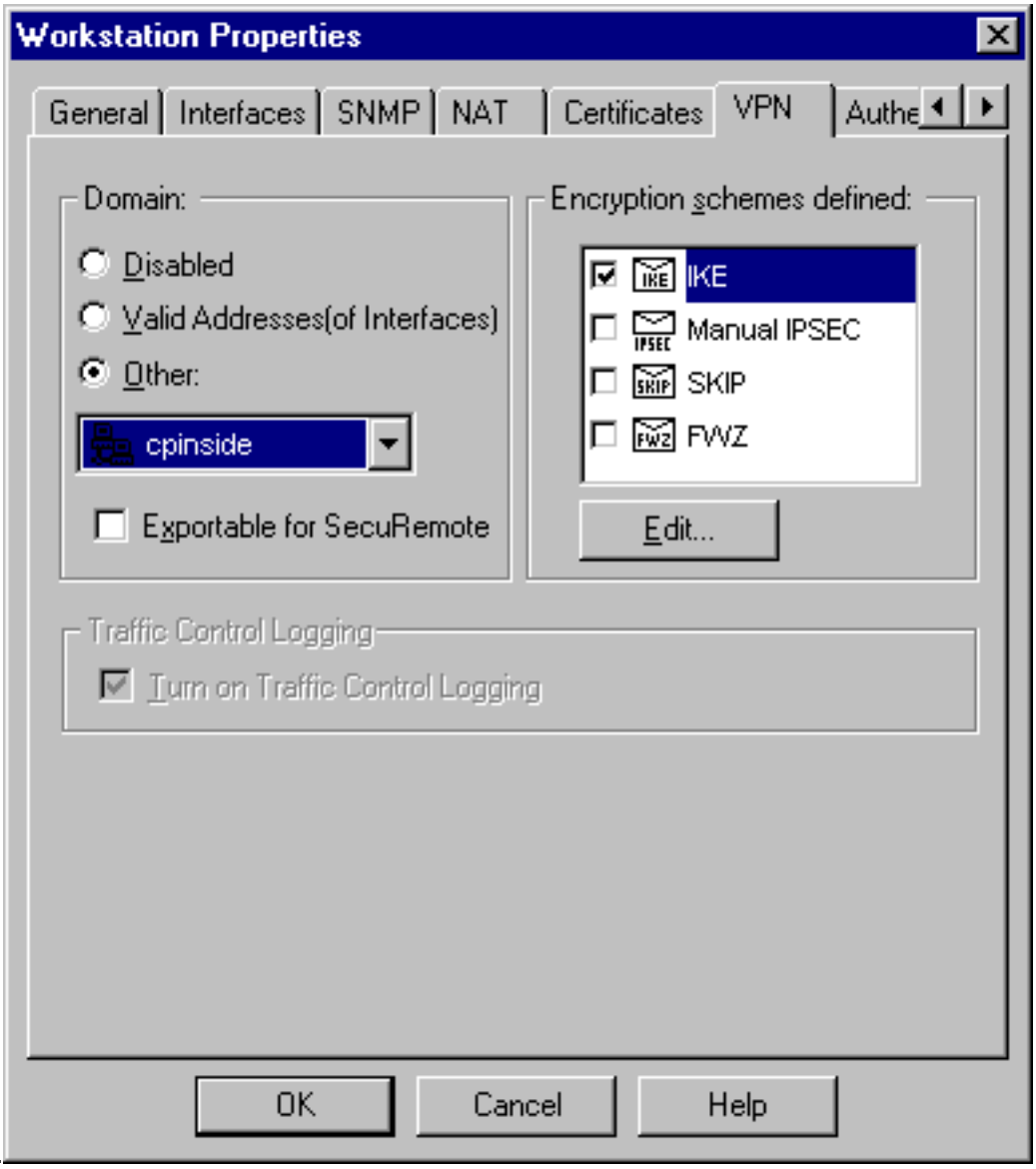


VPN.

5. Choisi **gérez > des objets de réseau > nouveau > poste de travail** pour ajouter un objet pour (« cisco_endpoint ») la passerelle externe de concentrateur VPN.C'est l'interface de « extérieur » du concentrateur VPN avec la Connectivité au point de reprise (dans ce document, 172.18.124.35 est l'adresse IP dans la commande d'**IP address = de <ip>**).Emplacement de dessous **externe** choisi. **Passerelle** choisie pour le type.**Note**: Ne vérifiez pas VPN-1/FireWall-

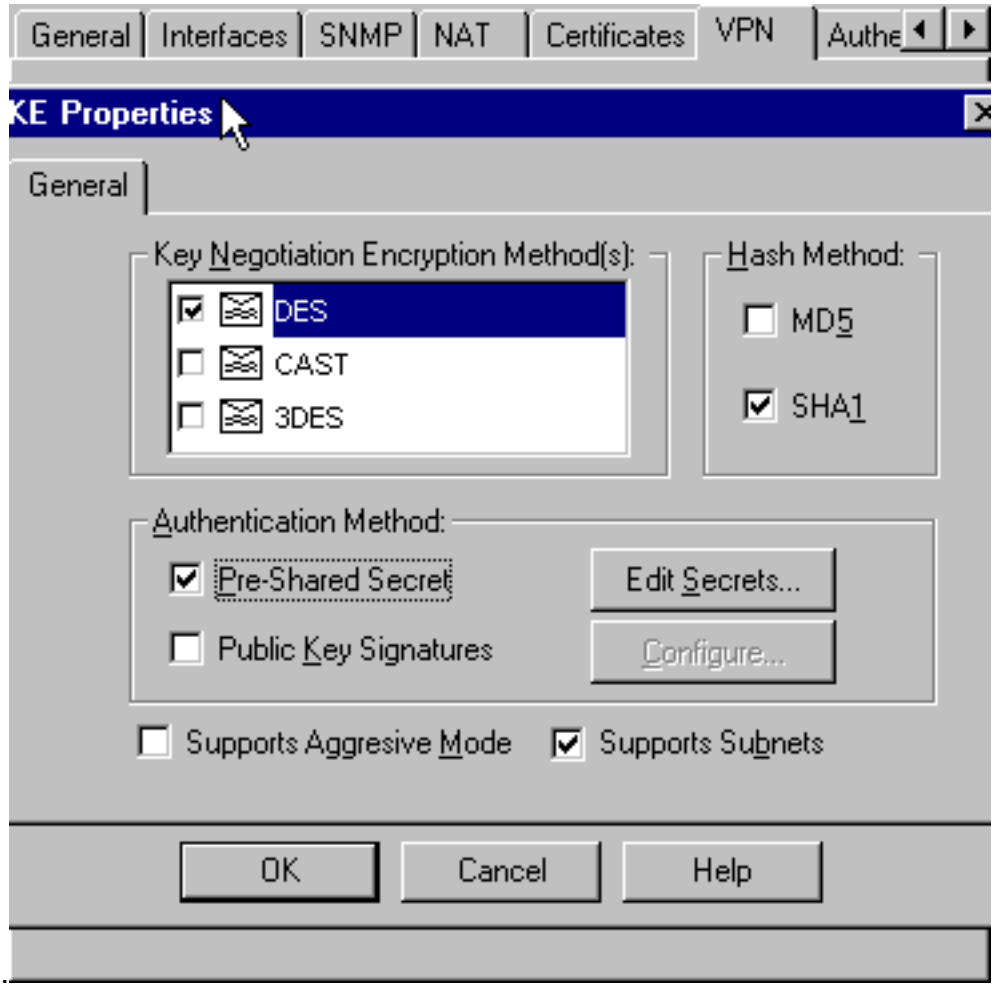
1. 

6. Choisi **gérez > des objets de réseau > éditent** pour éditer onglet VPN de point d'extrémité de passerelle avec point de contrôle (appelé le le « RTPCPVPN »). Sous le domaine, sélectionnez **autre** et puis sélectionnez l'intérieur du réseau de points de contrôle (appelé le « cpinside ») de la liste déroulante. Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit



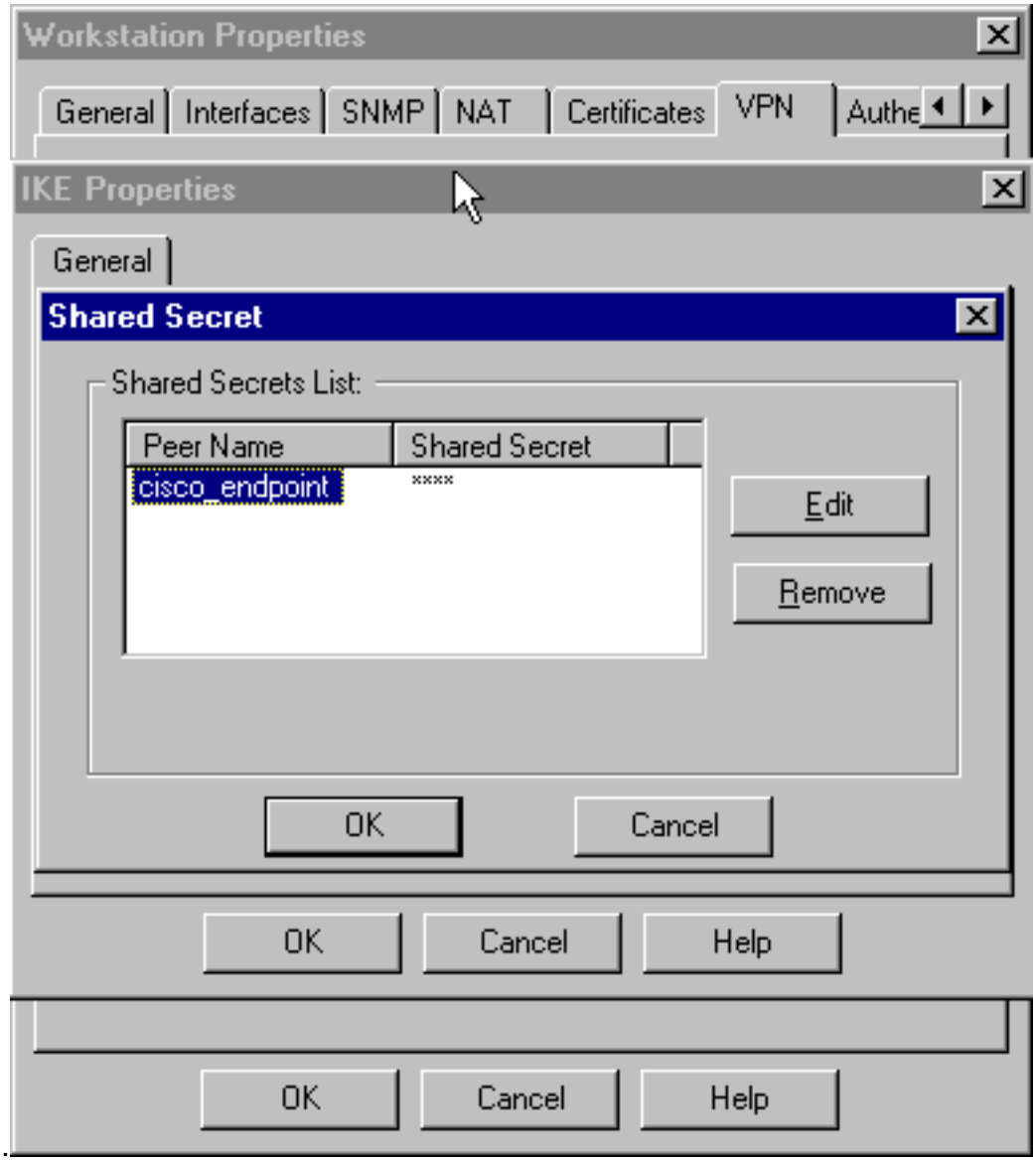
alors.

7. Changez les propriétés IKE au **chiffrement DES** et au hachage **SHA1** pour être d'accord avec la commande de concentrateur **SHA_DES_G2** VPN.**Note**: Le "G2" se rapporte au groupe 1 ou 2. de Diffie-Hellman. Dans le test, on l'a découvert que le point de reprise reçoit "G2" ou "G1."Changez ces configurations :Retirez le **mode agressif**.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode



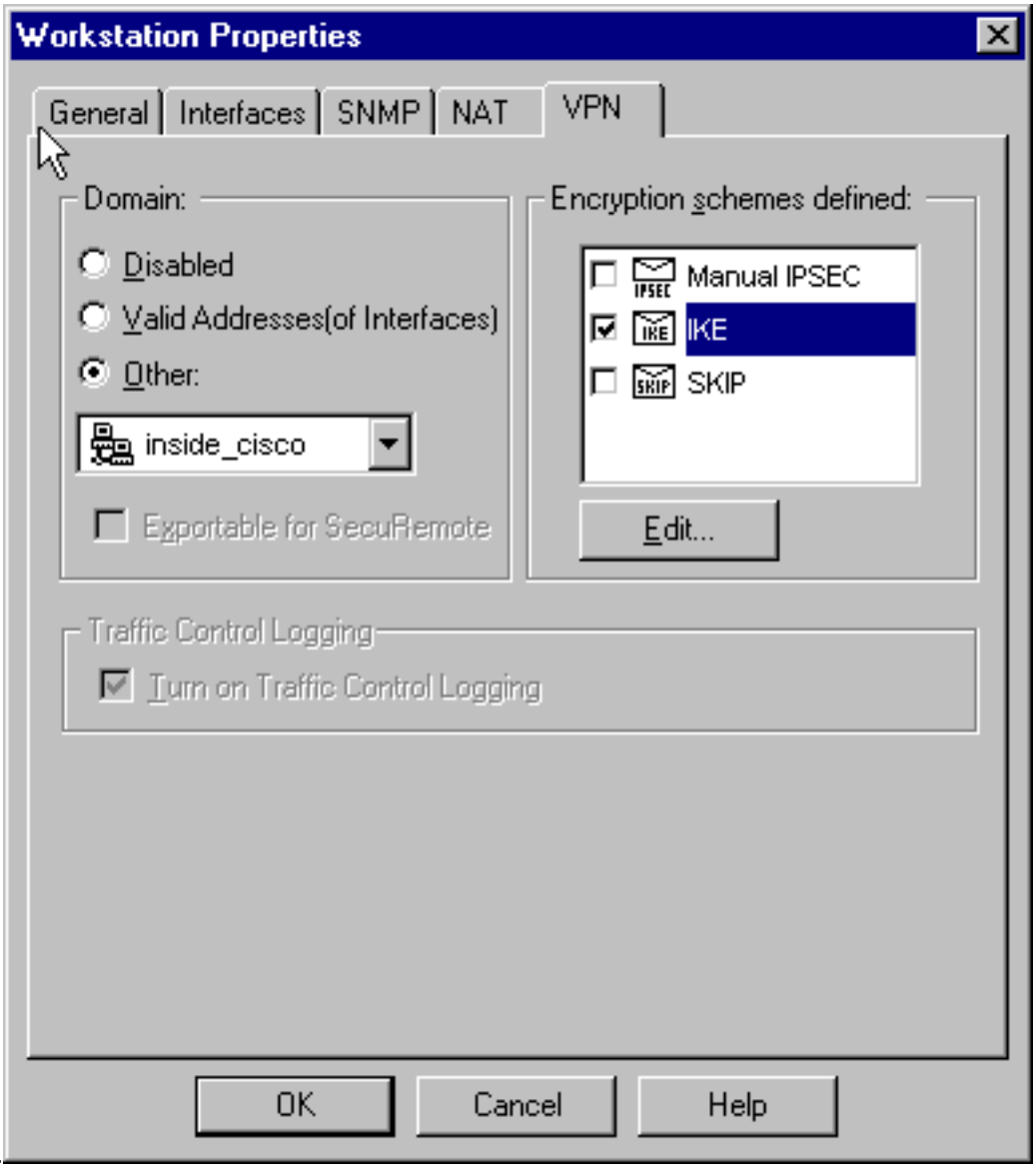
d'authentification.

8. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la commande de concentrateur de **SharedKey = de <key>**



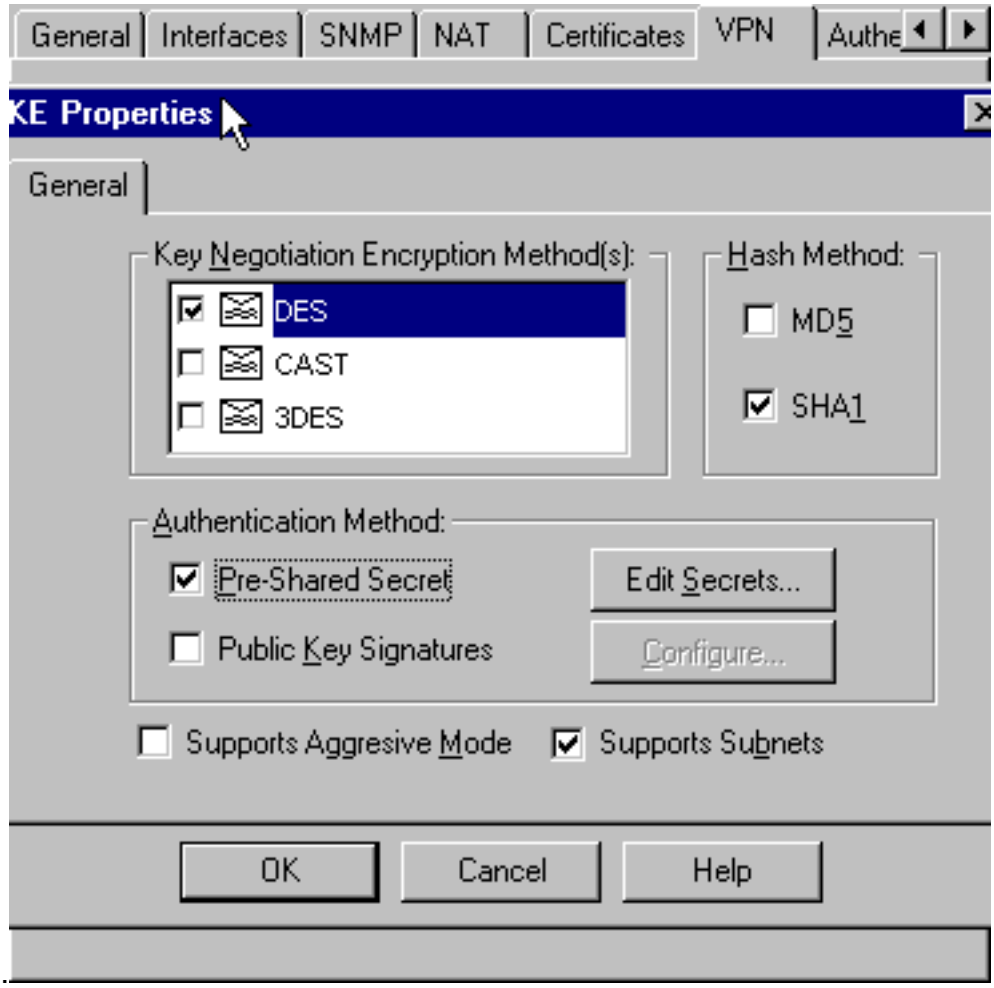
VPN.

9. Choisi **gérez > des objets de réseau > éditent** pour éditer l'onglet VPN de « cisco_endpoint ». Sous le domaine, sélectionnez **autre**, et puis sélectionnez l'intérieur du réseau de concentrateur VPN (appelé le « inside_cisco »). Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit



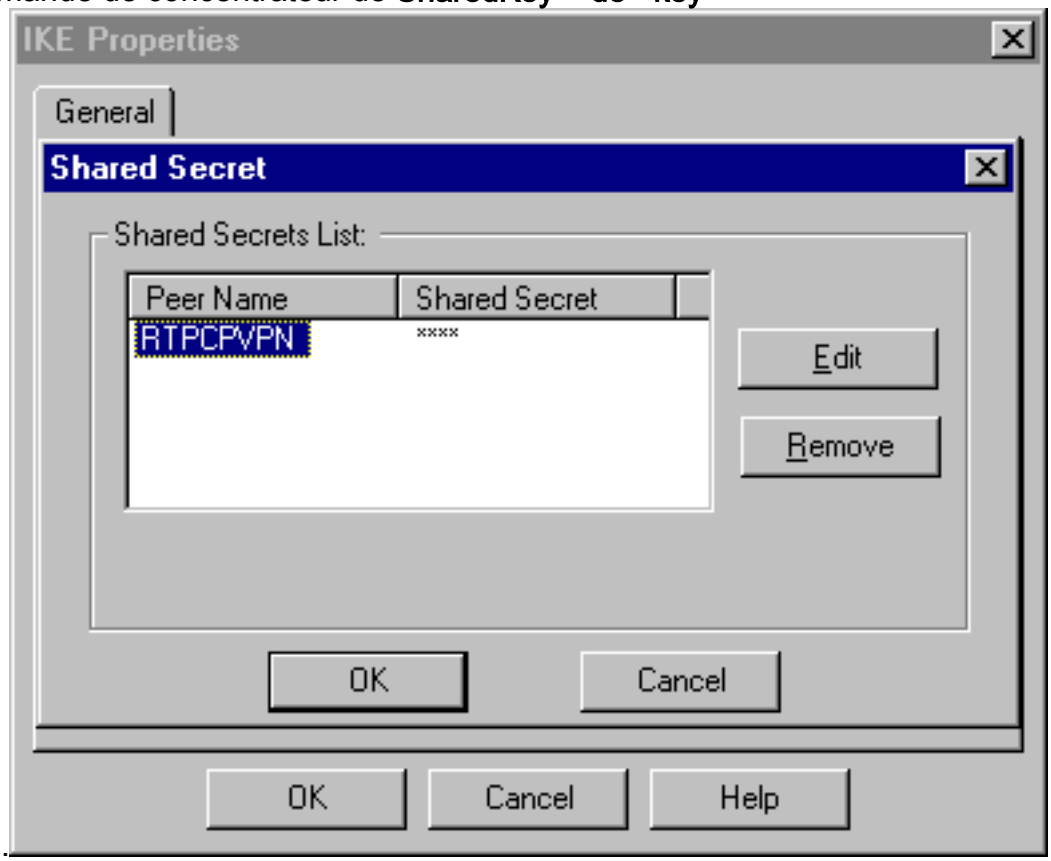
alors.

10. Changez les propriétés IKE au **chiffrement DES** et au hachage **SHA1** pour être d'accord avec la commande de concentrateur **SHA_DES_G2** VPN.**Note**: Le "G2" se rapporte au groupe 1 ou 2. de Diffie-Hellman. Dans le test, on l'a constaté que le point de reprise reçoit "G2" ou "G1."Changez ces configurations :Retirez le **mode agressif**.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode



d'authentification.

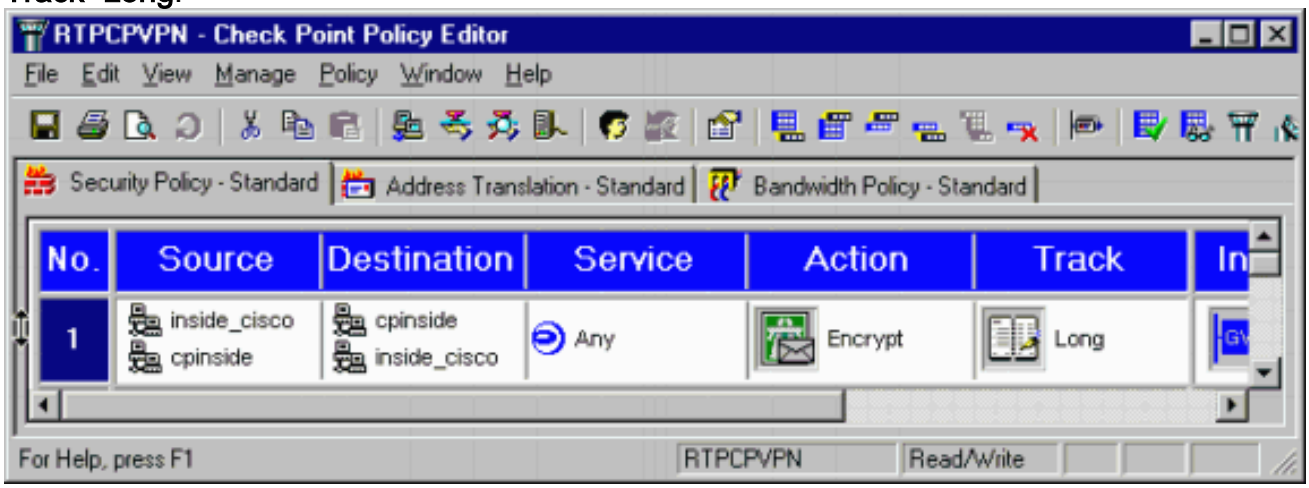
11. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la commande de concentrateur de **SharedKey = de <key>**



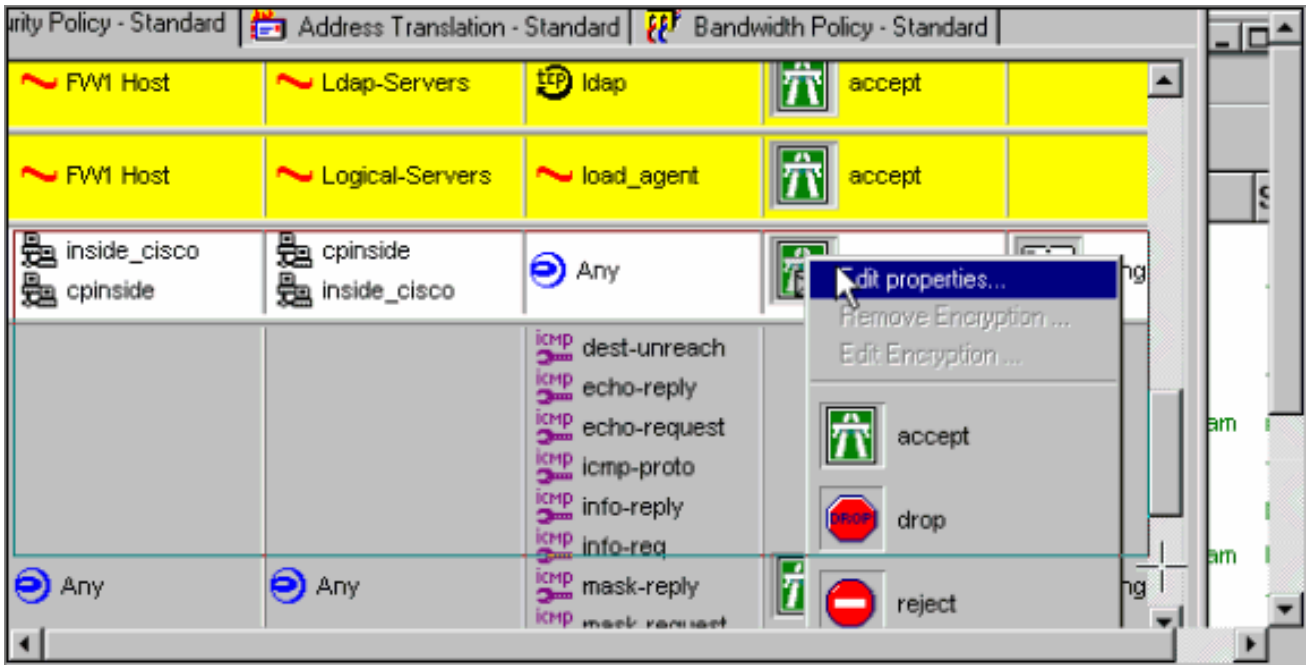
VPN.

12. Dans la fenêtre de l'éditeur de stratégie, insérez une règle avec la source et la destination en tant que le « inside_cisco » et « cpinside » (bidirectionnel). Placez **Service=Any**, **Action=Encrypt**, et

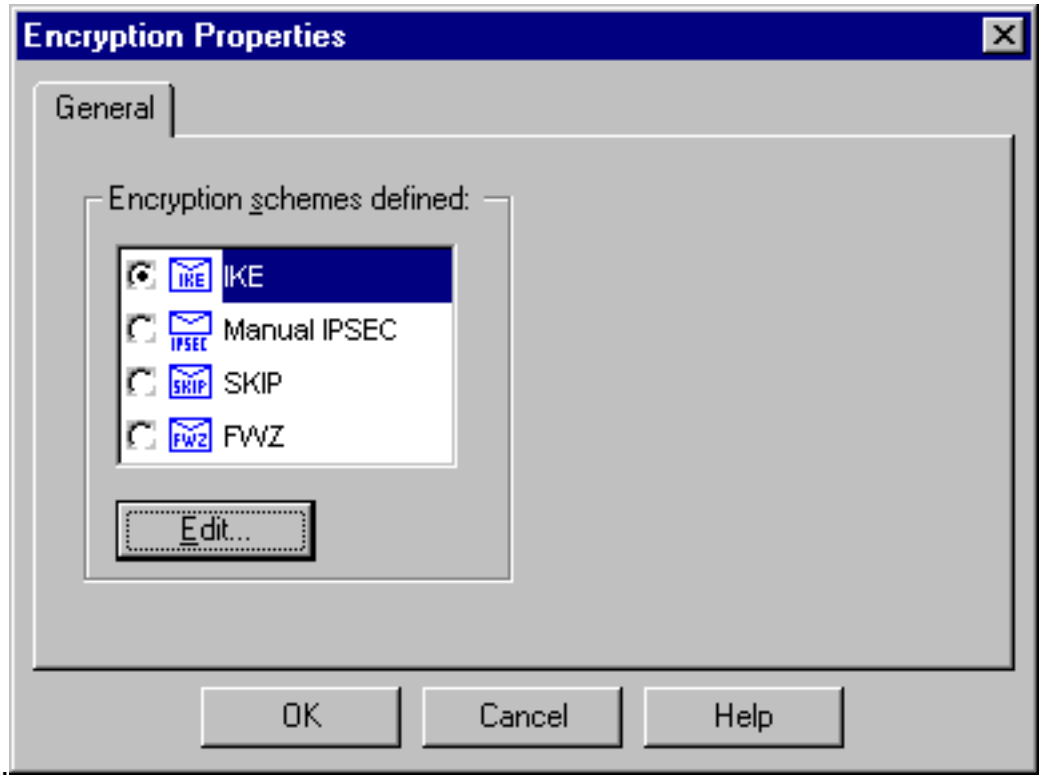
Track=Long.



13. Sous le titre d'action, cliquez sur l'icône verte chiffrement et choisi **éditez les propriétés** pour configurer des stratégies de chiffrement.

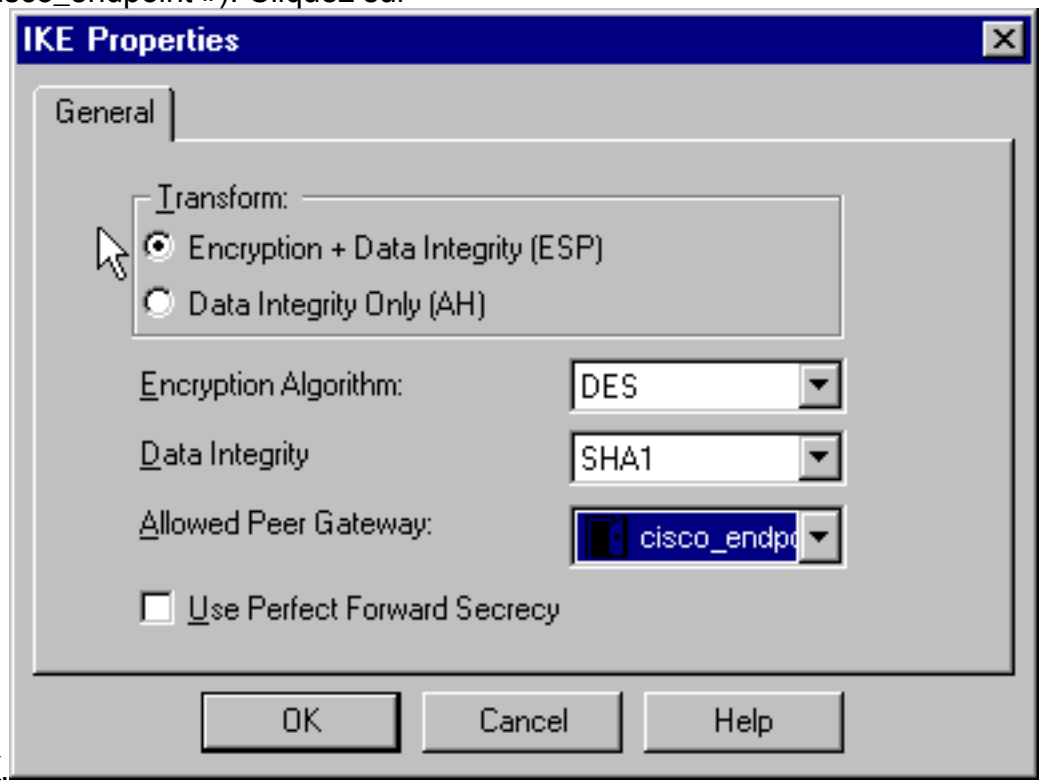


14. **L'IKE** choisi, et cliquent sur



Edit.

15. Sur la fenêtre de propriétés IKE, changez ces propriétés pour être d'accord avec la commande de concentrateur de **transformation = de l'ESP (SHA, DES)** VPN.Sous transformez, **cryptage + intégrité des données** choisis **(ESP)**. L'algorithme de chiffrement devrait être **DES**, intégrité des données devrait être **SHA1**, et la passerelle homologue permise devrait être la passerelle externe de concentrateur VPN (appelée le « cisco_endpoint »). Cliquez sur



OK.

16. Après que vous configuriez le point de reprise, la **stratégie** choisie **> installent** sur le menu du point de contrôle pour faire les prendre effet les modifications.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Commandes de dépannage du concentrateur VPN 5000

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** .

Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **le vidage mémoire de suivi de vpn** affiche **entièrement des** informations sur toutes les connexions VPN correspondantes, y compris des informations sur le temps, le nombre VPN, la vraie adresse IP du pair, que des scripts ont été exécuté, et dans le cas d'une erreur, la routine et le numéro de ligne de code logiciel où l'erreur s'est produite.
- **mémoire tampon de log de show system** — Affiche le contenu de la mémoire tampon de log interne.
- **affichez les statistiques de vpn** — Affiche ces informations pour des utilisateurs, des Partenaires, et le total pour chacun des deux. (Pour les modèles modulaires, l'affichage inclut une section pour chaque emplacement de module. Référez-vous à la section d'exemple de sortie de débogage.)`Active en cours` — Les connexions actives en cours.`Dans Negot` — Les connexions actuellement de négociation.`Hautes eaux` — Le nombre de connexions actives simultanément le plus élevé depuis la dernière réinitialisation.`Total cumulé` — Le nombre total de connexions réussies depuis la dernière réinitialisation.`OK de tunnel` — Le nombre de tunnels pour lesquels il n'y avait aucune erreur.`Débuts de tunnel` — Le nombre de débuts de tunnel.`Erreur de tunnel` — Le nombre de tunnels avec des erreurs.
- **affichez les statistiques de vpn bavardes** — Statistiques des négociations ISAKMP d'expositions, et beaucoup plus statistiques de connexion active.

Récapitulation de réseau

Quand des réseaux intérieurs adjacents de multiple sont configurés dans le domaine de cryptage sur le point de reprise, le périphérique pourrait automatiquement les récapituler 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, ils pourraient être récapitulés à 10.0.0.0 /23.

Debug de pare-feu Checkpoint 4.1

C'était une installation de NT de Microsoft Windows. Puisque le cheminement a été placé pour `long` dans la fenêtre de l'éditeur de stratégie (comme vu dans étape 12), refusé le trafic devrait apparaître en rouge dans le visualiseur de log. Plus bavard mettez au point peut être obtenu par :

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

et dans une autre fenêtre :

```
C:\WINNT\FW1\4.1\fwstart
```

Émettez ces commandes d'autoriser les associations de sécurité (SAS) sur le point de reprise :

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

La réponse **oui au** `sont vous sure ?` demande.

Exemple de sortie de débogage

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
```

```
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          ------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped              13
Unwrapped             9
BadEncap              0
BadAuth               0
BadEncrypt            0
rx IP                 9
rx IPX                0
rx Other              0
tx IP                13
tx IPX                0
tx Other              0
IKE rekey             0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
```

```
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          -----------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
```

```
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0
```

Informations connexes

- Annonce de fin de ventes de Concentrateur VPN de la gamme Cisco 5000
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems