Configuration d'un tunnel IPSec – entre un concentrateur Cisco VPN 3000 et un pare-feu Checkpoint 4.1

Contenu

Introduction

Il explique comment créer un tunnel IPSec avec des clés pré-partagées afin de joindre deux réseaux privés :

- Un réseau privé à l'intérieur du concentrateur de Cisco VPN 3000 (192.168.1.x).
- 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 cette configuration commence.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

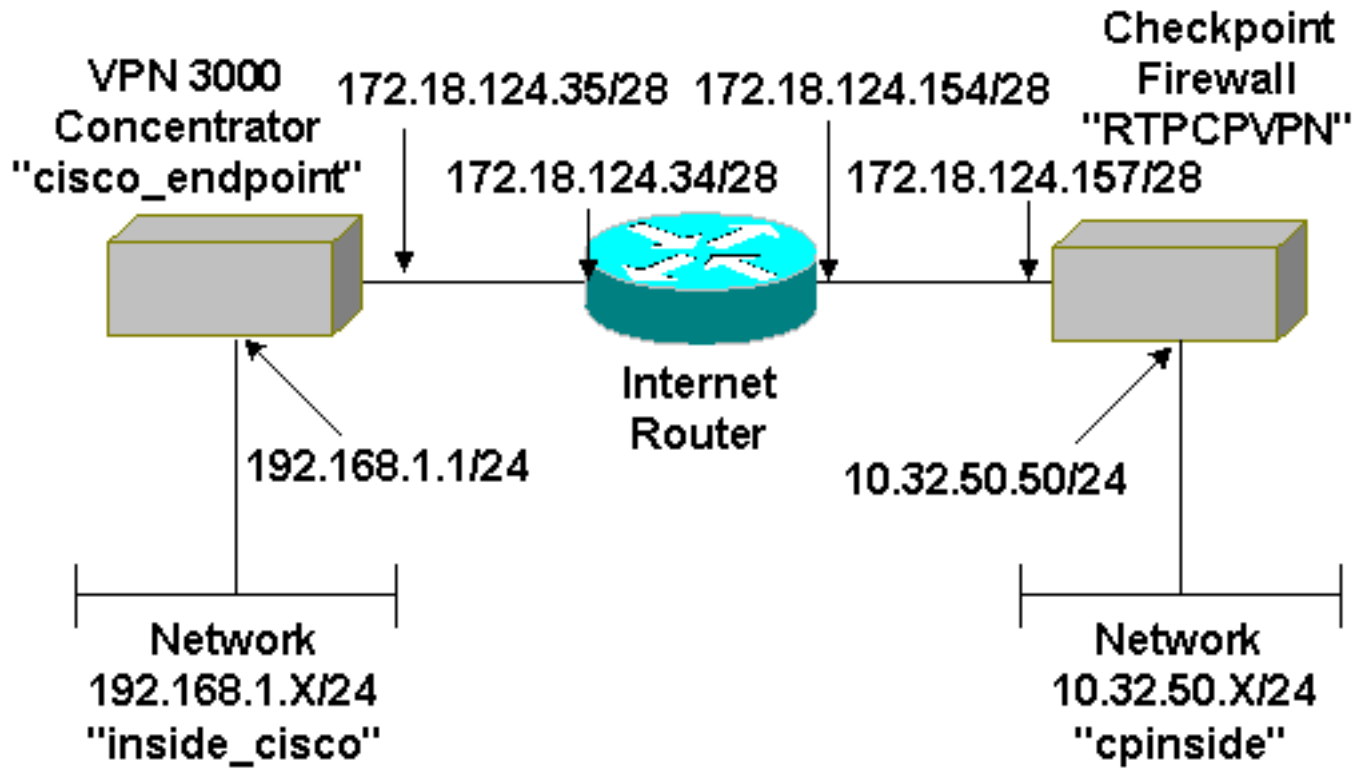
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur VPN 3000
- Version de logiciel 2.5.2.F de concentrateur VPN 3000
- 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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

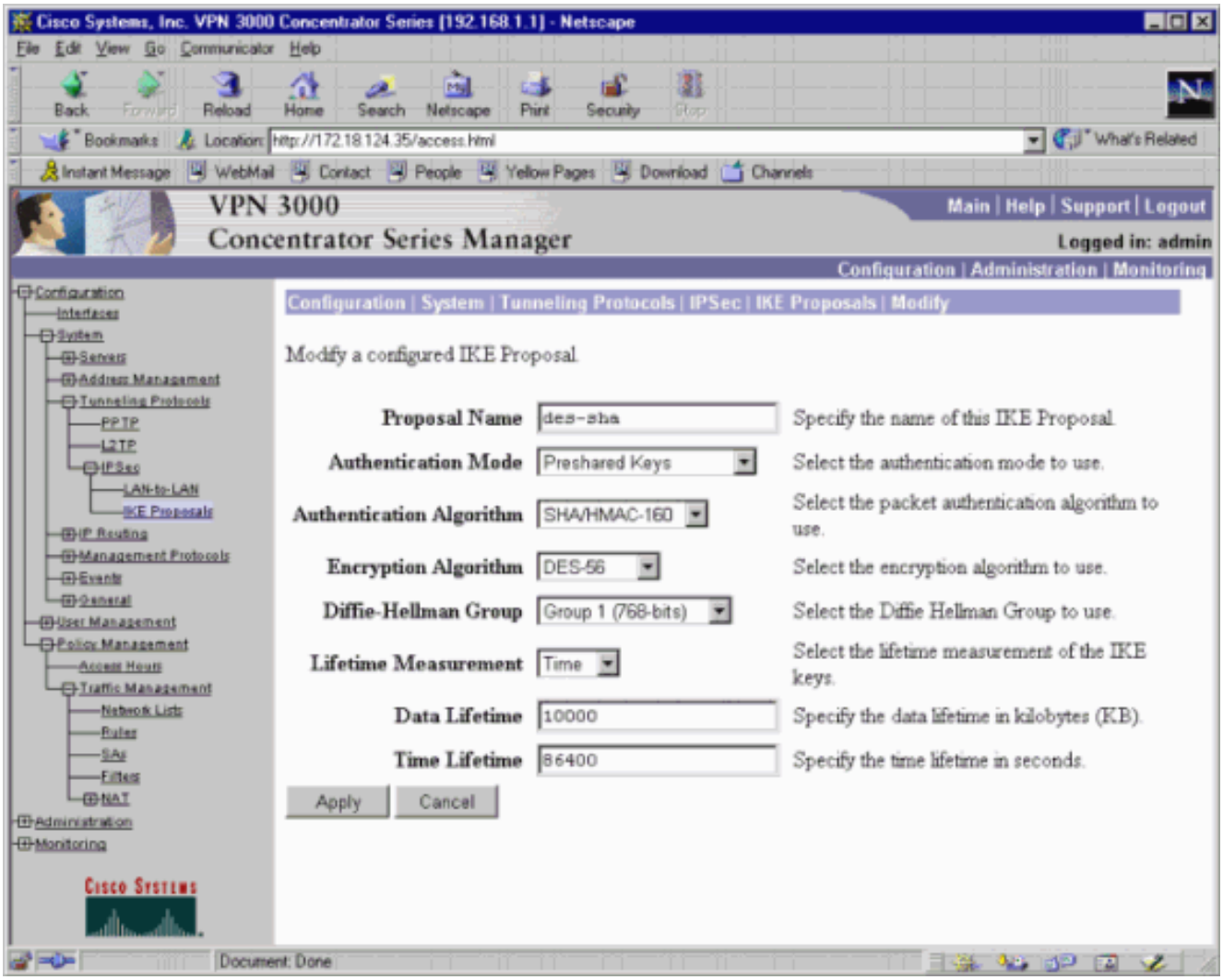
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez le concentrateur VPN 3000

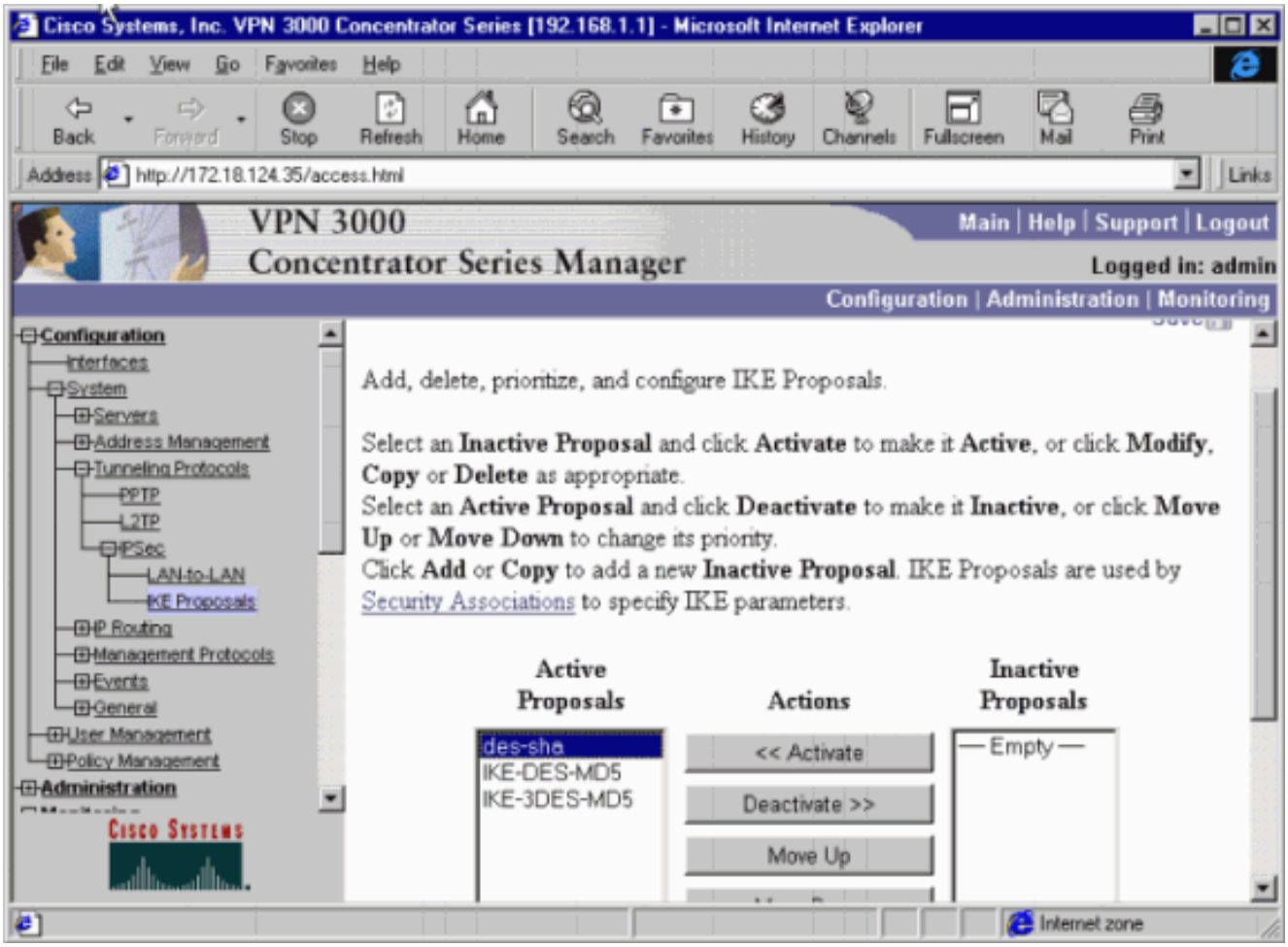
Terminez-vous ces étapes pour configurer le concentrateur VPN 3000.

1. **La configuration > les protocoles de système > de Tunnellisation > l'IPSec > les propositions** choisis d'**IKE > modifient** pour créer une proposition d'Échange de clés Internet (IKE) nommée « DES-SHA » avec le hachage d'Algorithme de hachage sûr (SHA), le Norme de chiffrement de données (DES), et le congé du groupe 1. de Diffie-Hellman la vie de temps au

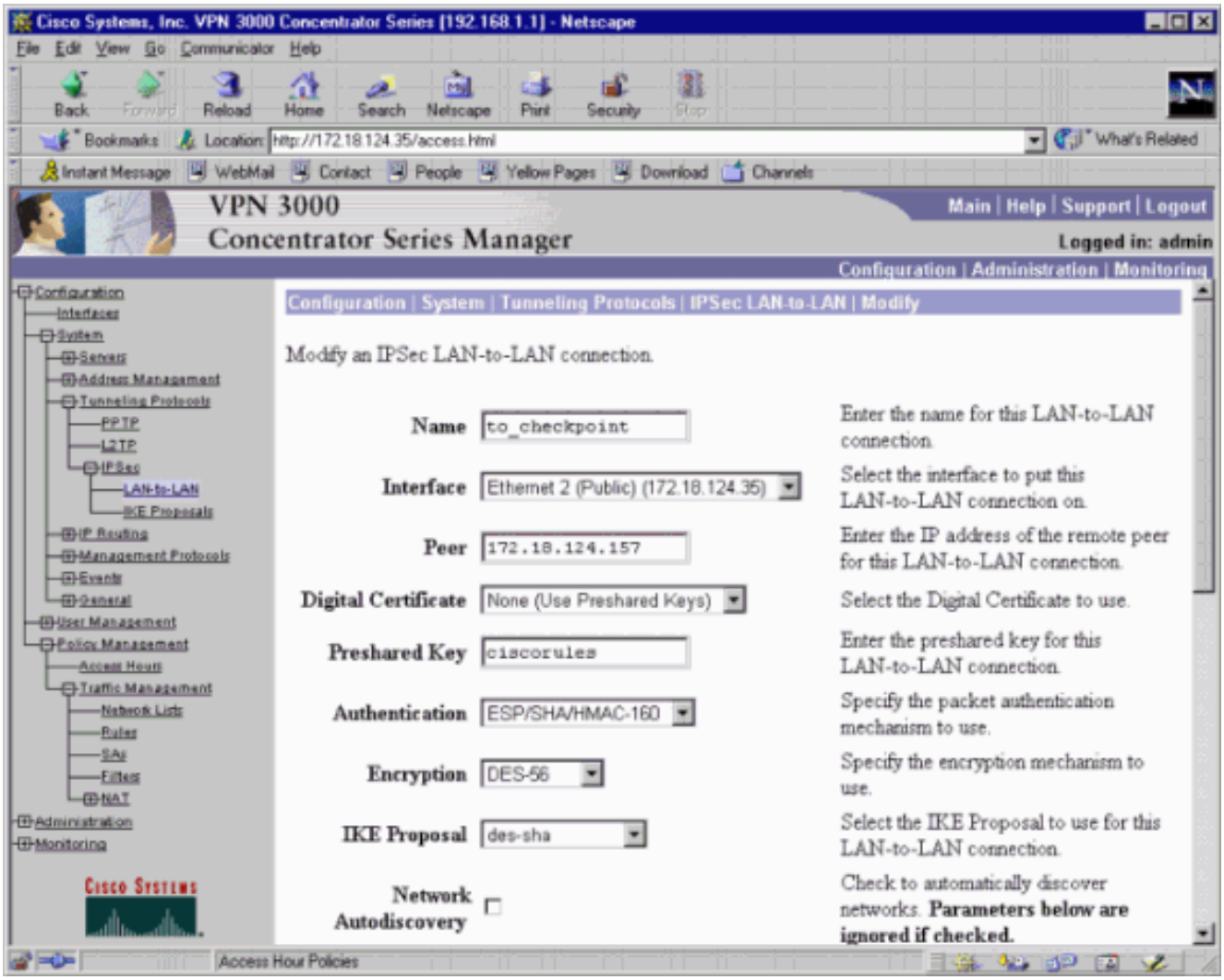
par défaut 86400 secondes.**Note**: La plage valide pour la vie d'IKE de concentrateur VPN est de 60-2147483647
secondes.

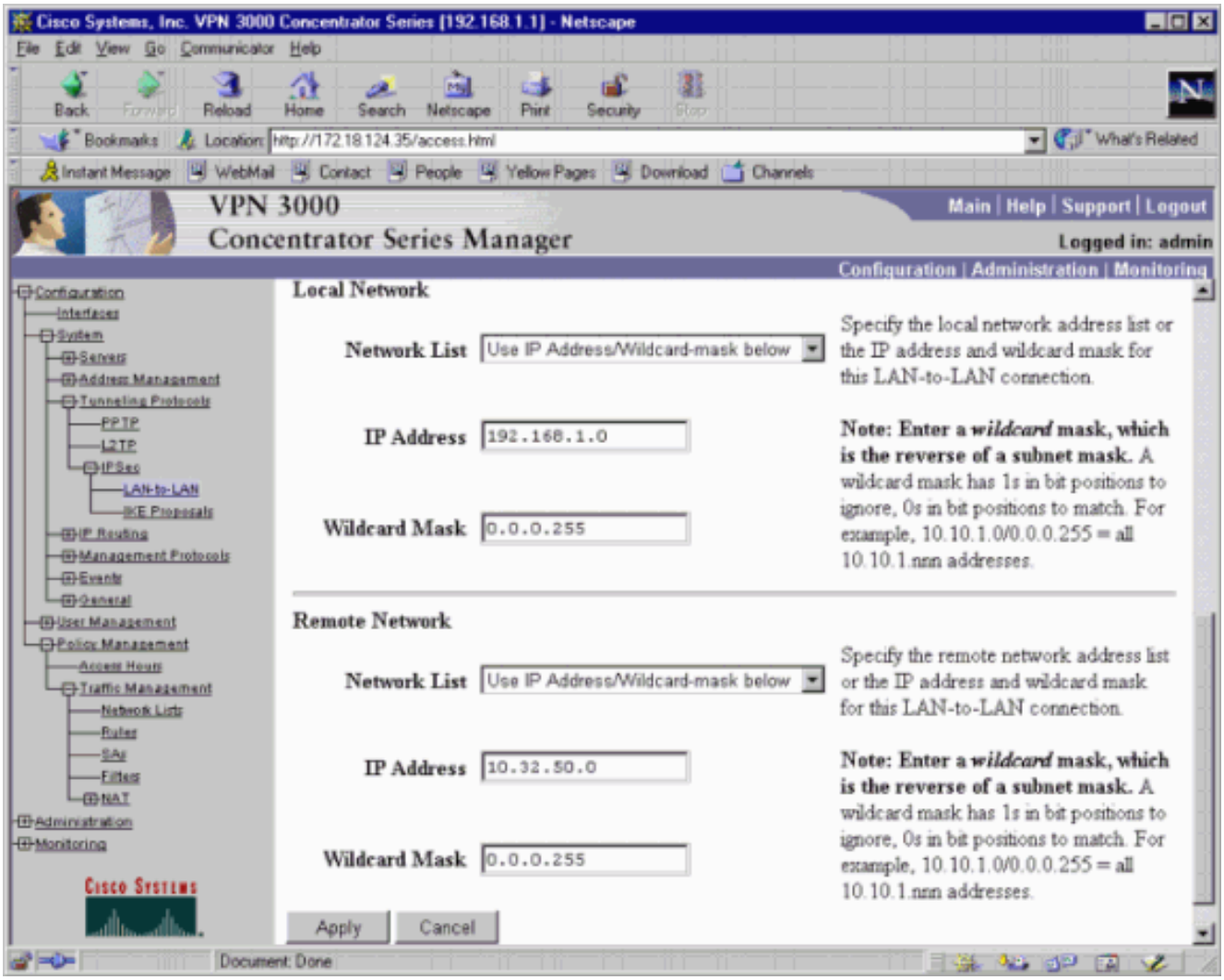


2. **Configuration > protocoles de système > de Tunnellisation > IPSec > propositions** choisis d'**IKE**. Sélectionnez le « DES-SHA » et le clic **lancent** pour lancer la proposition d'IKE.

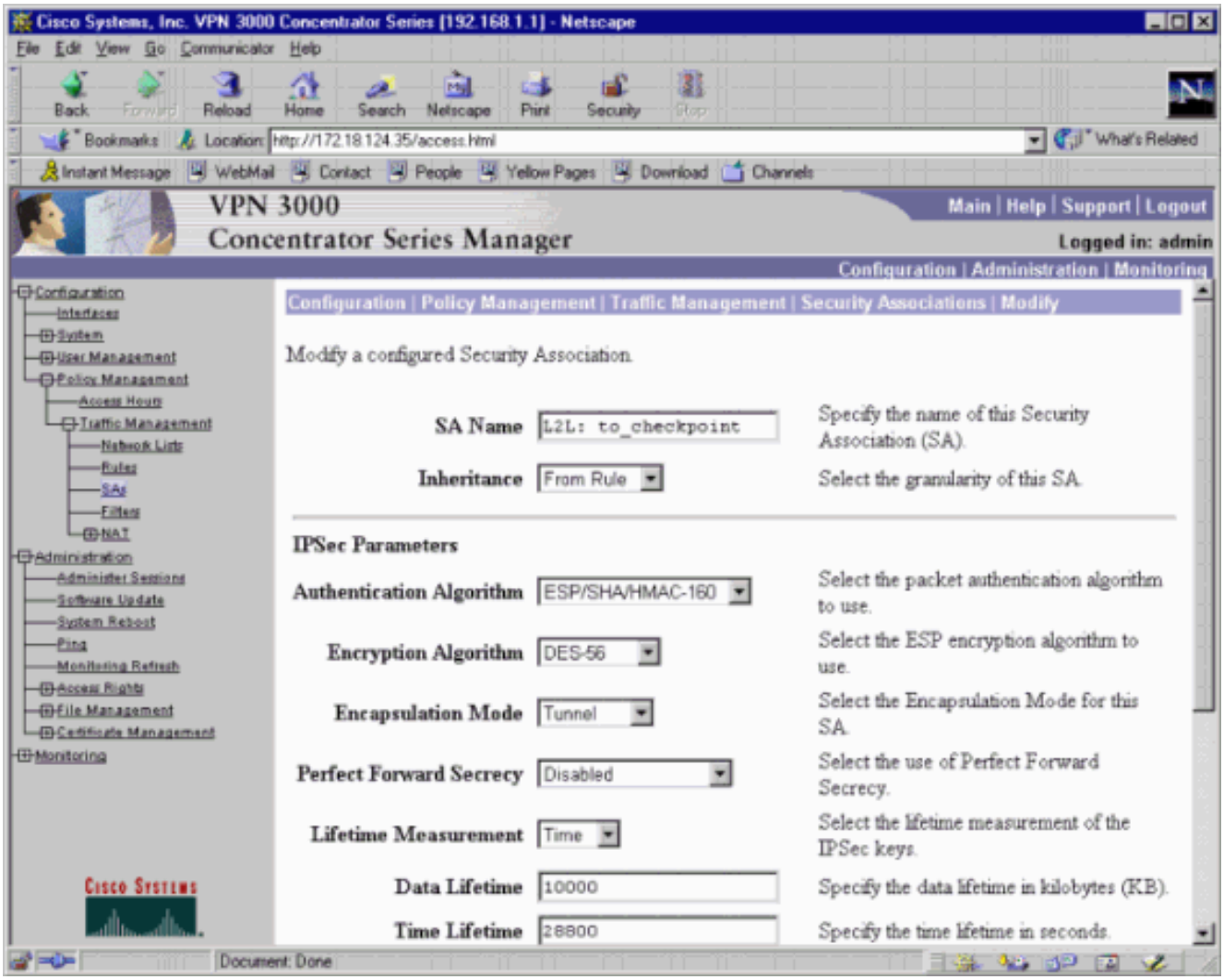


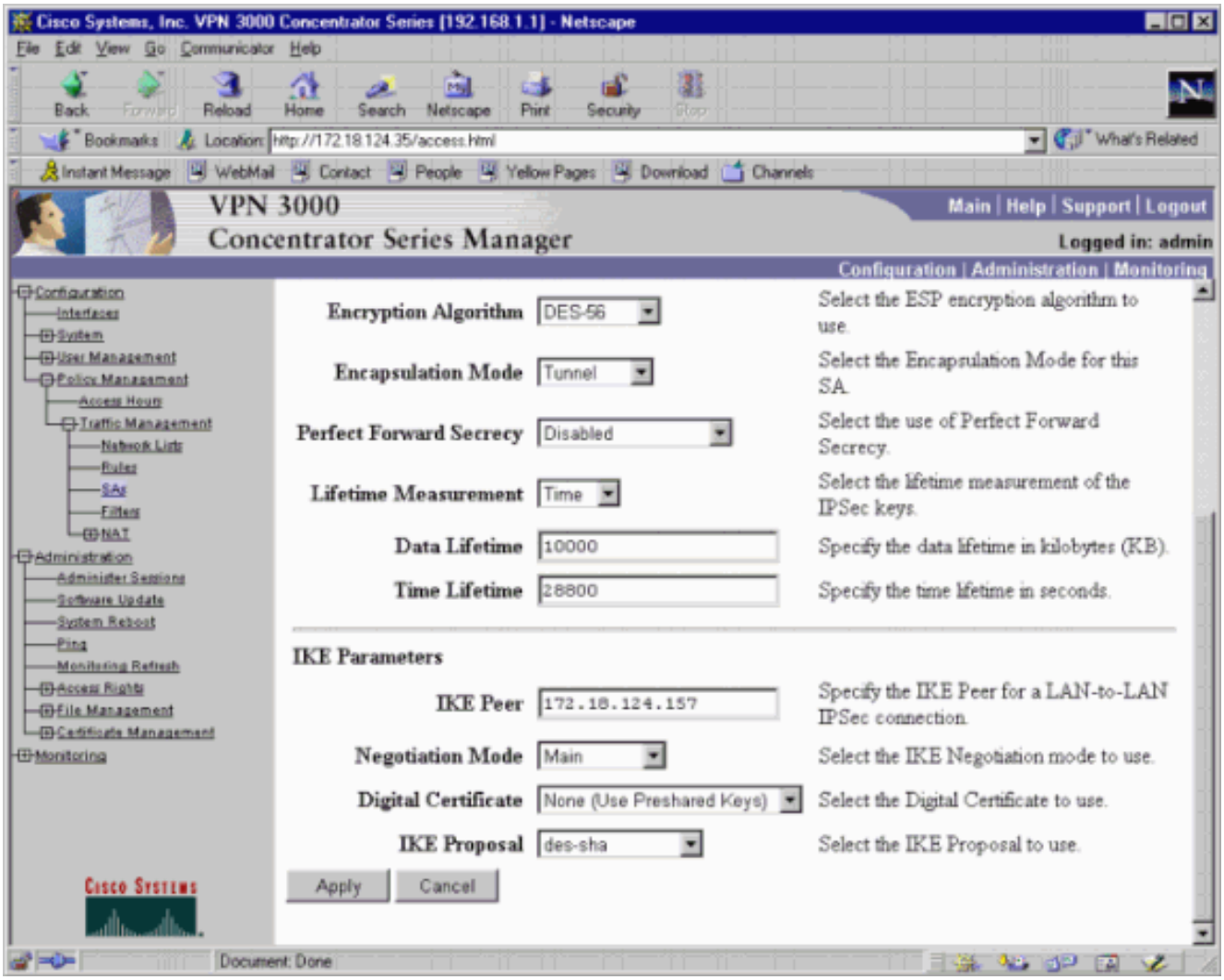
3. **La configuration > les protocoles de système > de Tunnellisation > l'entre réseaux locaux** choisis d'**IPSec > ajoutent**.Installez un tunnel d'IPsec appelé le « to_checkpoint » avec l'adresse de point de reprise en tant que pair. Pour la clé pré-partagée, introduisez l'adresse réelle. Sous l'authentification, l'ESP/SHA/HMAC-160 choisi, et le DES-56 choisi pour le cryptage. Écrivez la proposition d'IKE (« DES-SHA » dans cet exemple), et les gens du pays et les réseaux
distants.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
Servers
Address Management
Tunneling Protocols
PPTP
L2TP
IPSec
LAN-to-LAN
IKE Proposals
IP Routing
Management Protocols
Events
General
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Monitoring
Cisco Systems
Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Modify
Modify an IPSec LAN-to-LAN connection.
Name
to_checkpoint
Enter the name for this LAN-to-LAN connection.
Interface
Ethernet 2 (Public) (172.18.124.35)
Select the interface to put this LAN-to-LAN connection on.
Peer
172.18.124.157
Enter the IP address of the remote peer for this LAN-to-LAN connection.
Digital Certificate
None (Use Preshared Keys)
Select the Digital Certificate to use.
Preshared Key
ciscorules
Enter the preshared key for this LAN-to-LAN connection.
Authentication
ESP/SHA/HMAC-160
Specify the packet authentication mechanism to use.
Encryption
DES-56
Specify the encryption mechanism to use.
IKE Proposal
des-sha
Select the IKE Proposal to use for this LAN-to-LAN connection.
Network Autodiscovery
Check to automatically discover networks. Parameters below are ignored if checked.
Access Hour Policies



4. **La configuration > la Gestion des stratégies > la gestion de trafic > les associations de sécurité** choisies **> modifient**. Vérifiez que le perfect forward secrecy **est désactivé** et laissez à la vie de temps d'IPsec au par défaut **28800** secondes.**Note**: La plage valide pour la vie d'IPsec de concentrateur VPN est de 60-2147483647
secondes.


Cisco Systems, Inc. VPN 3000 Concentrator Series [192.168.1.1] - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: http://172.18.124.35/access.html What's Related
Instant Message WebMail Contact People Yellow Pages Download Channels
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Access Hours
Traffic Management
Network Lists
Rules
SAs
Filters
NAT
Administration
Administer Sessions
Software Update
System Reboot
Ping
Monitoring Refresh
Access Rights
File Management
Certificate Management
Monitoring
Cisco Systems
Configuration | Policy Management | Traffic Management | Security Associations | Modify
Modify a configured Security Association.
SA Name L2L: to_checkpoint Specify the name of this Security Association (SA).
Inheritance From Rule Select the granularity of this SA.
IPSec Parameters
Authentication Algorithm ESP/SHA/HMAC-160 Select the packet authentication algorithm to use.
Encryption Algorithm DES-56 Select the ESP encryption algorithm to use.
Encapsulation Mode Tunnel Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy Disabled Select the use of Perfect Forward Secrecy.
Lifetime Measurement Time Select the lifetime measurement of the IPSec keys.
Data Lifetime 10000 Specify the data lifetime in kilobytes (KB).
Time Lifetime 28800 Specify the time lifetime in seconds.
Document: Done

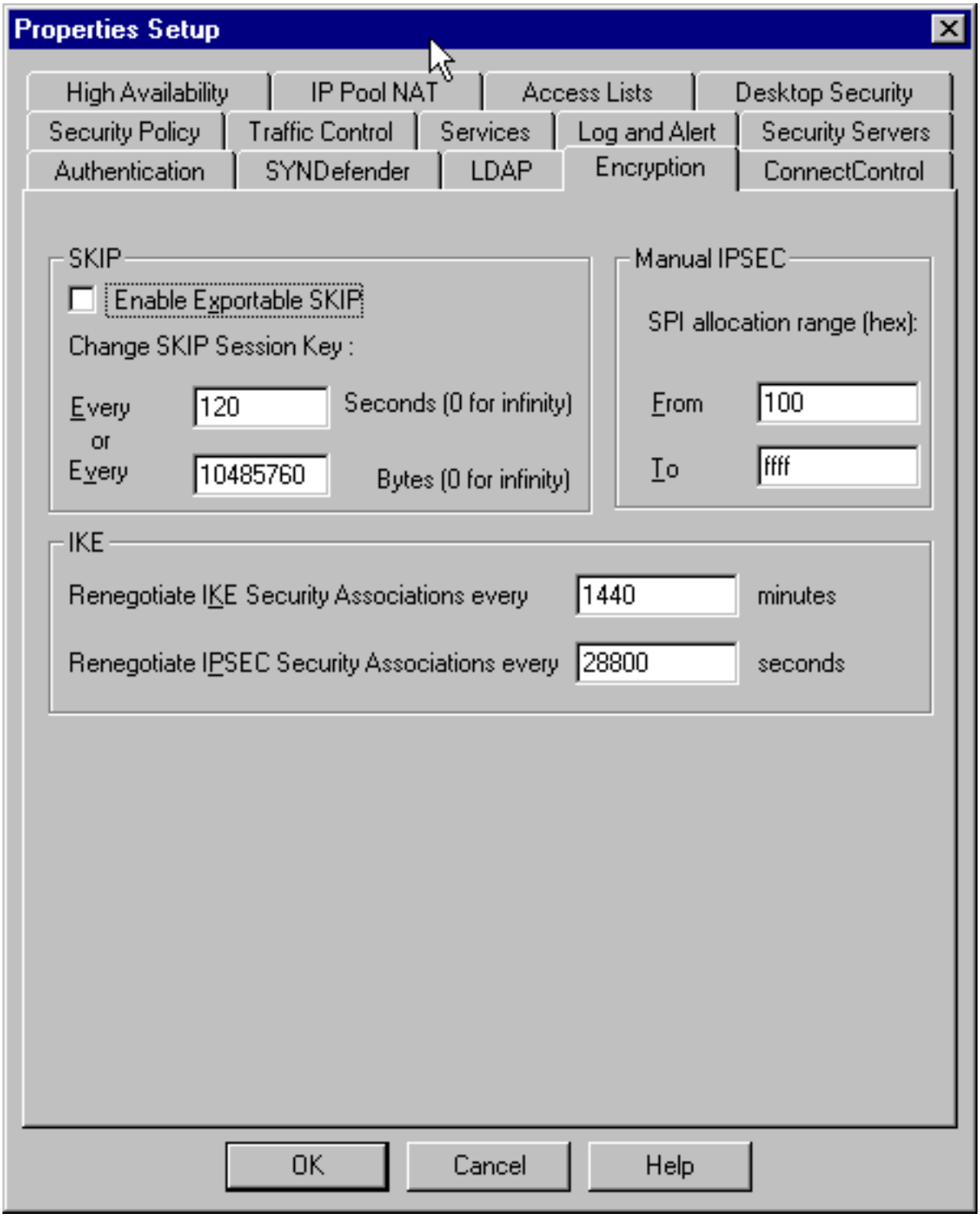


5. Enregistrez la configuration.

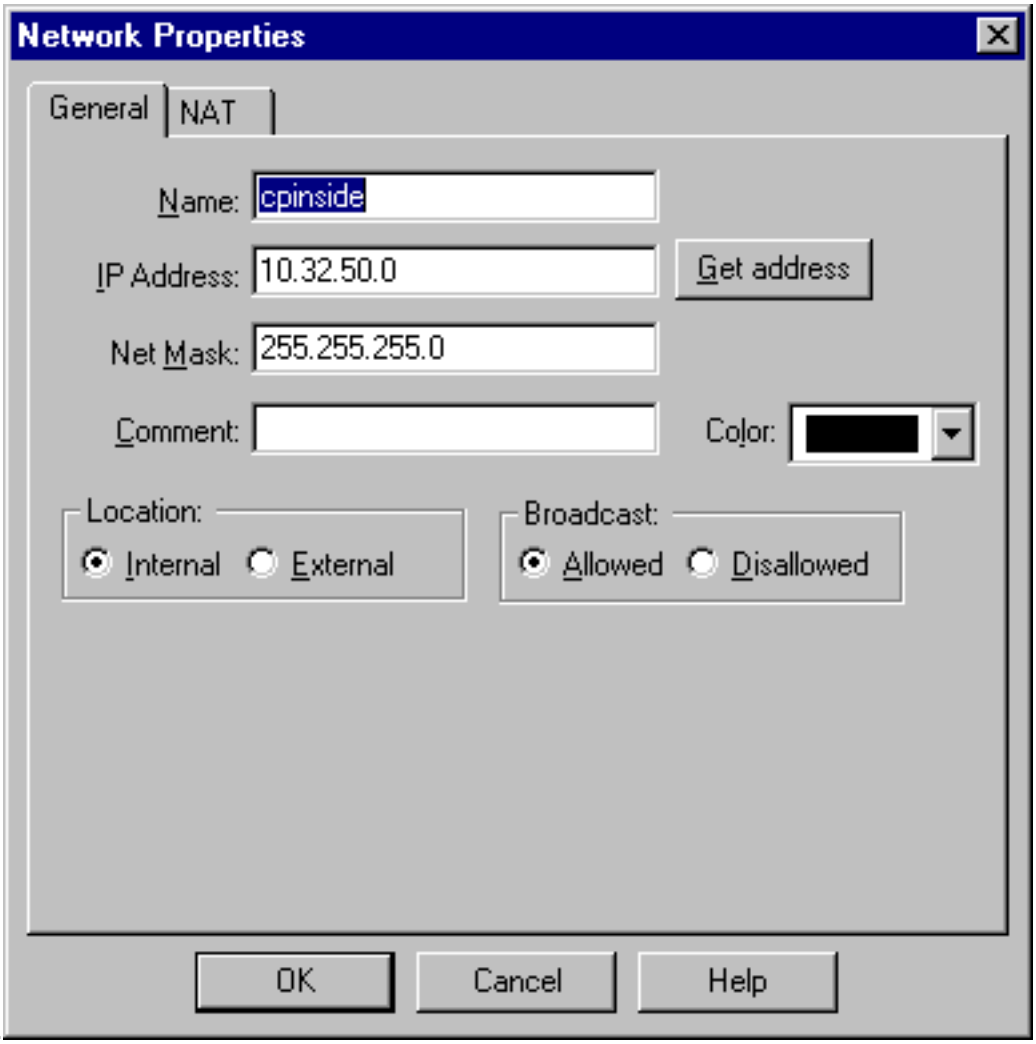
Configurez le pare-feu Checkpoint 4.1

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

1. Puisque l'IKE et les vies par défaut d'IPsec diffèrent entre les constructeurs, **Properties** choisi **> le cryptage** pour placer les durées de vie du point de contrôle pour être d'accord avec le concentrateur VPN se transfère.La vie d'IKE de par défaut de concentrateur VPN est de 86400 secondes (minutes =1440).La vie d'IPsec de par défaut de concentrateur VPN est de 28800
secondes.

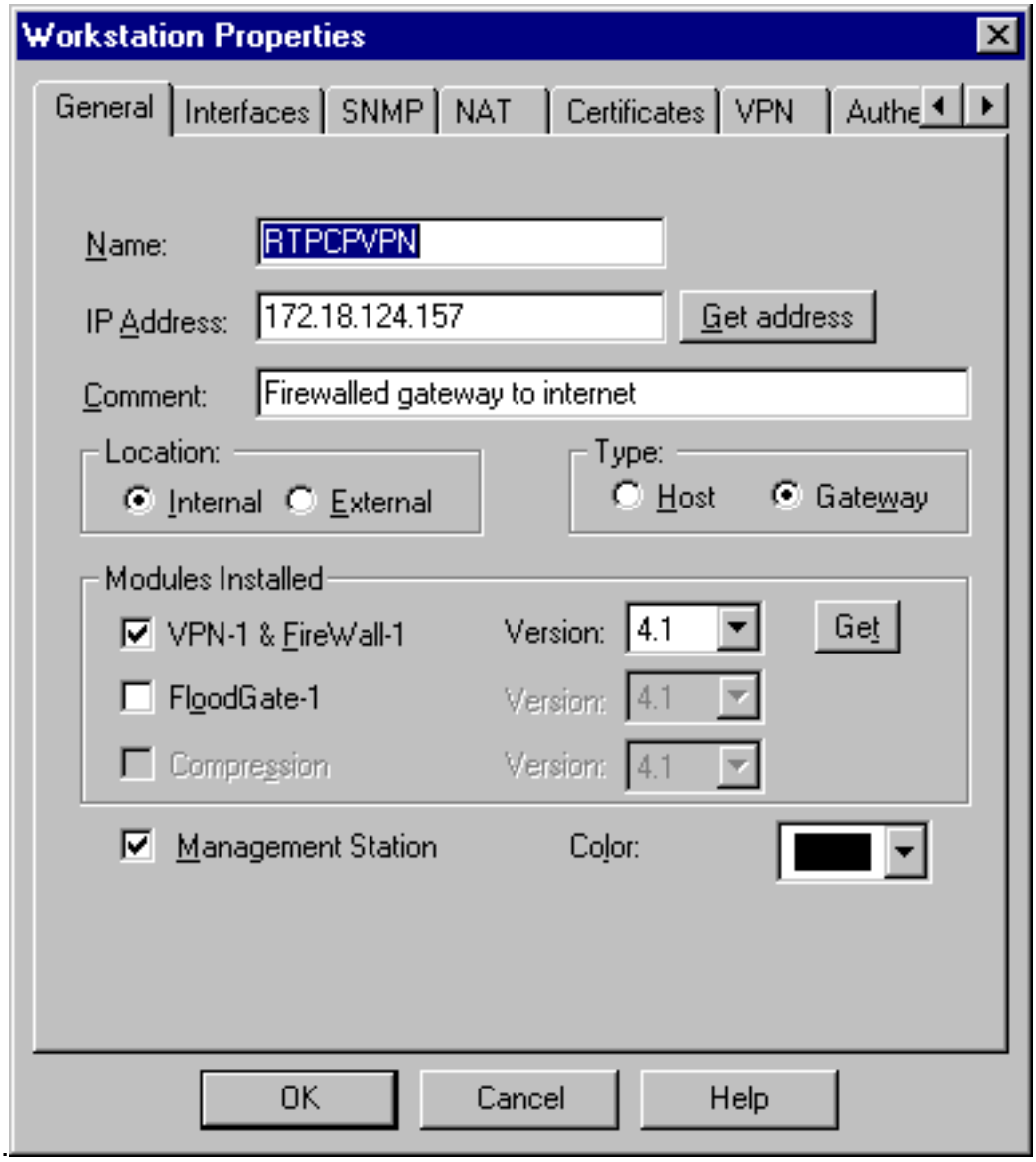


2. Choisi **gérez > des objets de réseau > nouveau (ou éditez) > réseau** pour configurer l'objet pour (« cpinside ») le réseau interne derrière le point de reprise. Ceci devrait être conforme au « réseau distant » dans le concentrateur



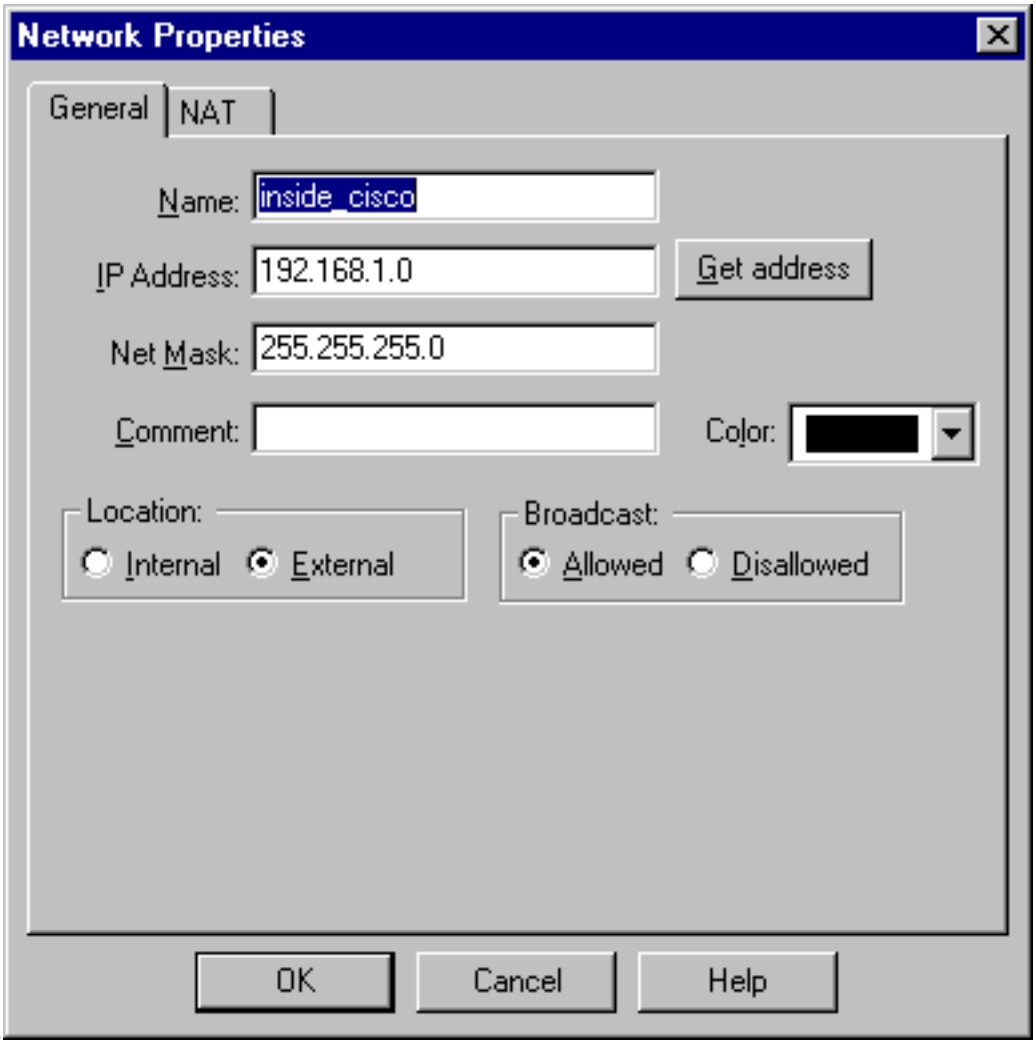
VPN.

3. Choisi **gérez > des objets de réseau > éditent** pour éditer l'objet pour point final de passerelle (point de reprise le « RTPCPVPN ») que le concentrateur VPN a dans son paramètre de pair.Sous l'emplacement, **interne** choisi. Pour le type, **passerelle** choisie. Sous des modules installés, vérifiez **VPN-1 et FireWall-1** et vérifiez la **station de**



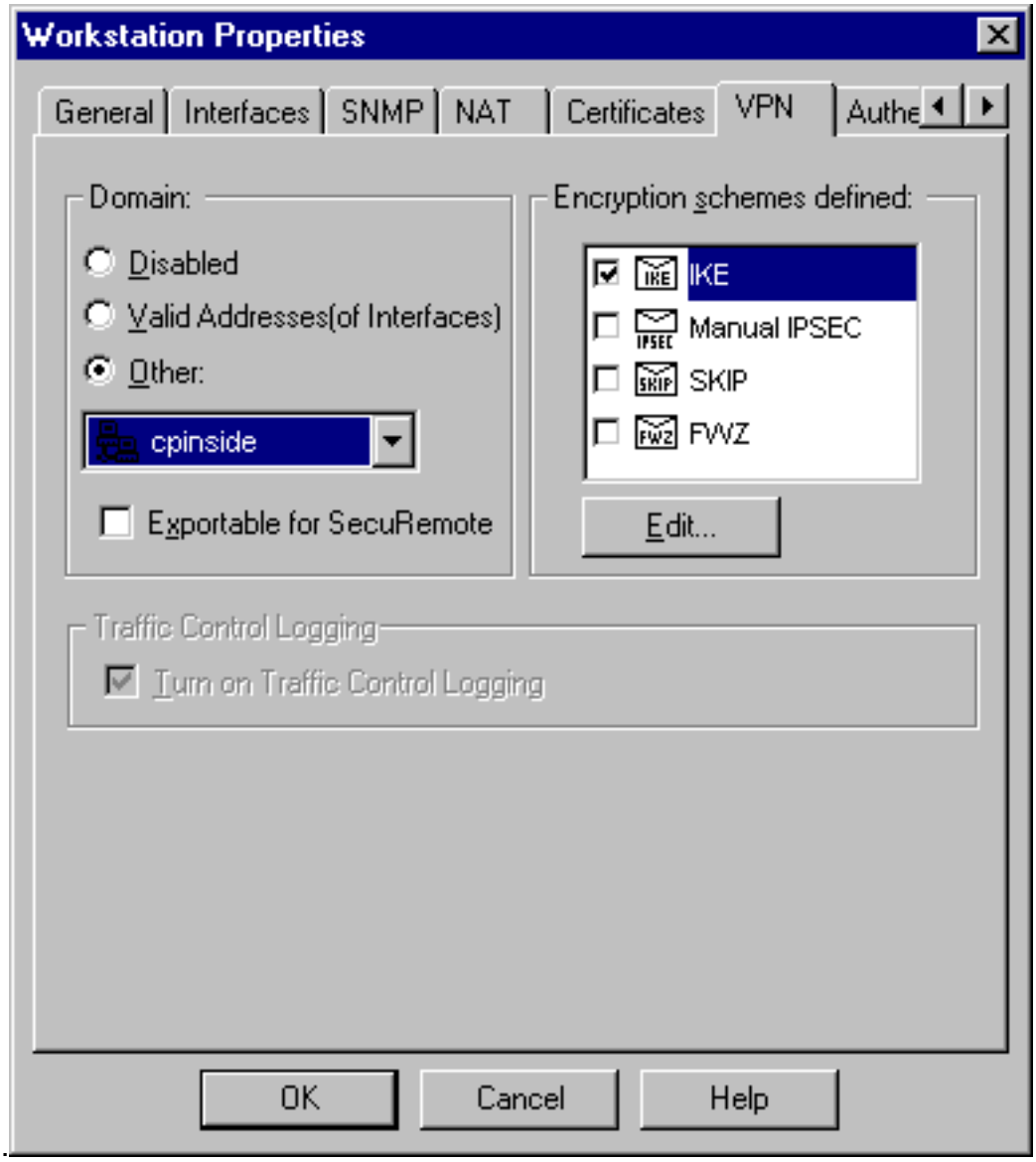
Gestion.

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 au réseau « local » dans le concentrateur



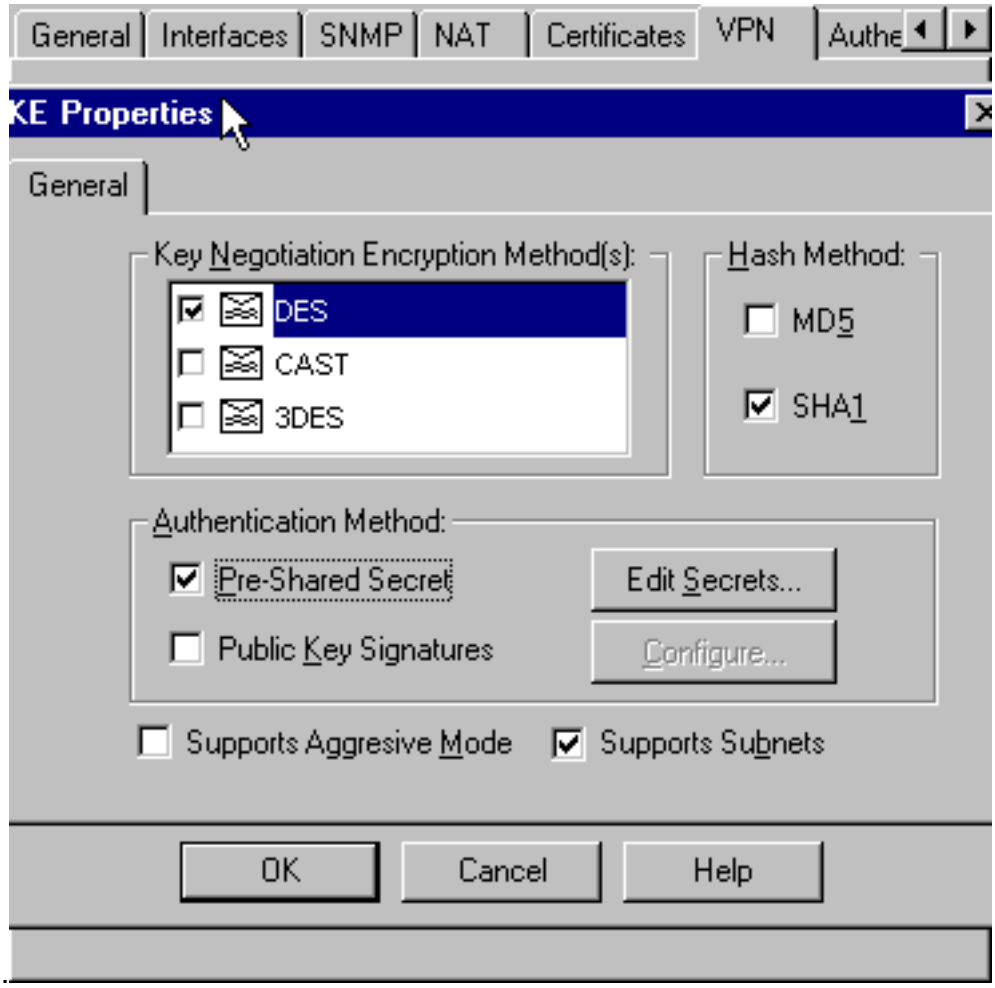
VPN.

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 interface la « publique » de concentrateur VPN.Sous l'emplacement, **externe** choisi. Pour le type, **passerelle** choisie.**Note**: Ne sélectionnez pas la case 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



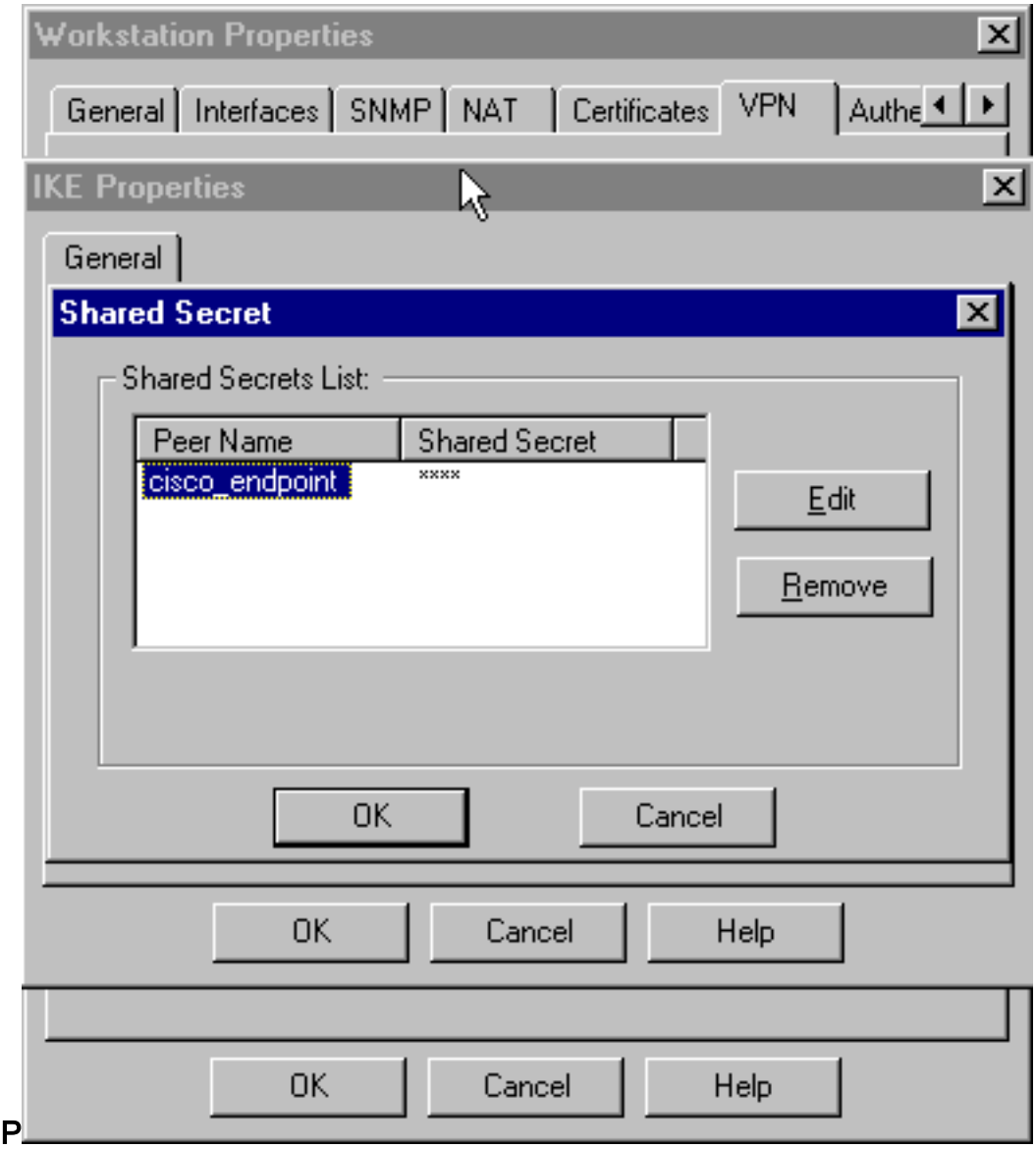
alors.

7. Changez les propriétés IKE pour le chiffrement DES pour être d'accord avec le **DES-56** et l'**algorithme de chiffrement** sur le concentrateur VPN.
8. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec l'algorithme **SHA/HMAC-160** dans le concentrateur VPN.Retirez le **mode agressif**.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à l'authentication mode de concentrateur VPN, des clés pré-



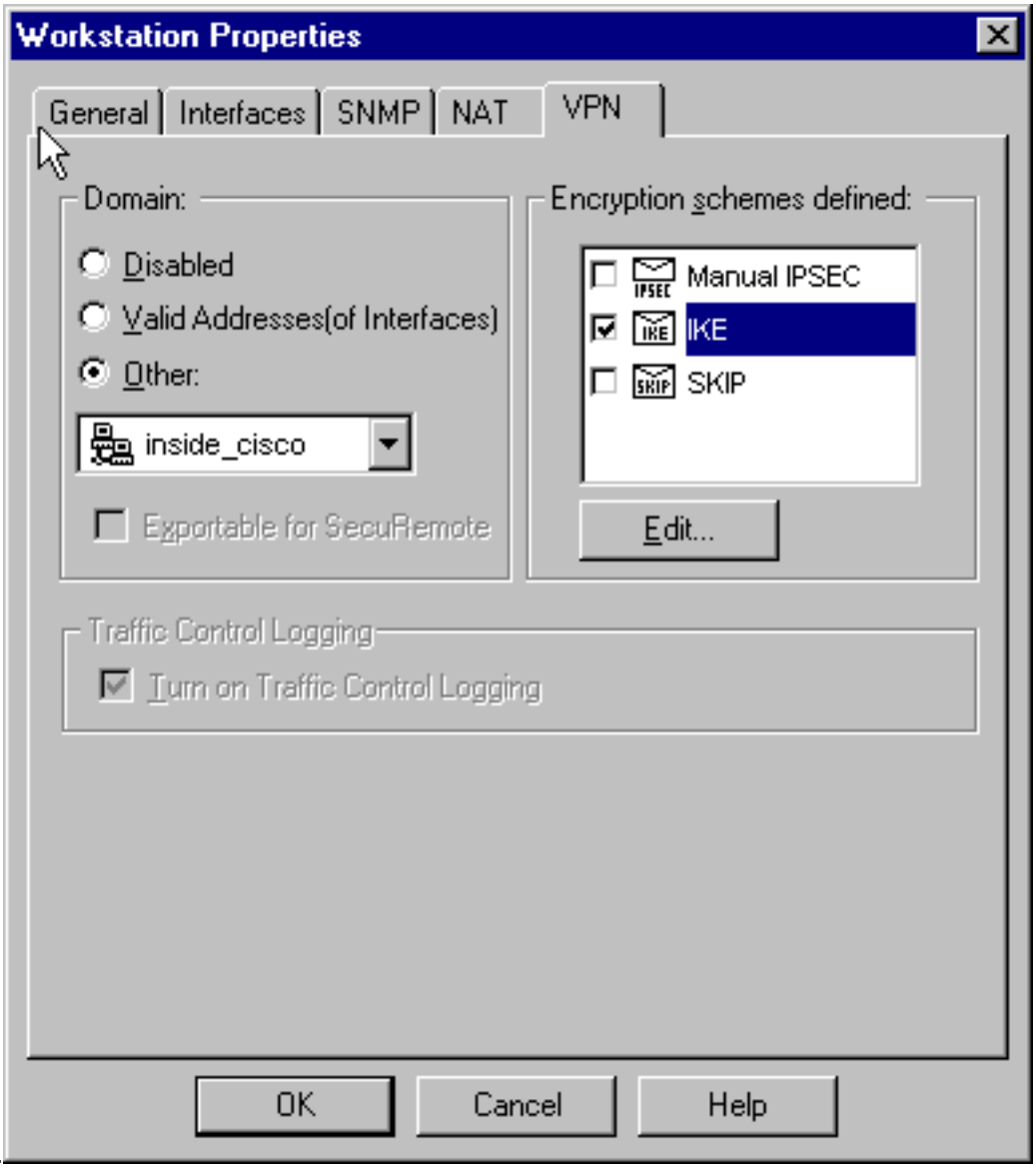
partagées.

9. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la **clé pré-partagée de** concentrateur de l'effectif VPN.**netmask principal principal de netmask d'address address**



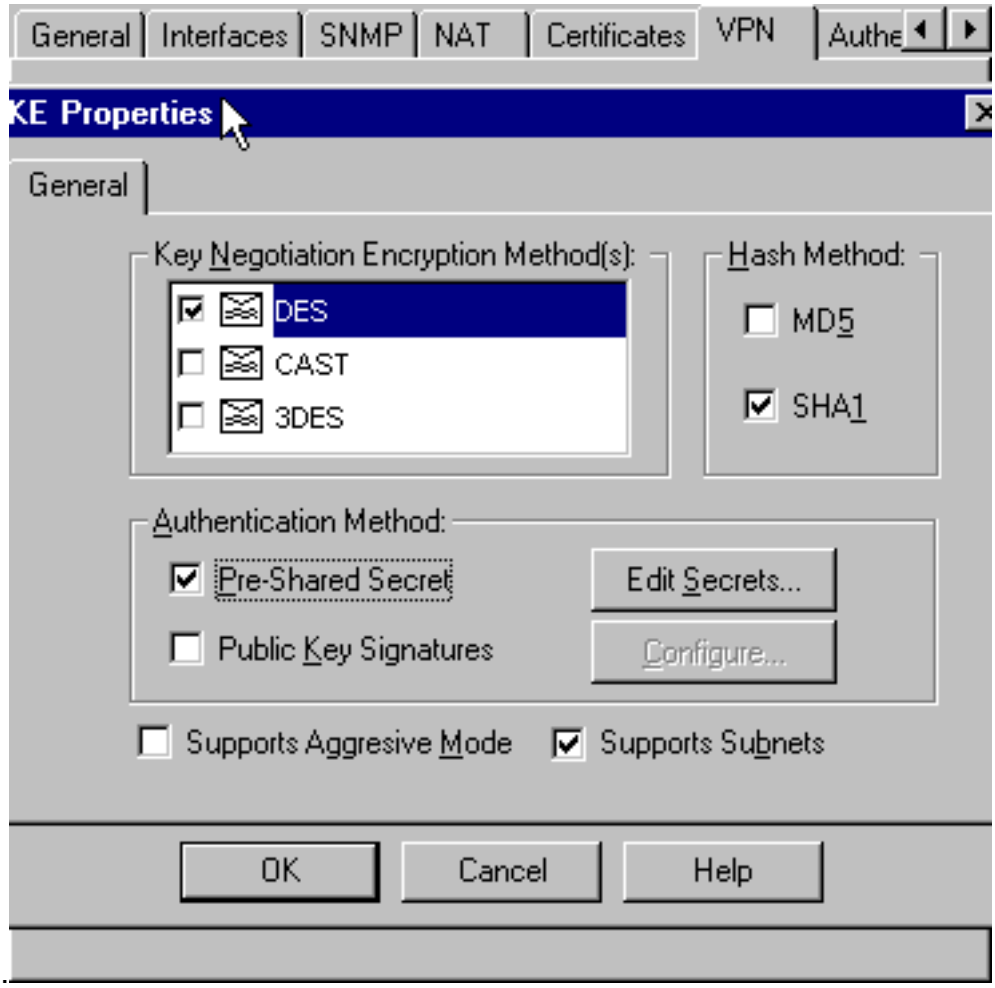
d'ISAKMP

10. 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 Cisco (appelé le « inside_cisco »). Sous des structures de chiffrement définies, l'**IKE** choisi, et cliquent sur Edit



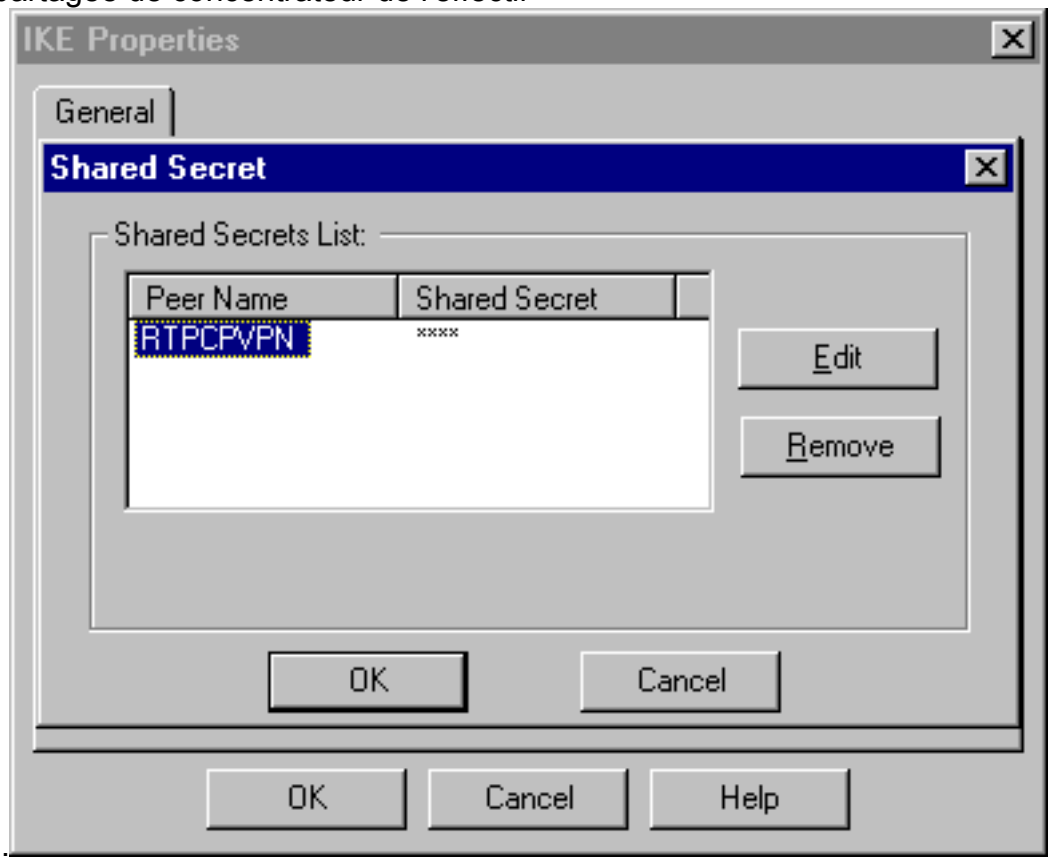
alors.

11. Changez le chiffrement DES de propriétés IKE pour être d'accord avec le **DES-56, algorithme de chiffrement** sur le concentrateur VPN.
12. Changez les propriétés IKE au hachage SHA1 pour être d'accord avec l'algorithme **SHA/HMAC-160** dans le concentrateur VPN.Changez ces configurations :**Mode de** DeselectAggressive.Le contrôle **prend en charge des sous-réseaux**.**Secret pré-partagé de** contrôle sous la méthode d'authentification. Ceci est conforme à l'authentication mode de concentrateur VPN des clés pré-



partagées.

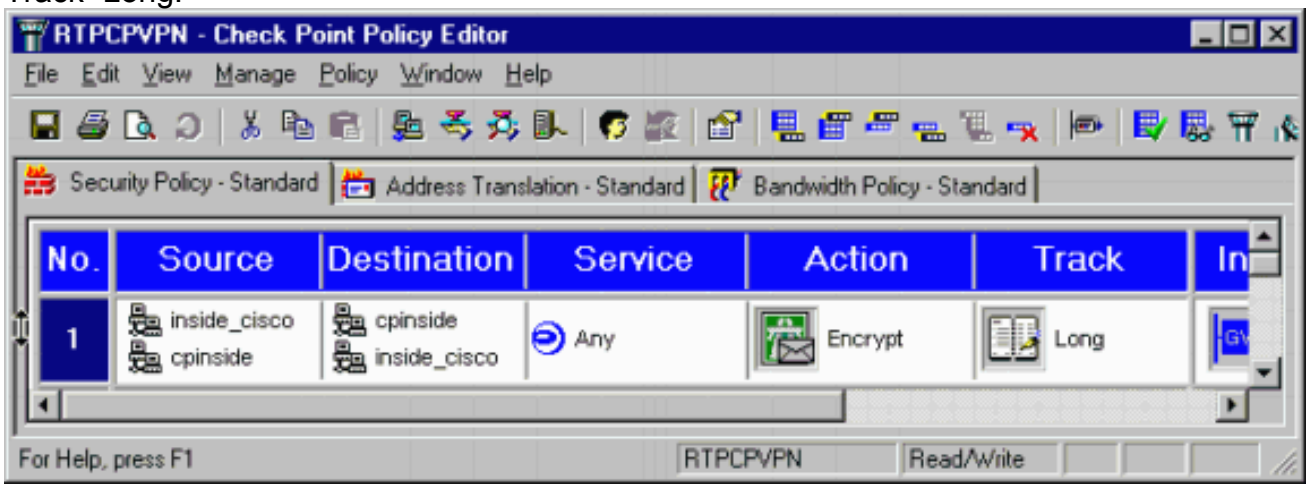
13. Cliquez sur Edit les **secrets** pour placer la clé pré-partagée pour être d'accord avec la clé pré-partagée de concentrateur de l'effectif



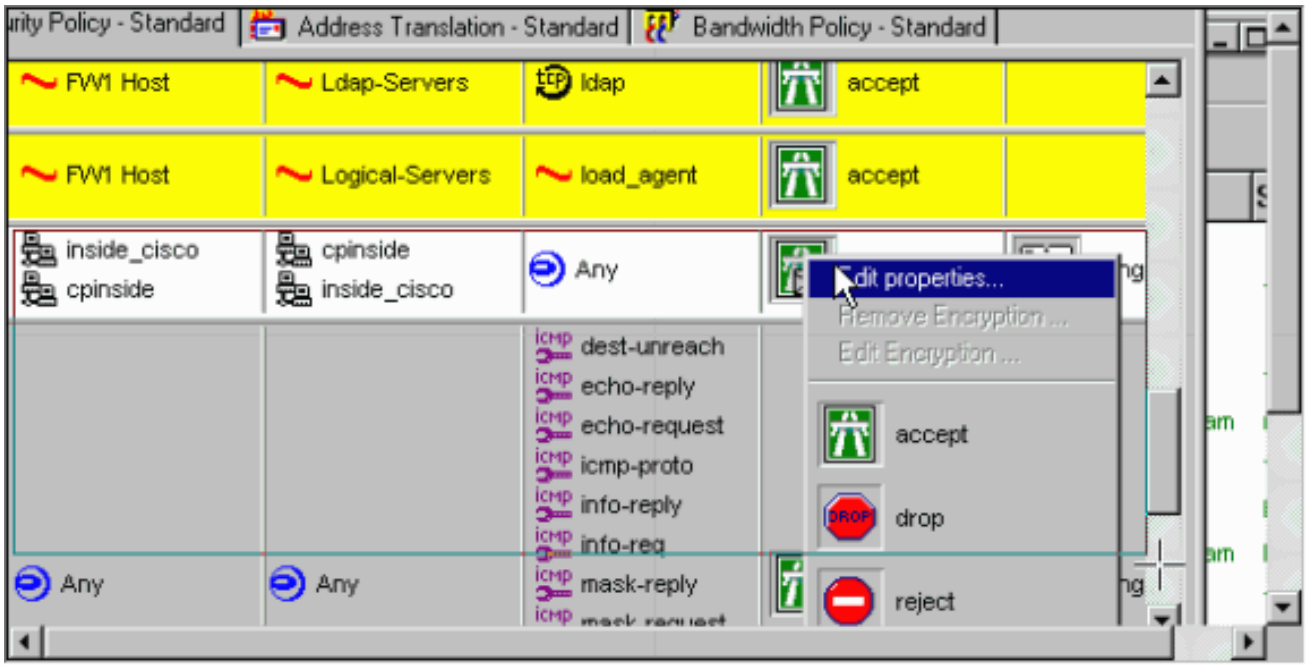
VPN.

14. 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

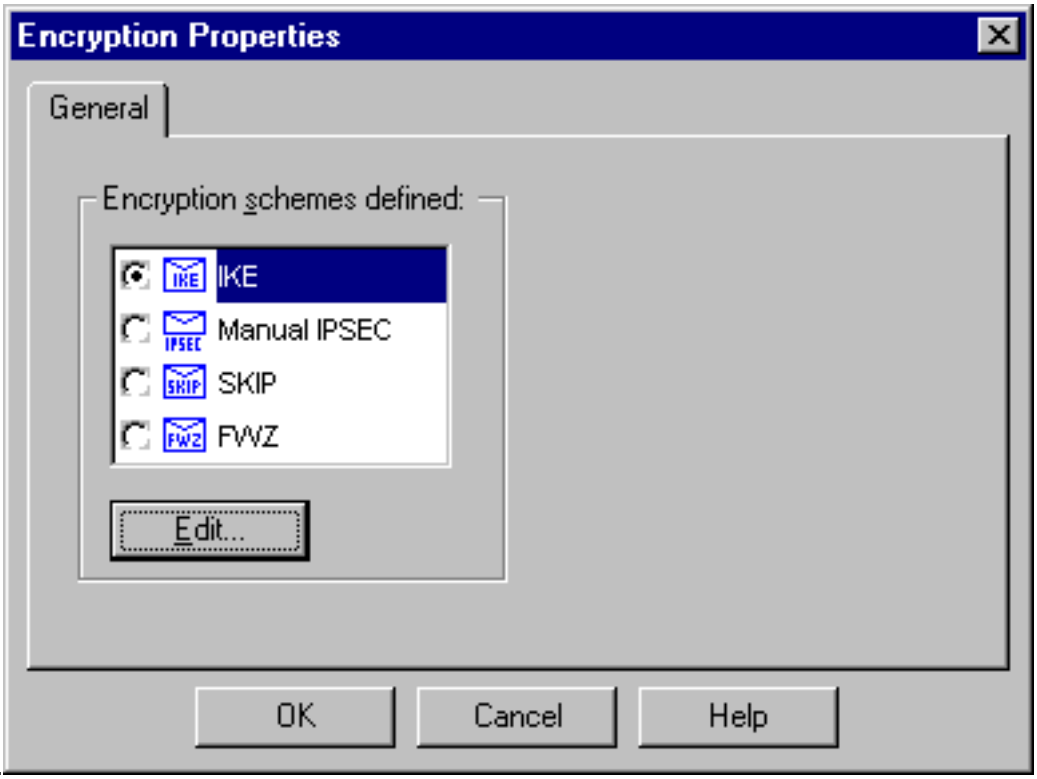
Track=Long.



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

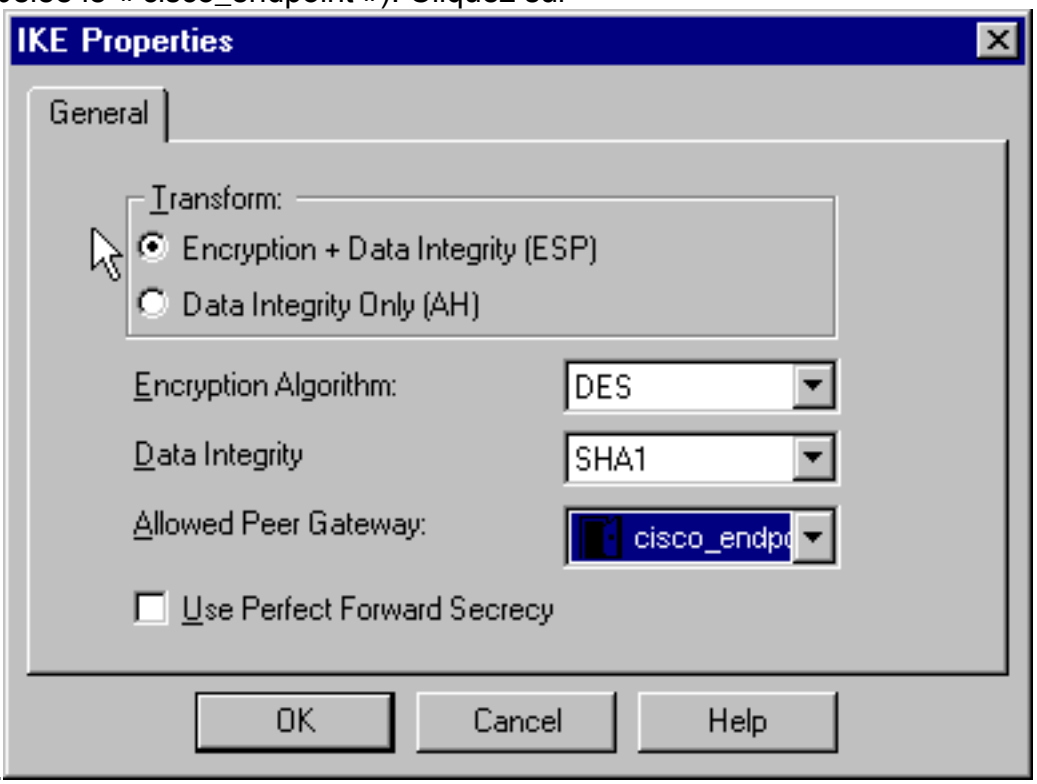


16. **L'IKE** choisi, et cliquent sur Edit



alors.

17. Sur la fenêtre de propriétés IKE, changez ces propriétés pour être d'accord avec le concentrateur IPsec VPN transforme.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 Cisco externe (appelée le « cisco_endpoint »). Cliquez sur



OK.

18. 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

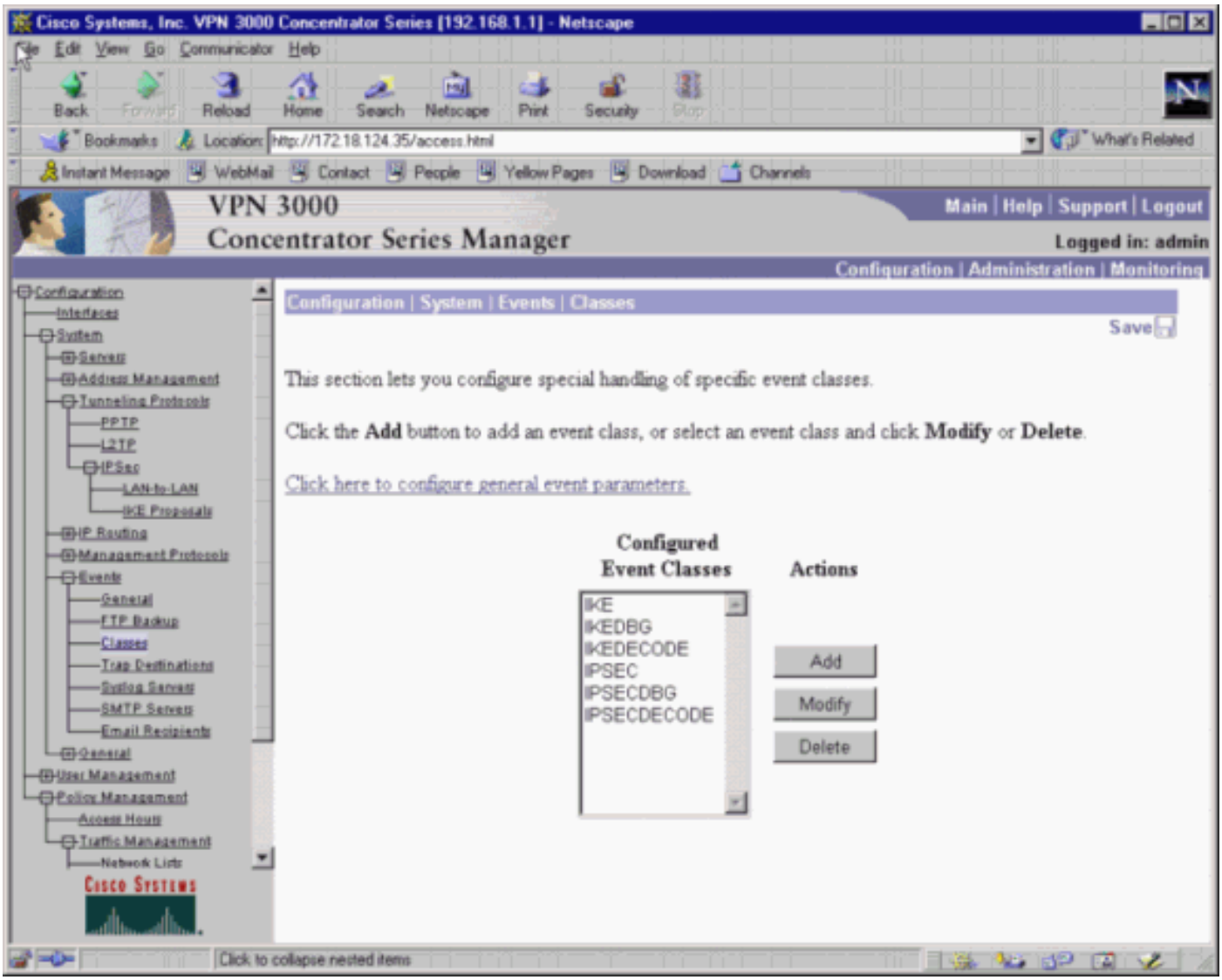
Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

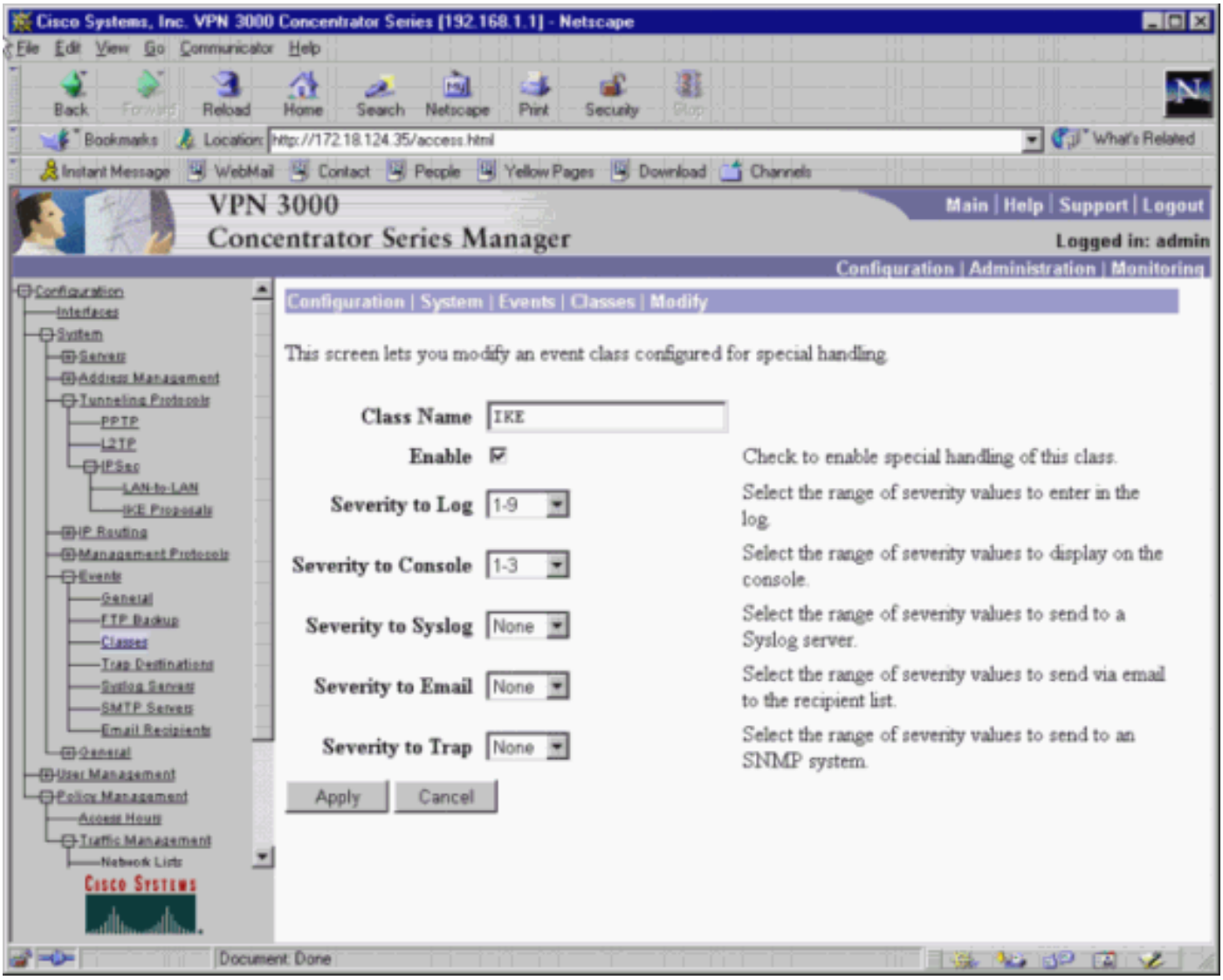
Récapitulation de réseau

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.

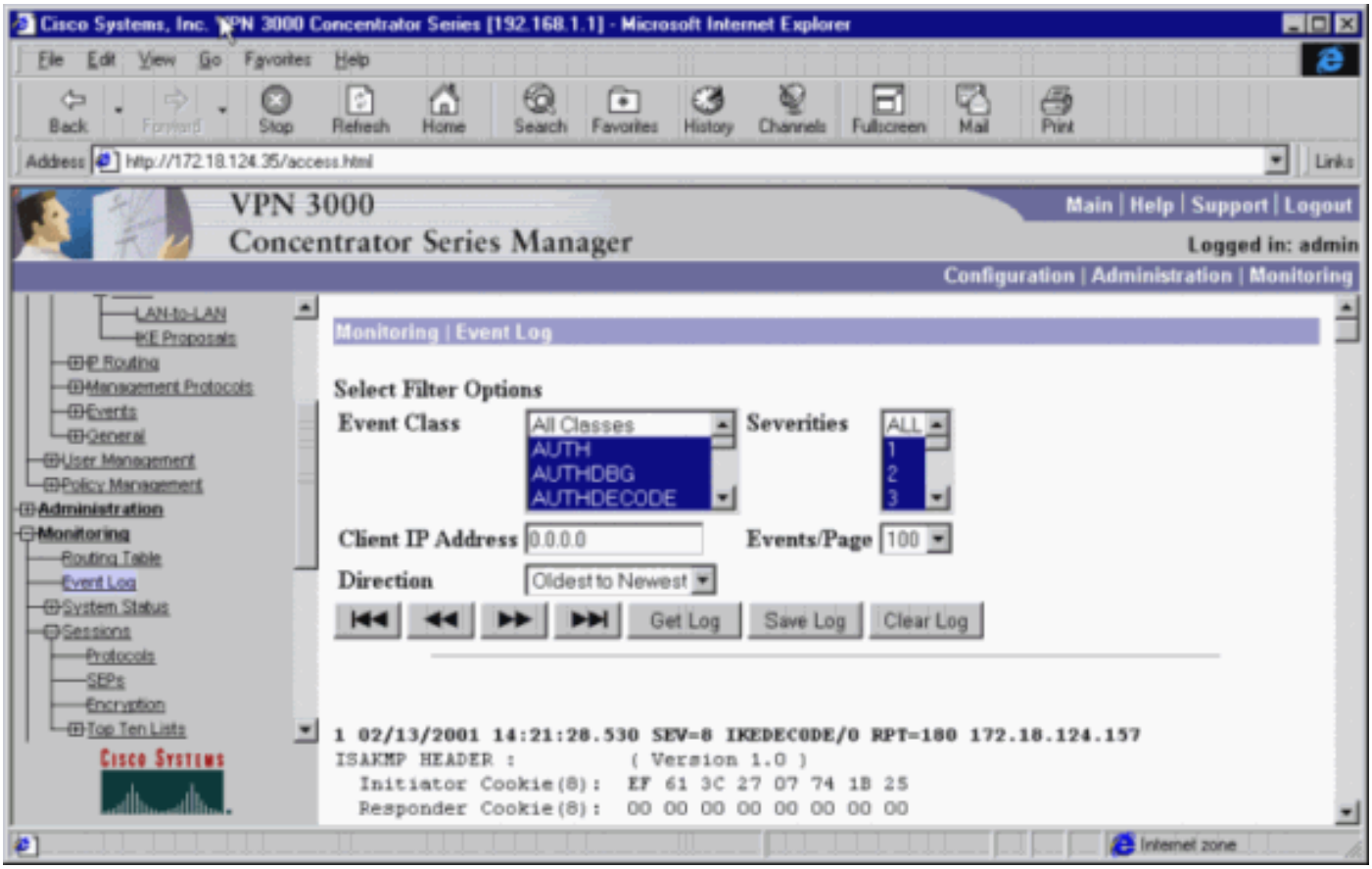
Debug de concentrateur VPN 3000

Le concentrateur possible VPN met au point incluent l'IKE, IKEDBG, IKEDECODE, IPSEC, IPSECDBG, IPSECDECODE. Ceci est installé dans la **configuration > le système > les événements > les classes**.

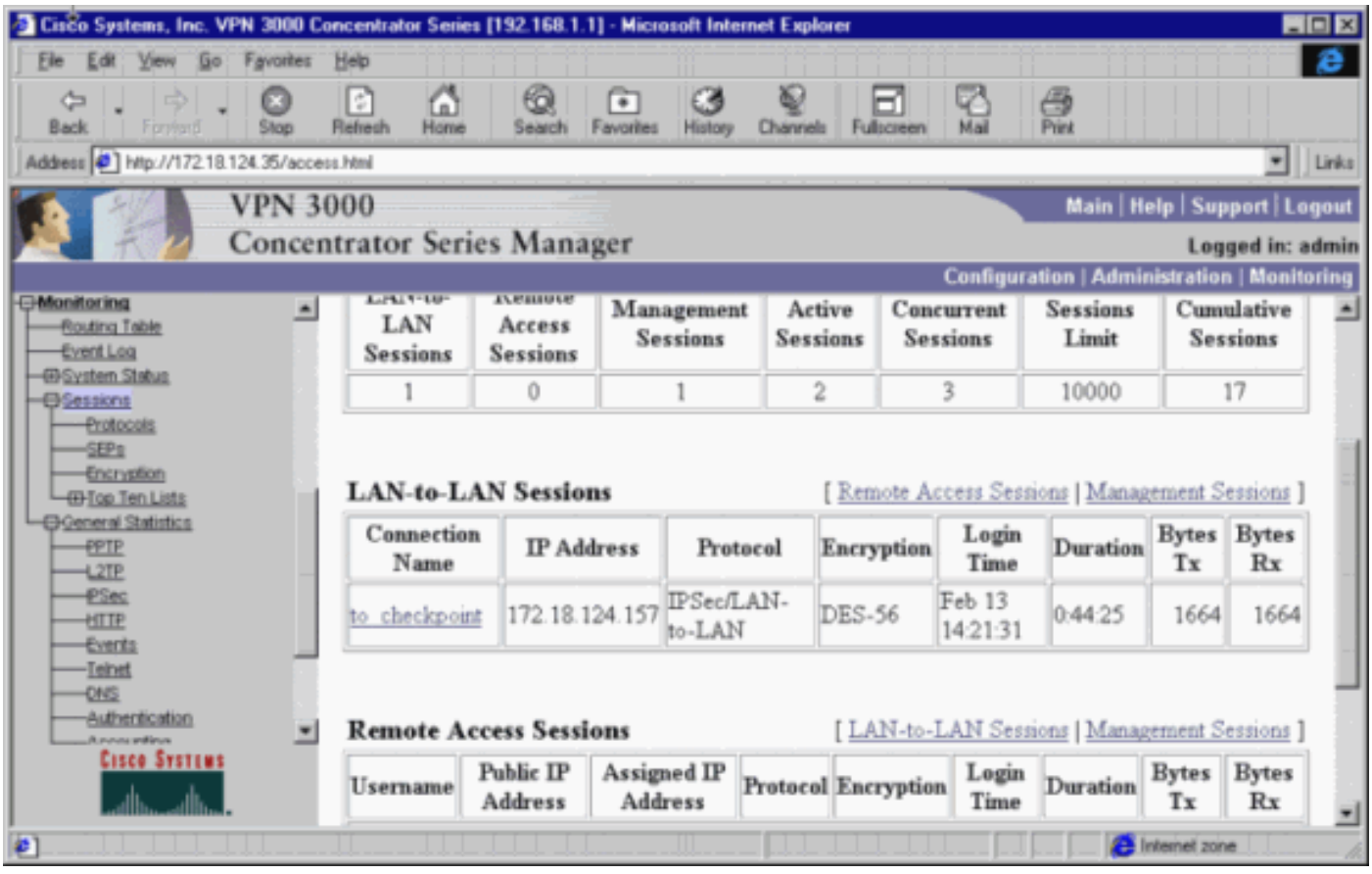




Vous pouvez visualiser met au point dans la **surveillance > le journal d'événements > obtenez le log**.



Monitoring > Sessions choisi pour surveiller le trafic de tunnel entre réseaux locaux.



La gestion choisie **> gèrent des sessions > des sessions entre réseaux locaux > des actions - déconnectez-vous** pour effacer le tunnel.

Debug de pare-feu Checkpoint 4.1

Note: 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, refusé le trafic devrait apparaître en rouge dans le visualiseur de log. Plus bavard mettez au point peut être obtenu avec :

```
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'effacer 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

Concentrateur Cisco VPN 3000

```
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
```

Informations connexes

- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems