# Configuration de la transmission tunnel partagée pour les clients VPN sur l'ASA

## Table des matières



## Introduction

Ce document décrit le processus permettant aux clients VPN d'accéder à Internet tout en effectuant une tunnellisation vers un dispositif de sécurité de la gamme Cisco ASA 5500.

## Conditions préalables

### Exigences

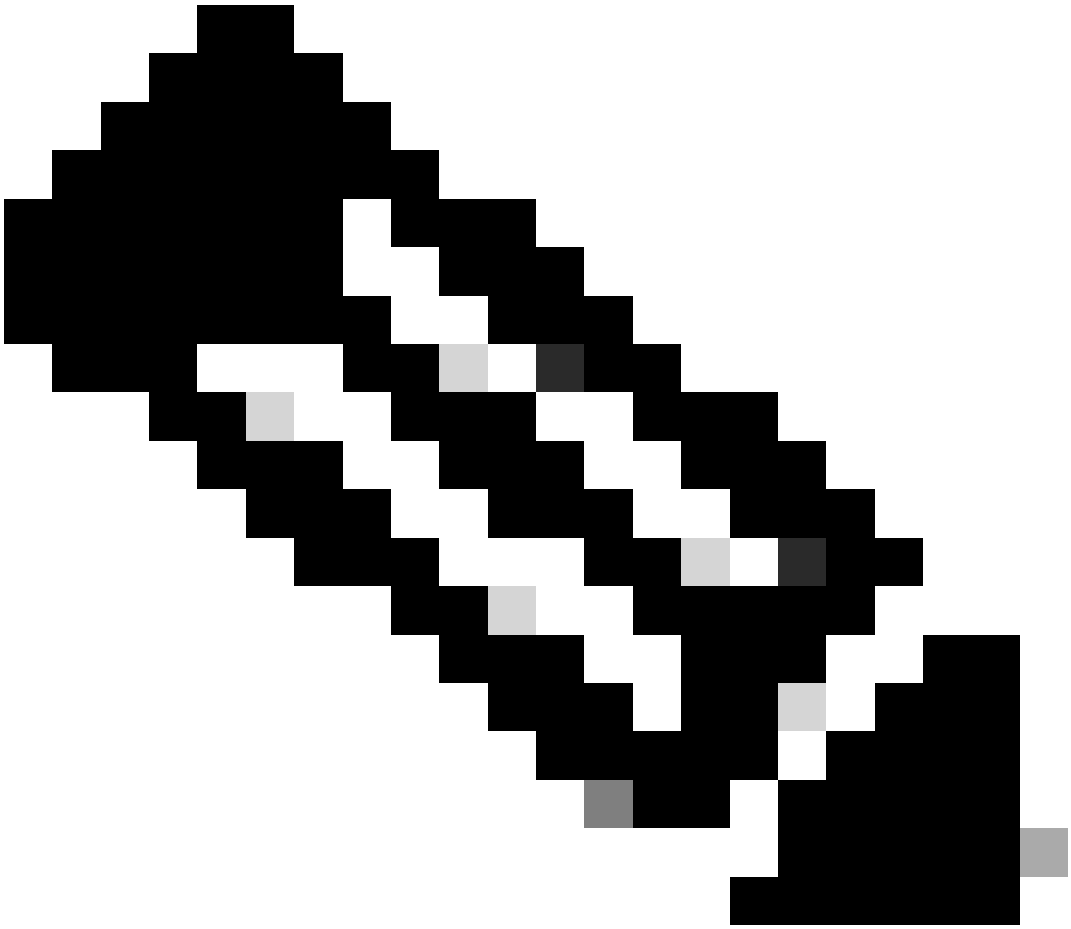
Ce document suppose qu'une configuration de VPN d'accès à distance opérationnelle existe déjà sur l'ASA. Référez-vous à Exemple de configuration de PIX/ASA 7.x comme serveur VPN distant avec l'ASDM si cette configuration n'est pas encore effectuée.

### Composants utilisés

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

- Logiciel du dispositif de sécurité de la gamme Cisco ASA 5500 version 7.x et ultérieures
- Client VPN version 4.0.5 de Cisco Systems
- Adaptive Security Device Manager (ASDM)

---



> Remarque : ce document contient également la configuration CLI PIX 6.x qui est compatible avec le client VPN Cisco 3.x.

---

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Diagramme du réseau

Le client VPN est situé sur un réseau SOHO standard et se connecte à travers l'Internet au bureau central.

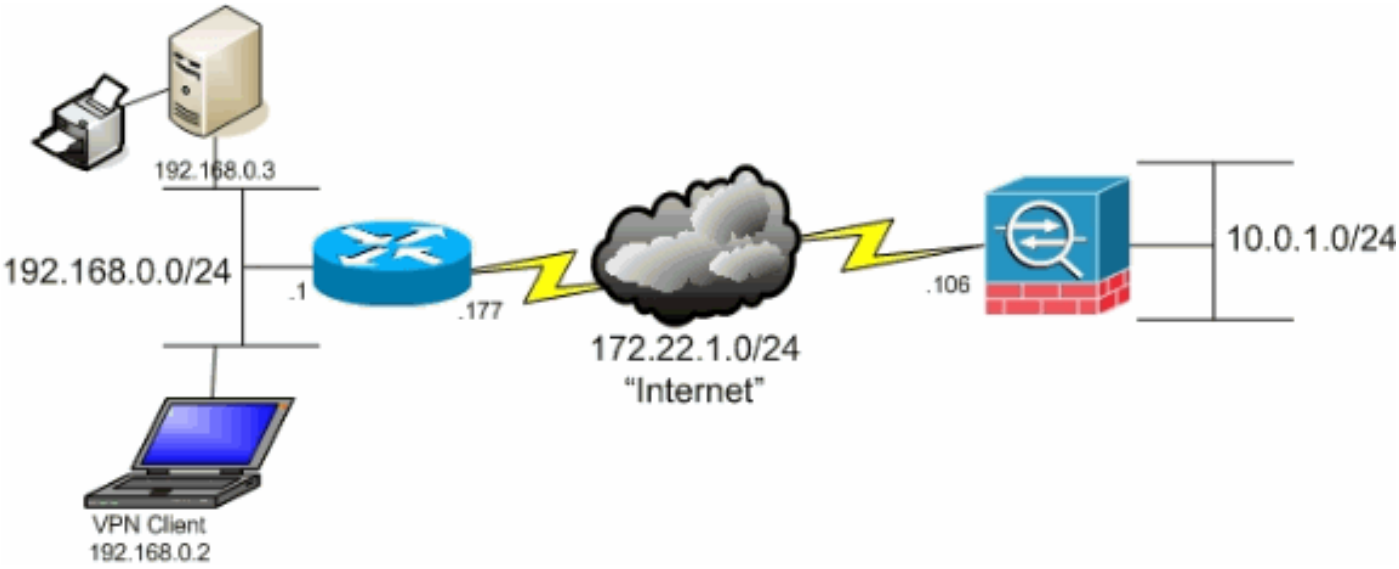



Diagramme du réseau

### Produits connexes

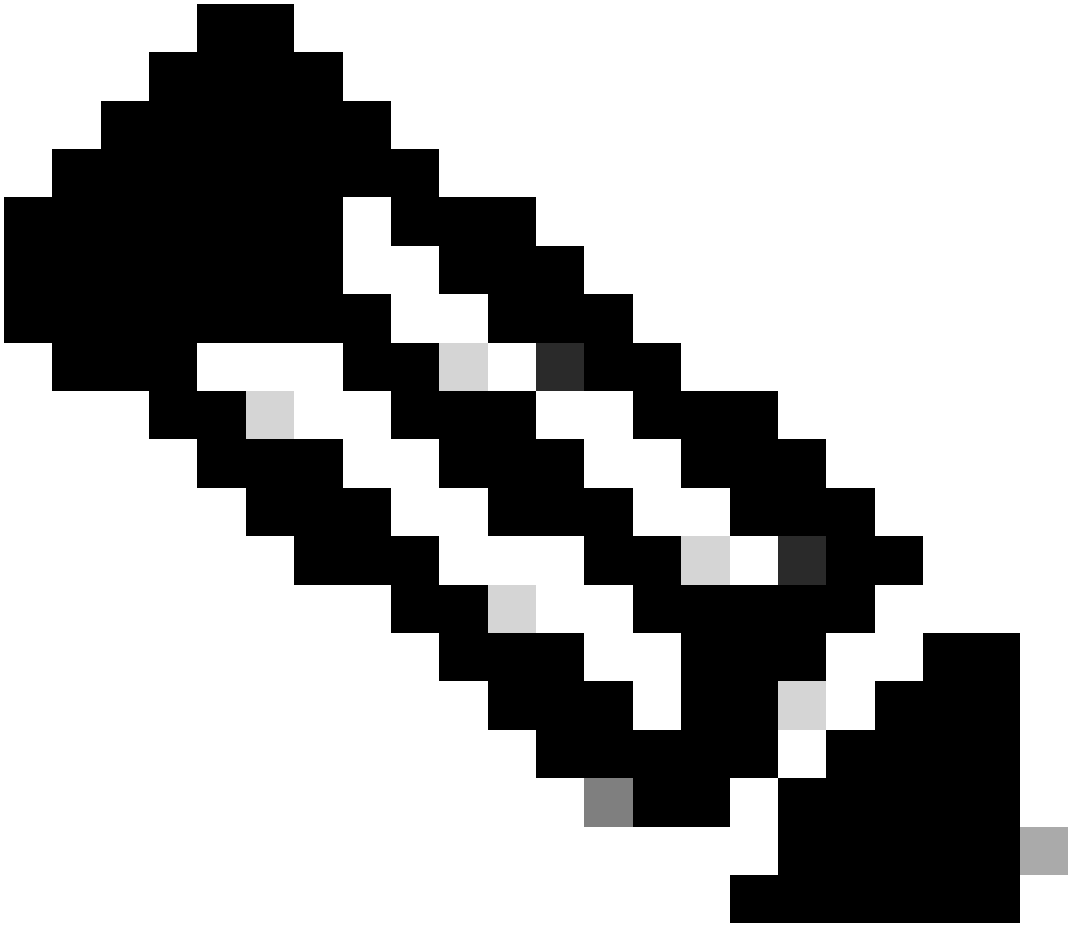
Cette configuration peut également être utilisée avec le logiciel du dispositif de sécurité de la gamme Cisco PIX 500 version 7.x et ultérieures.

### Conventions

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

## Informations générales

Ce document fournit des instructions pas à pas sur la façon d'autoriser l'accès des clients VPN à l'Internet tandis qu'ils sont reliés par tunnel à un dispositif de sécurité adaptatif dédié de la gamme Cisco ASA 5500. Cette configuration offre aux clients VPN un accès sécurisé aux ressources de l'entreprise par l'intermédiaire d'IPsec tout en bénéficiant d'un accès non sécurisé à 'Internet.



Remarque : la transmission tunnel complète est considérée comme la configuration la plus sécurisée, car elle n'autorise pas l'accès simultané des périphériques à Internet et au réseau local de l'entreprise. Un compromis entre tunnellisation complète et split tunneling permet aux clients VPN d'accéder au LAN local uniquement. Référez-vous à Exemple de configuration de PIX/ASA 7.x : Allow Local LAN Access for VPN Clients pour plus d'informations.

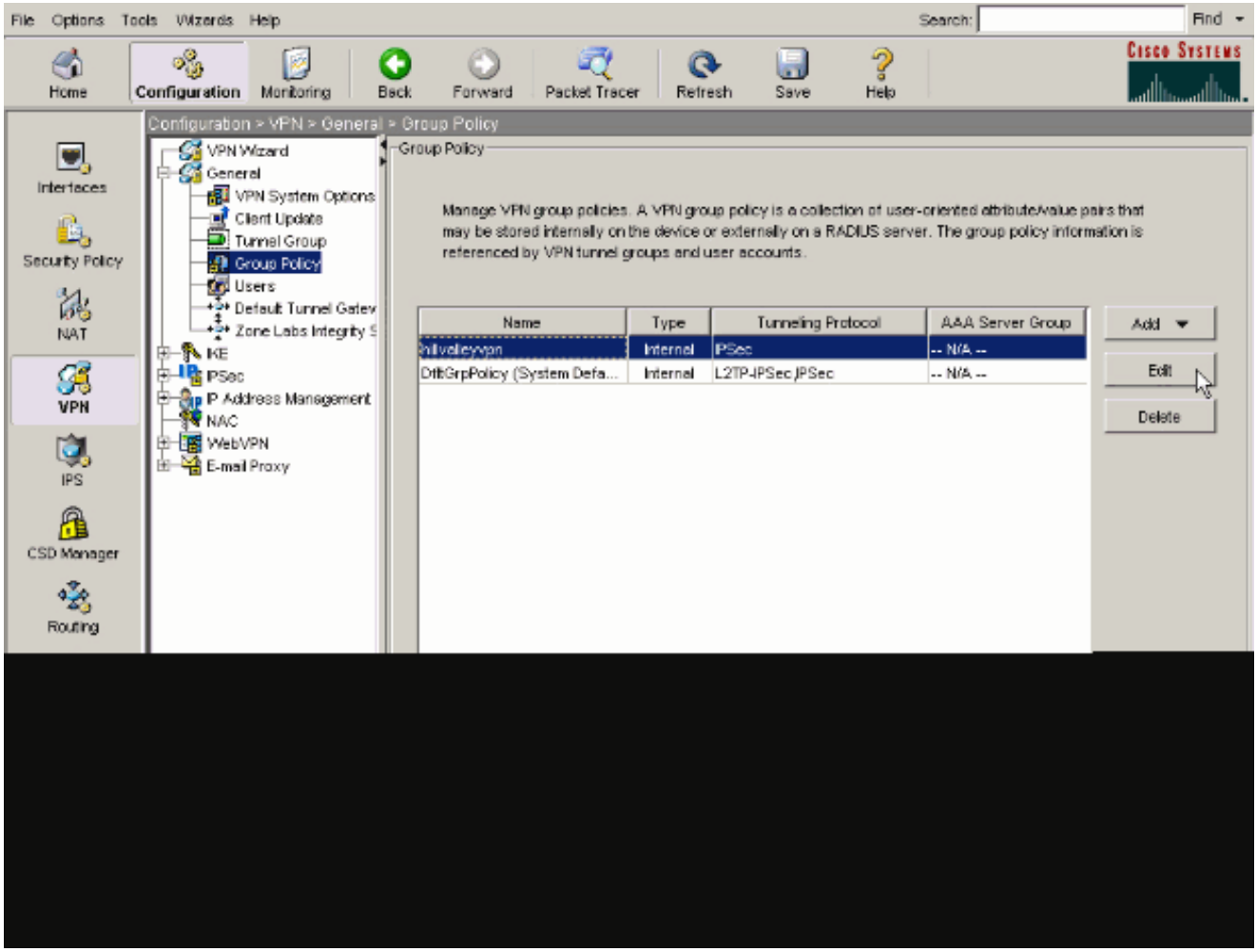
Dans un scénario de connexion de base d'un client VPN à ASA, tout le trafic provenant du client VPN est crypté et envoyé à ASA quelle que soit sa destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande passante. La transmission tunnel partagée peut aider à résoudre ce problème puisqu'elle permet aux utilisateurs de n'envoyer que le trafic qui est destiné au réseau de l'entreprise à travers le tunnel. Tout autre trafic, comme la messagerie instantanée, l'email, ou la navigation occasionnelle, est envoyé à l'Internet par l'intermédiaire du LAN local du client VPN.

## Configurer la transmission tunnel partagée sur ASA

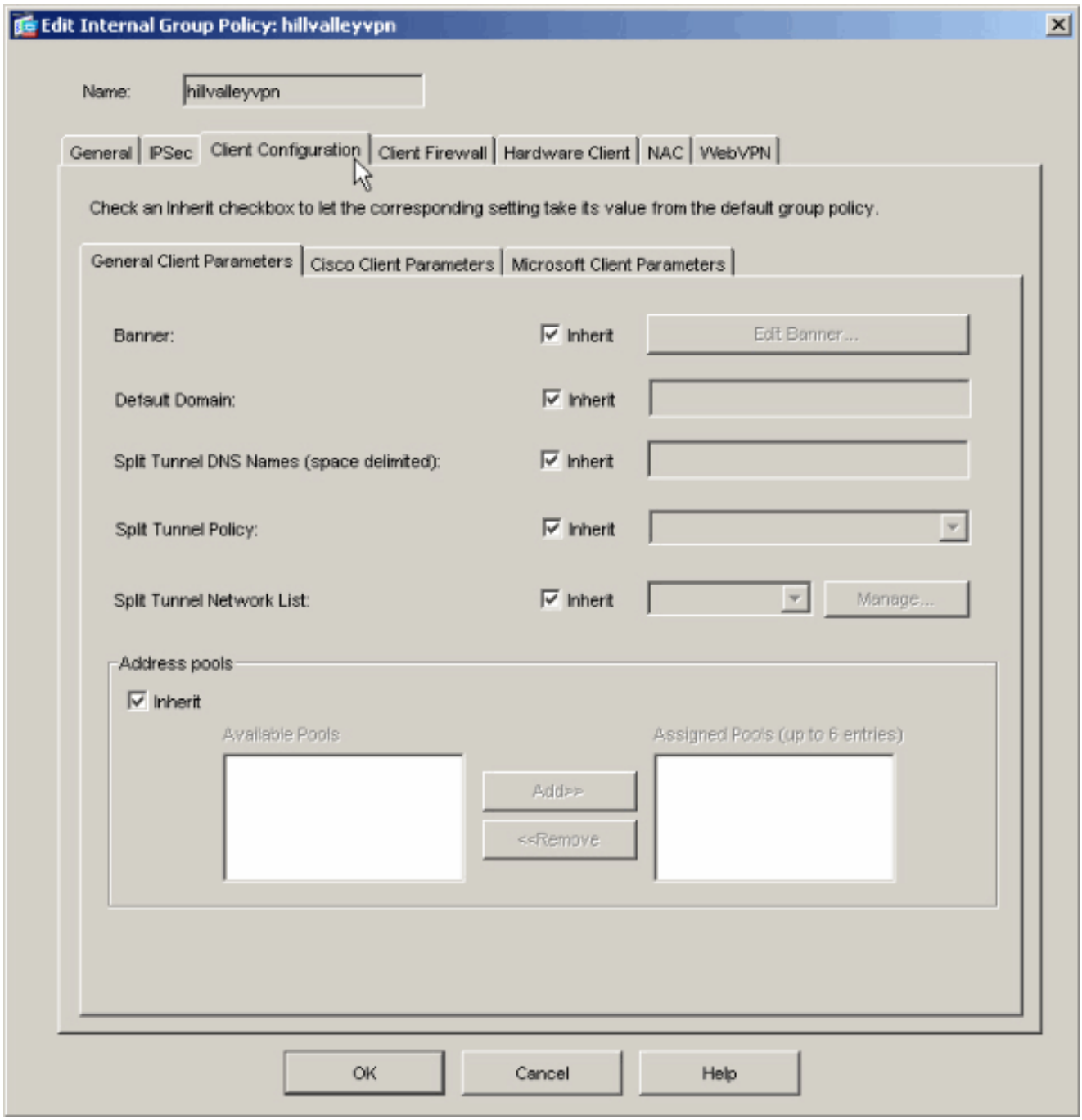
## Configurer ASA 7.x avec l'Adaptive Security Device Manager (ASDM) 5.x

Complétez ces étapes afin de configurer votre groupe de tunnels de façon à permettre la transmission tunnel partagée pour les utilisateurs du groupe.

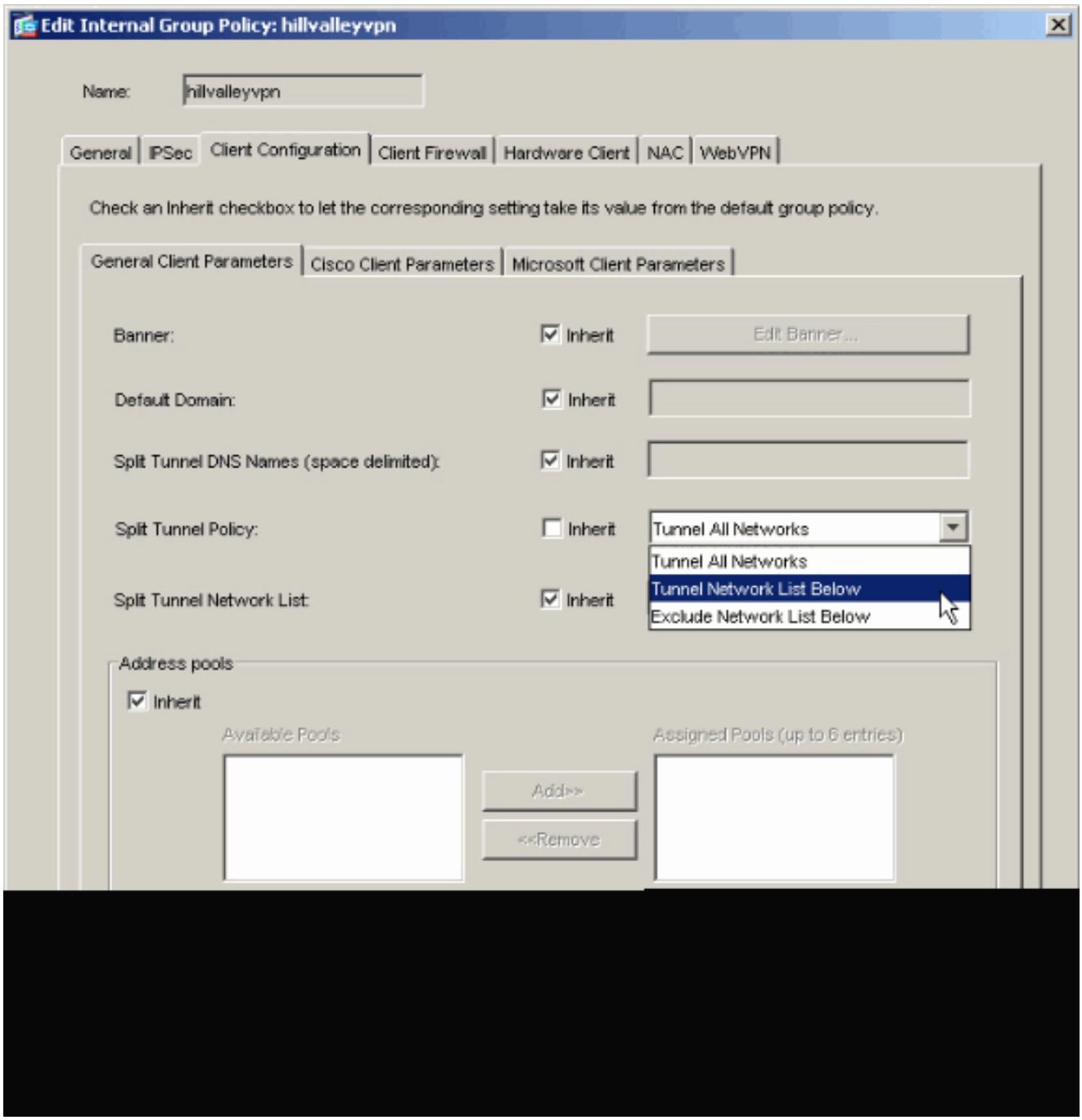
1. Choisissez Configuration > VPN > General > Group Policy et sélectionnez la stratégie de groupe dans laquelle vous souhaitez activer l'accès au LAN local. Cliquez alors sur Edit.




2. Accédez à l'onglet Client Configuration.

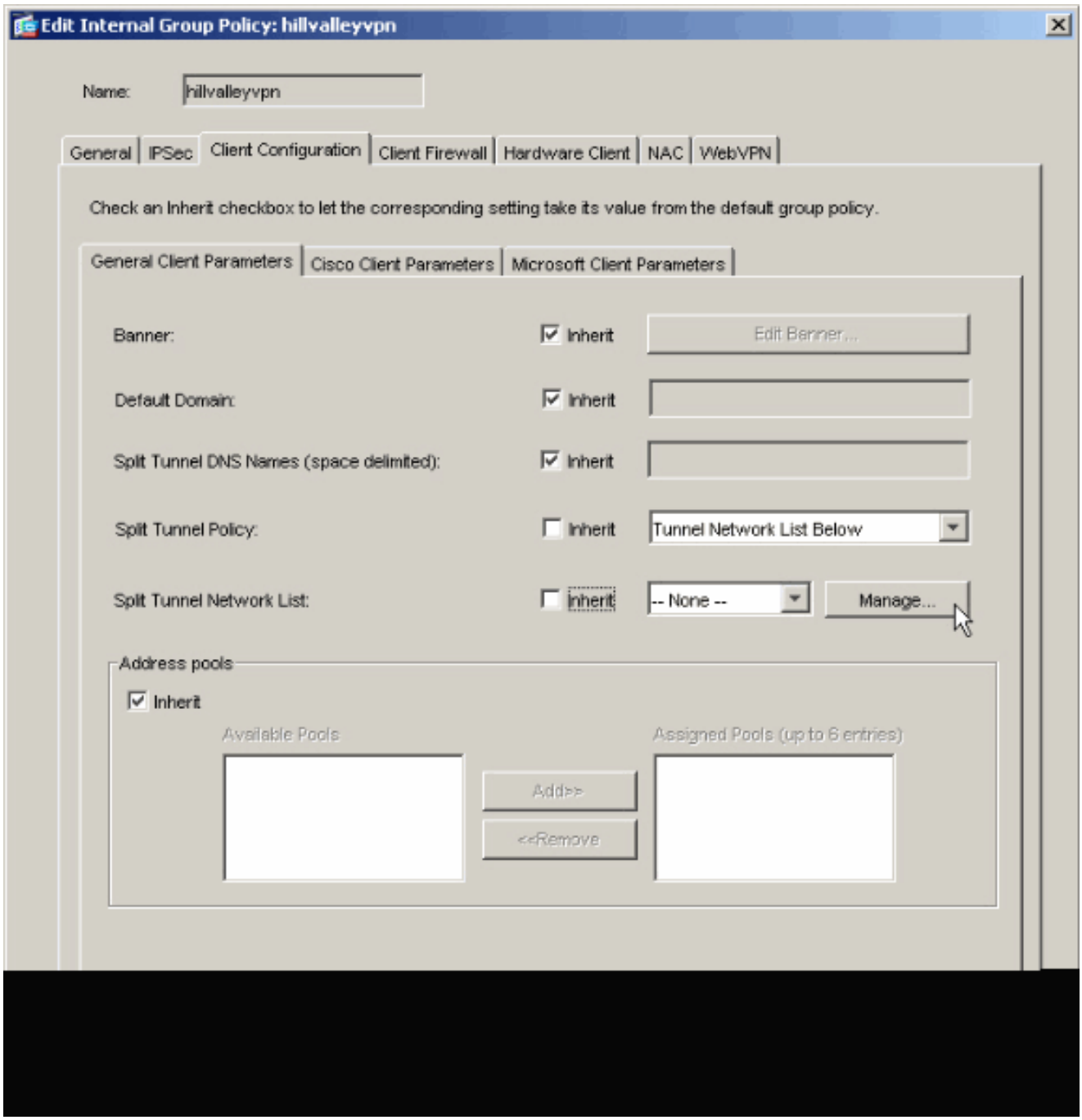



3. Décochez la case Inherit pour Split Tunnel Policy et choisissez Tunnel Network List Below ..



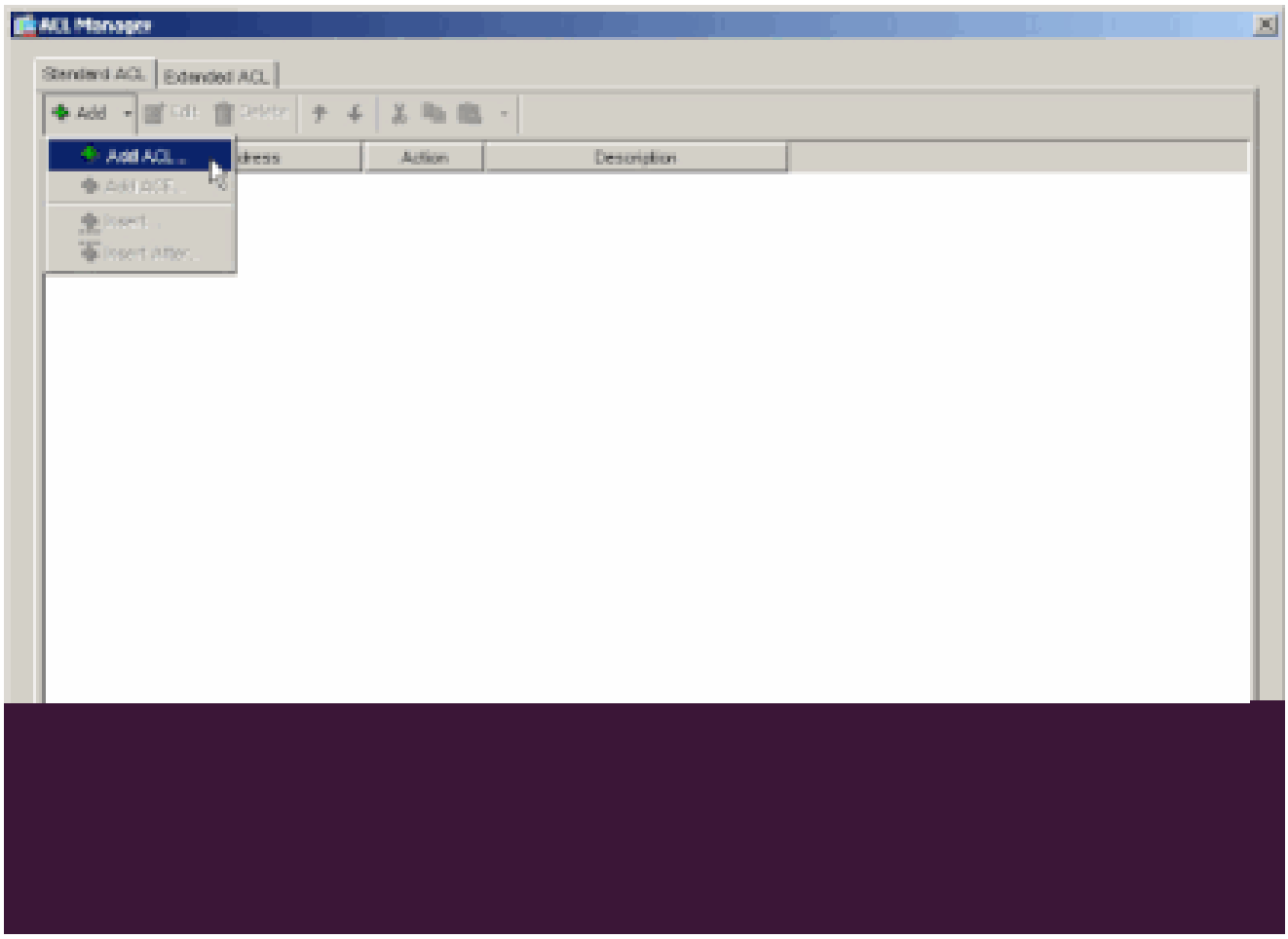

•

Désactivez la case Inherit pour la liste Split Tunnel Network List, puis cliquez sur Manage pour lancer l'ACL Manager.



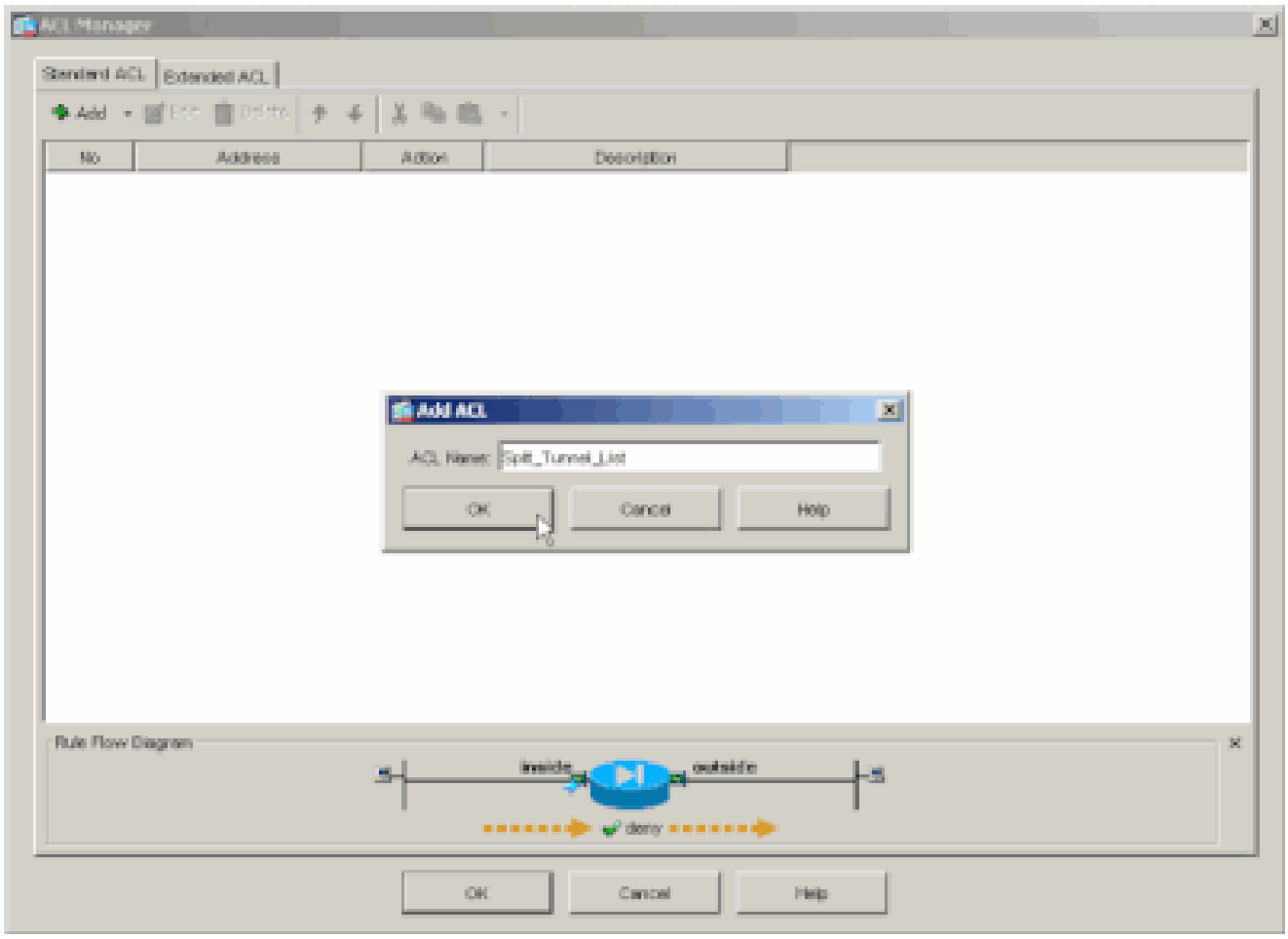

•

Dans le gestionnaire de listes de contrôle d’accès (ACL), choisissez « Add > Add ACL... » (ajouter > ajouter une ACL...) pour créer une nouvelle liste d’accès.



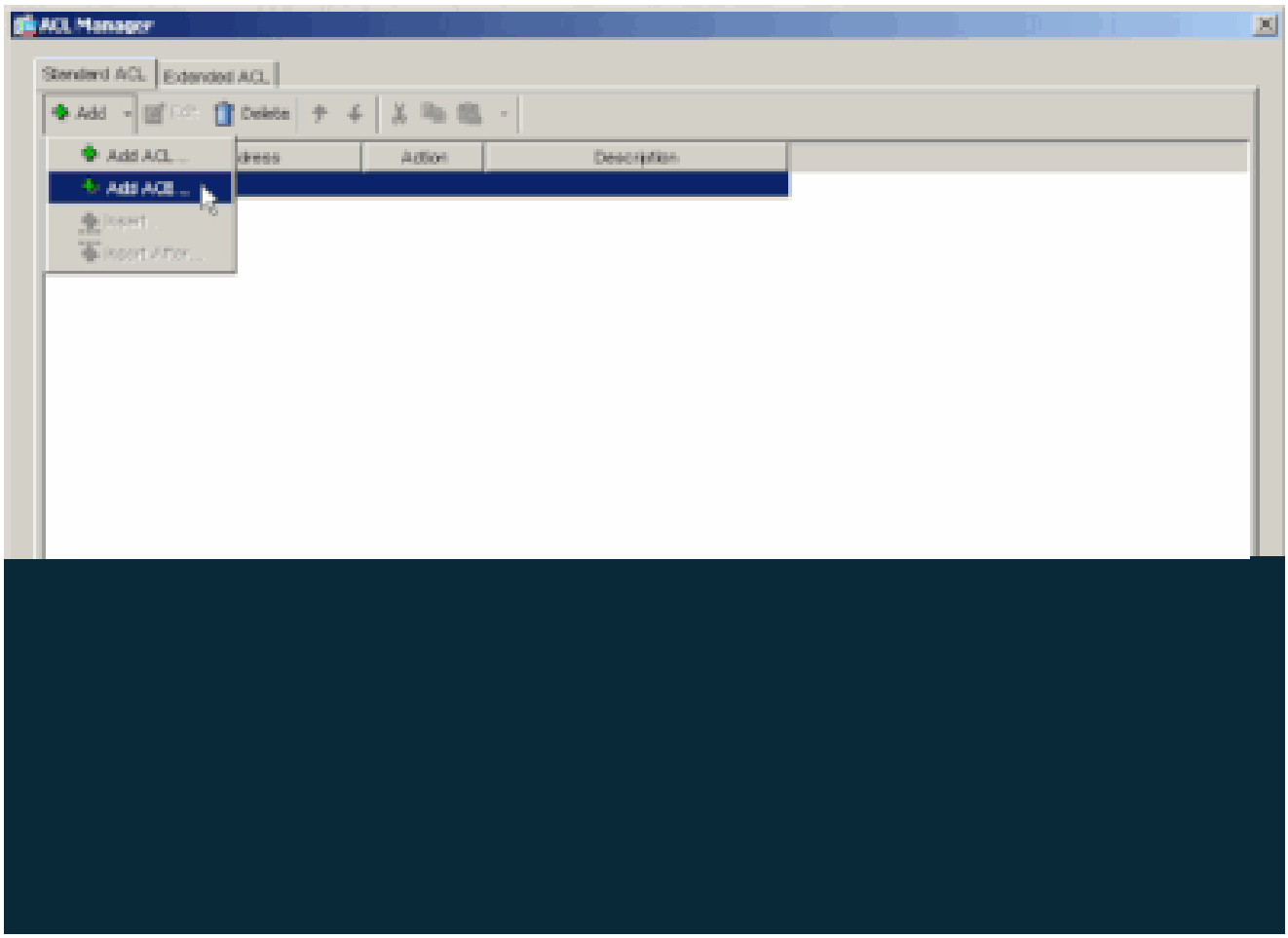

•

Fournissez un nom pour l'ACL et cliquez sur **OK.**




•

Une fois la liste de contrôle d'accès créée, choisissez **Add > Add ACE. .**afin d'ajouter une entrée de contrôle d'accès (ACE).




•

Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.0.1.0/24.

a.

Choisissez Permit.

b.

Choisissez une adresse IP 10.0.1.0

c.

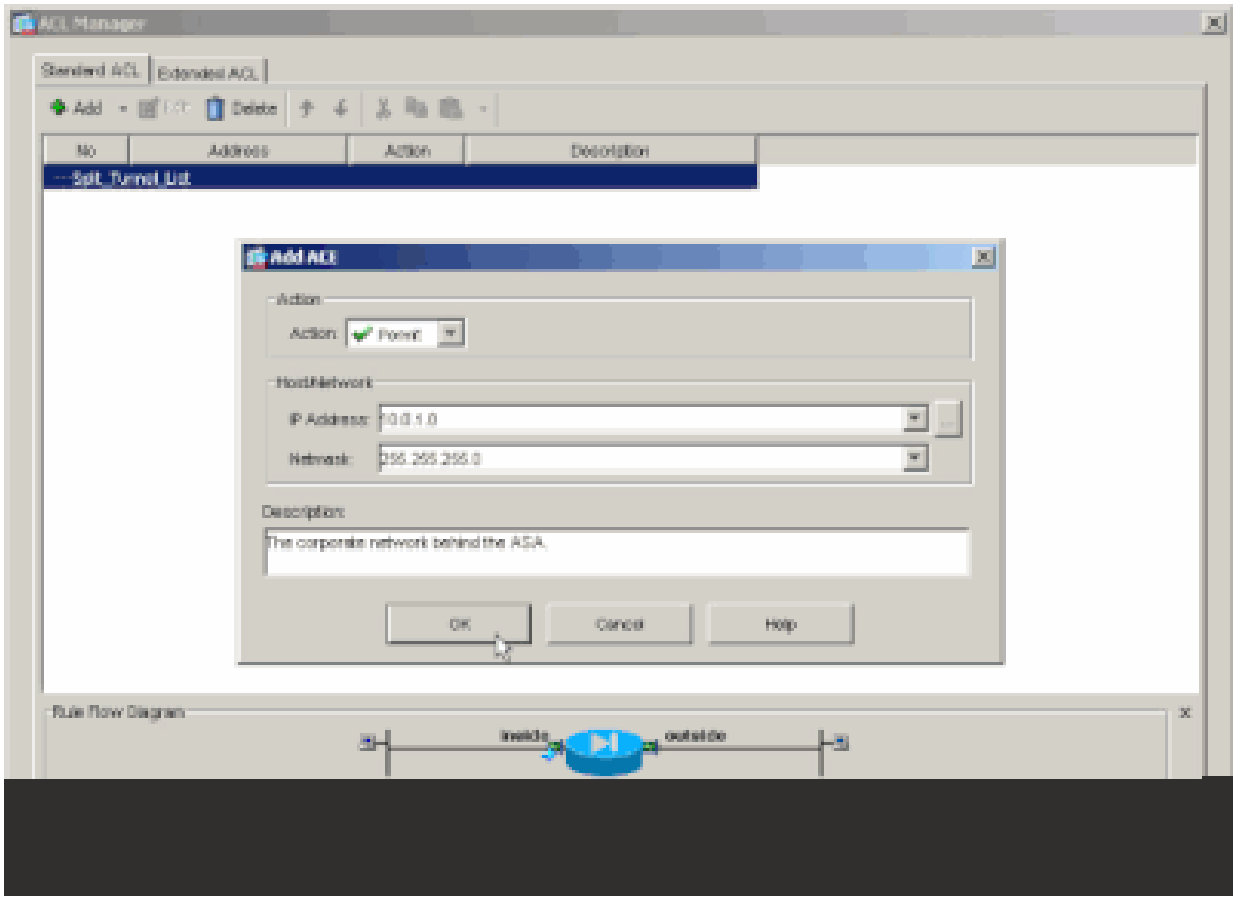
Choisissez un masque de réseau **255.255.255.0.**

d.

*(Facultatif) Fournissez une description.*

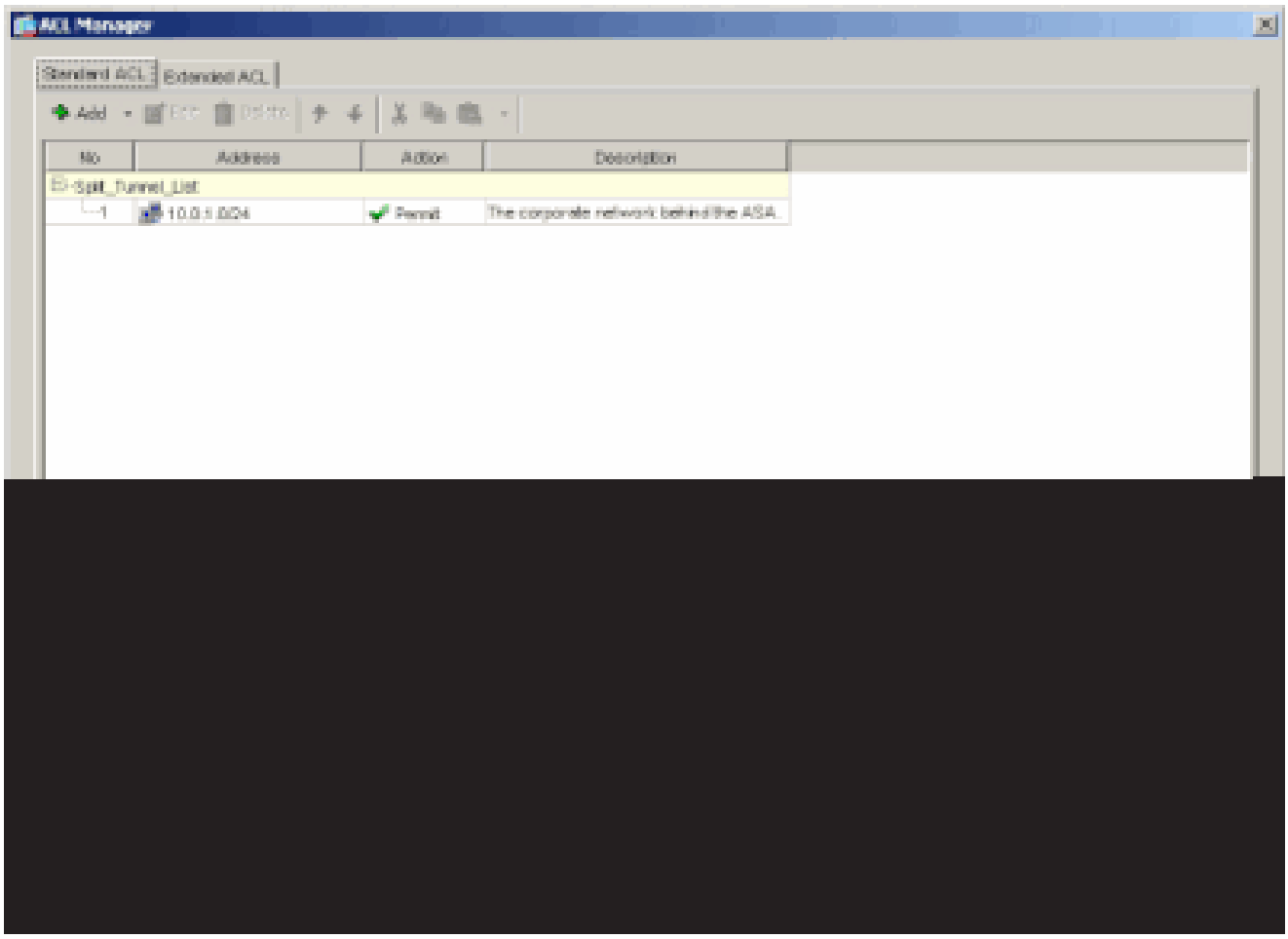
e.

Cliquez sur > **OK**.



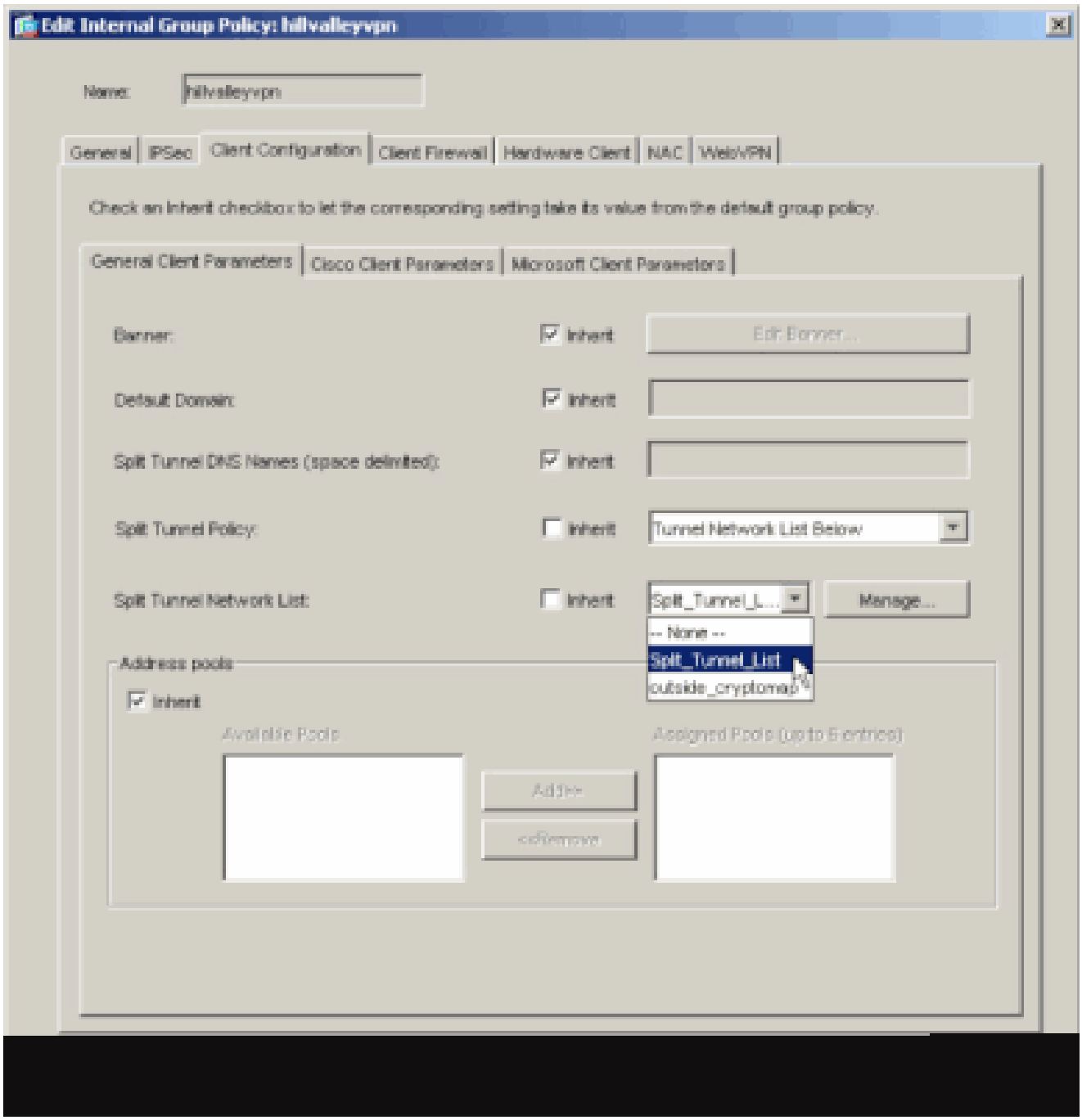

•

Cliquez sur **OK afin de quitter l'ACL Manager.**



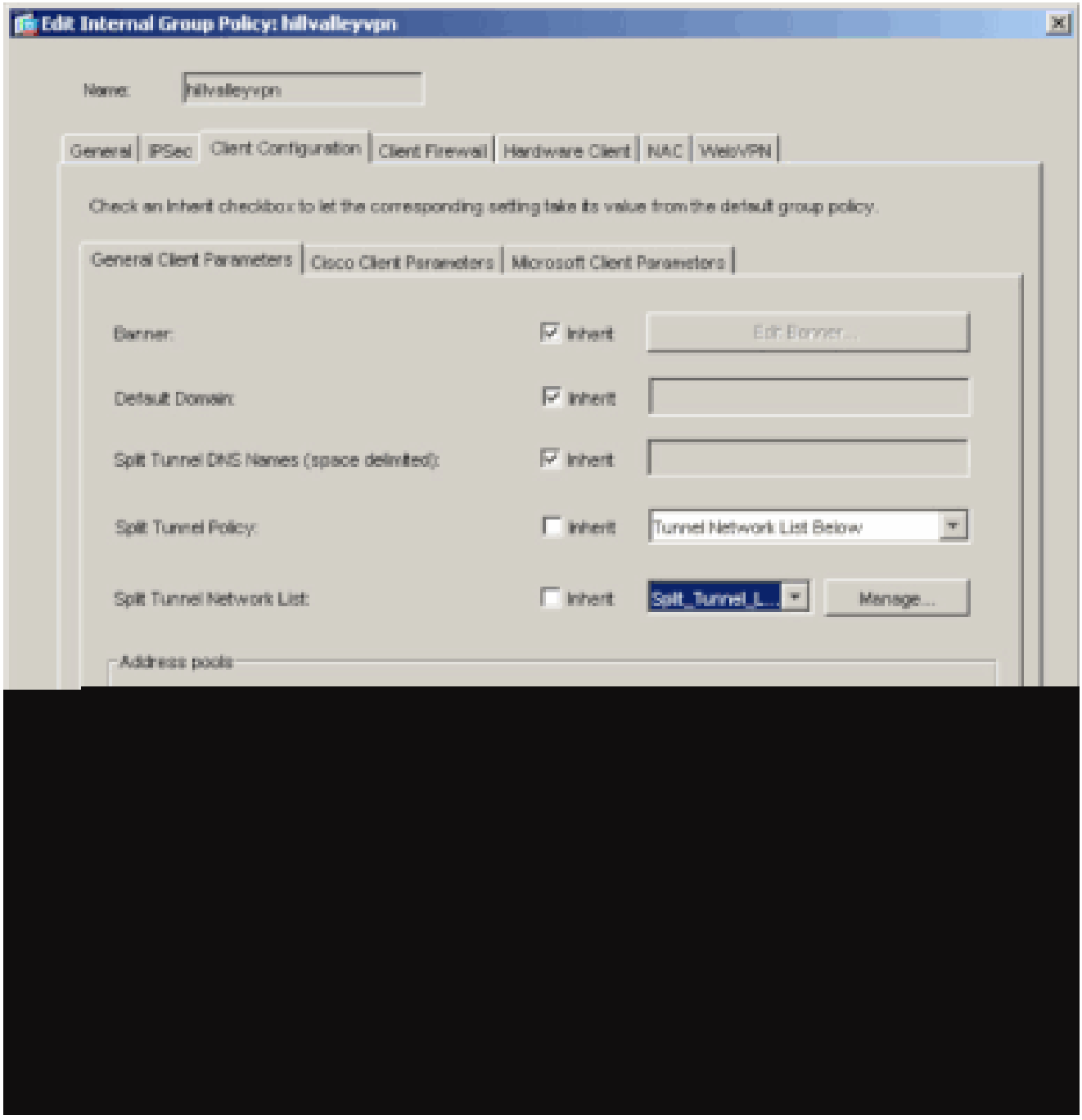

•

Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network List.



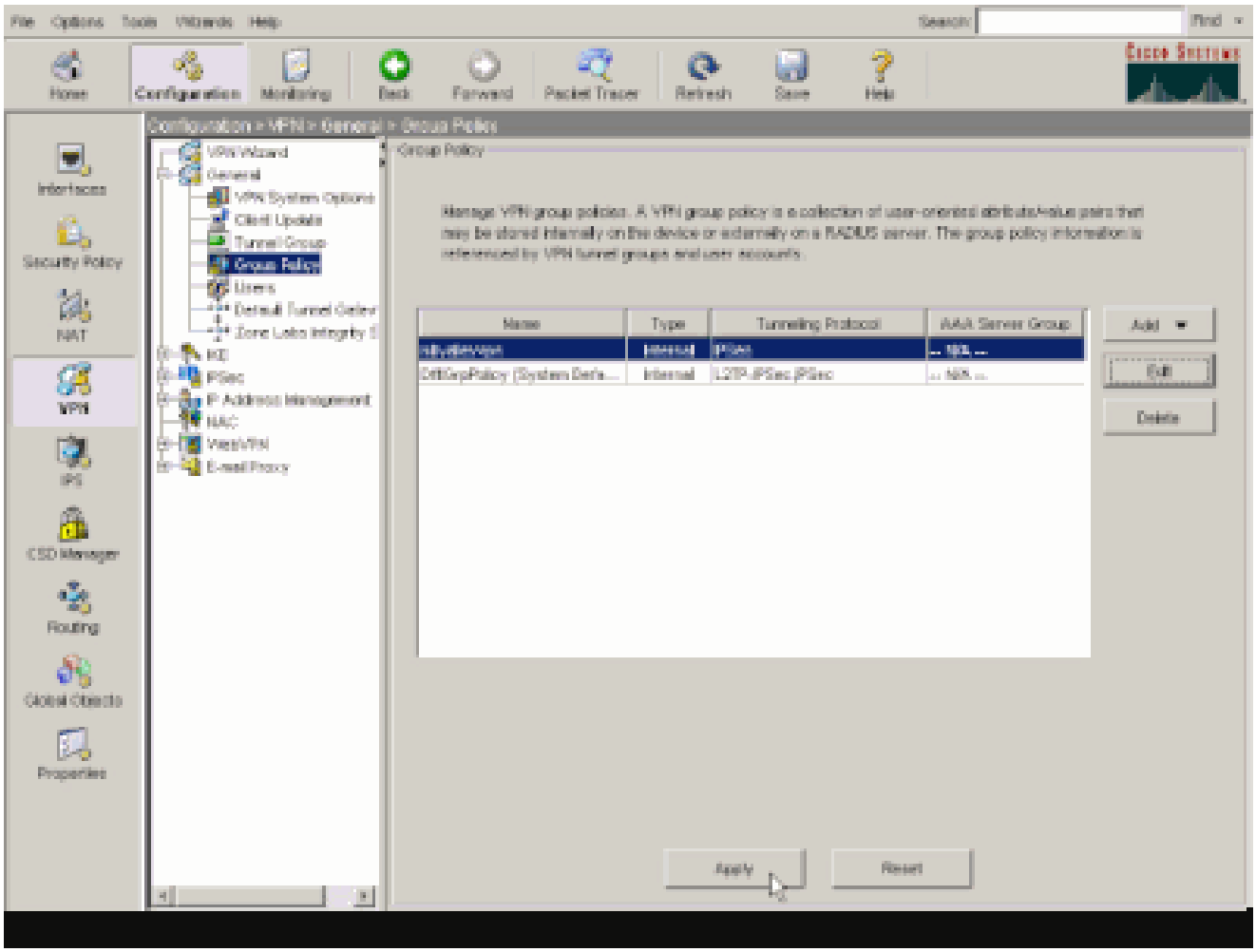

•

Cliquez sur **OK afin de retourner à la configuration de la stratégie de groupe.**




•

Cliquez sur Apply puis sur Send (s'il y a lieu) afin d'envoyer les commandes à l'ASA.

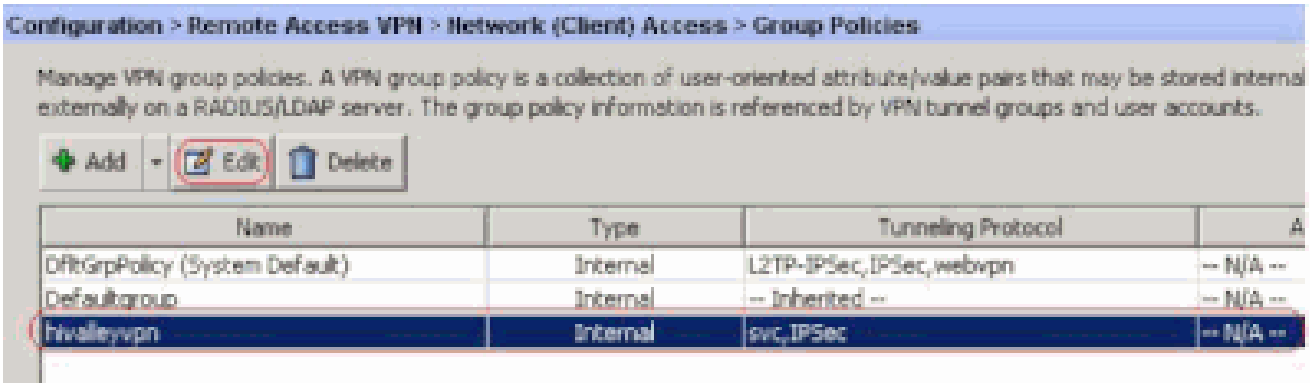


Configurer ASA 8.x avec ASDM 6.x

Complétez ces étapes afin de configurer votre groupe de tunnels de façon à permettre la transmission tunnel partagée pour les utilisateurs du groupe.

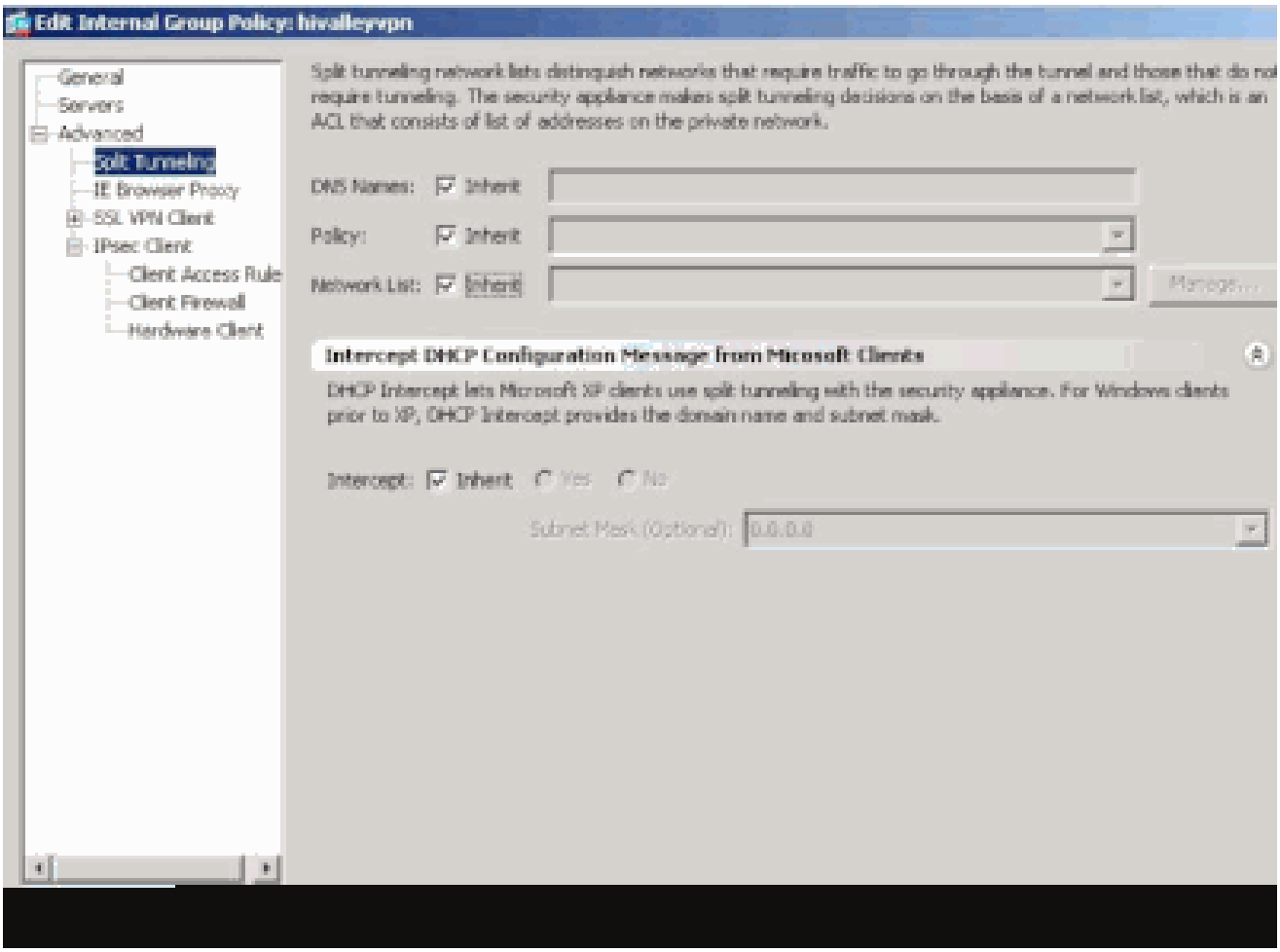
- 

Choisissez Configuration > Remote Access VPN > Network (Client) Access > Group Policies, et choisissez la stratégie de groupe dans laquelle vous souhaitez activer l'accès au LAN local. Cliquez alors sur Edit.



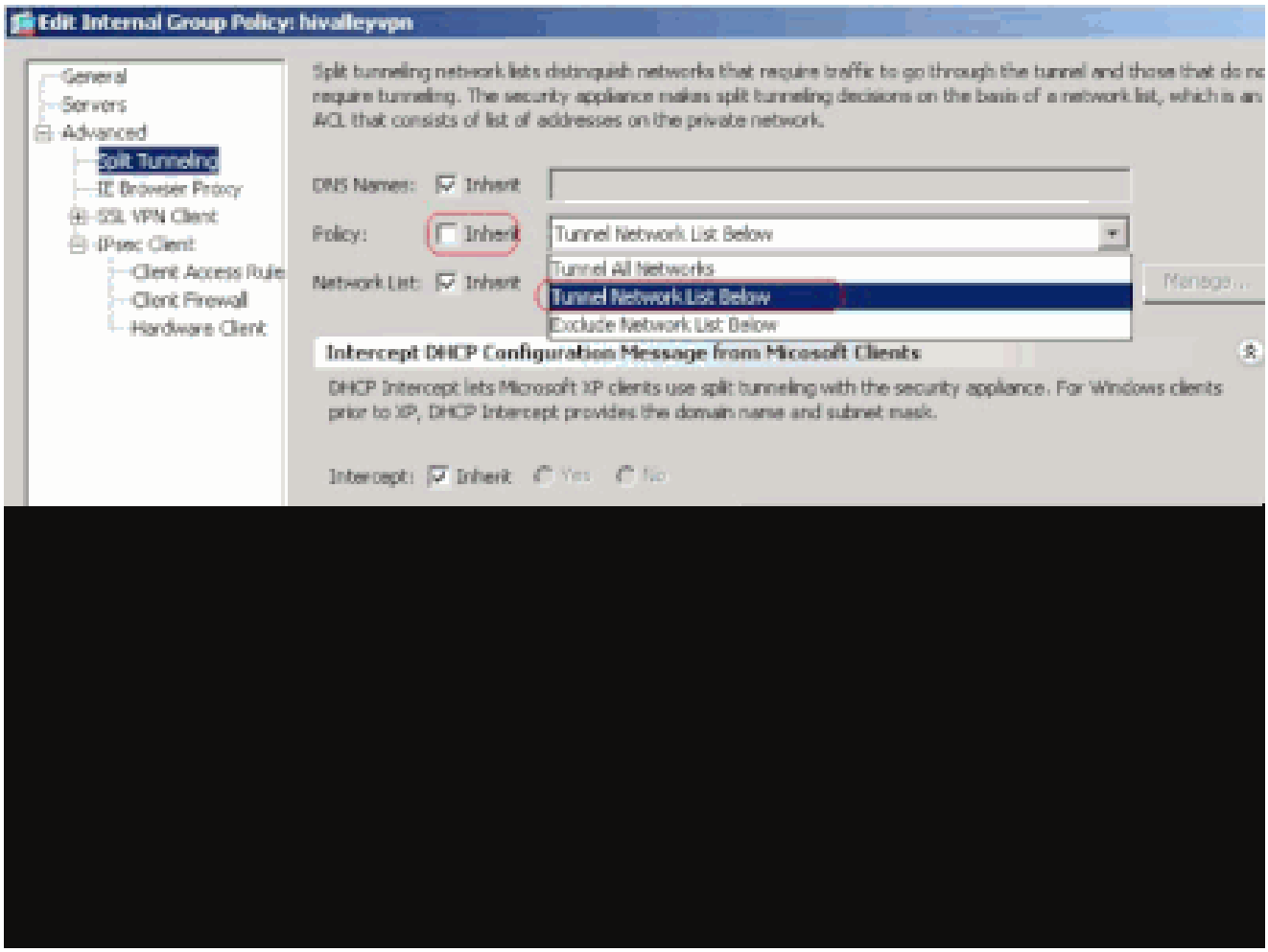

- 

Cliquez sur Split Tunneling.



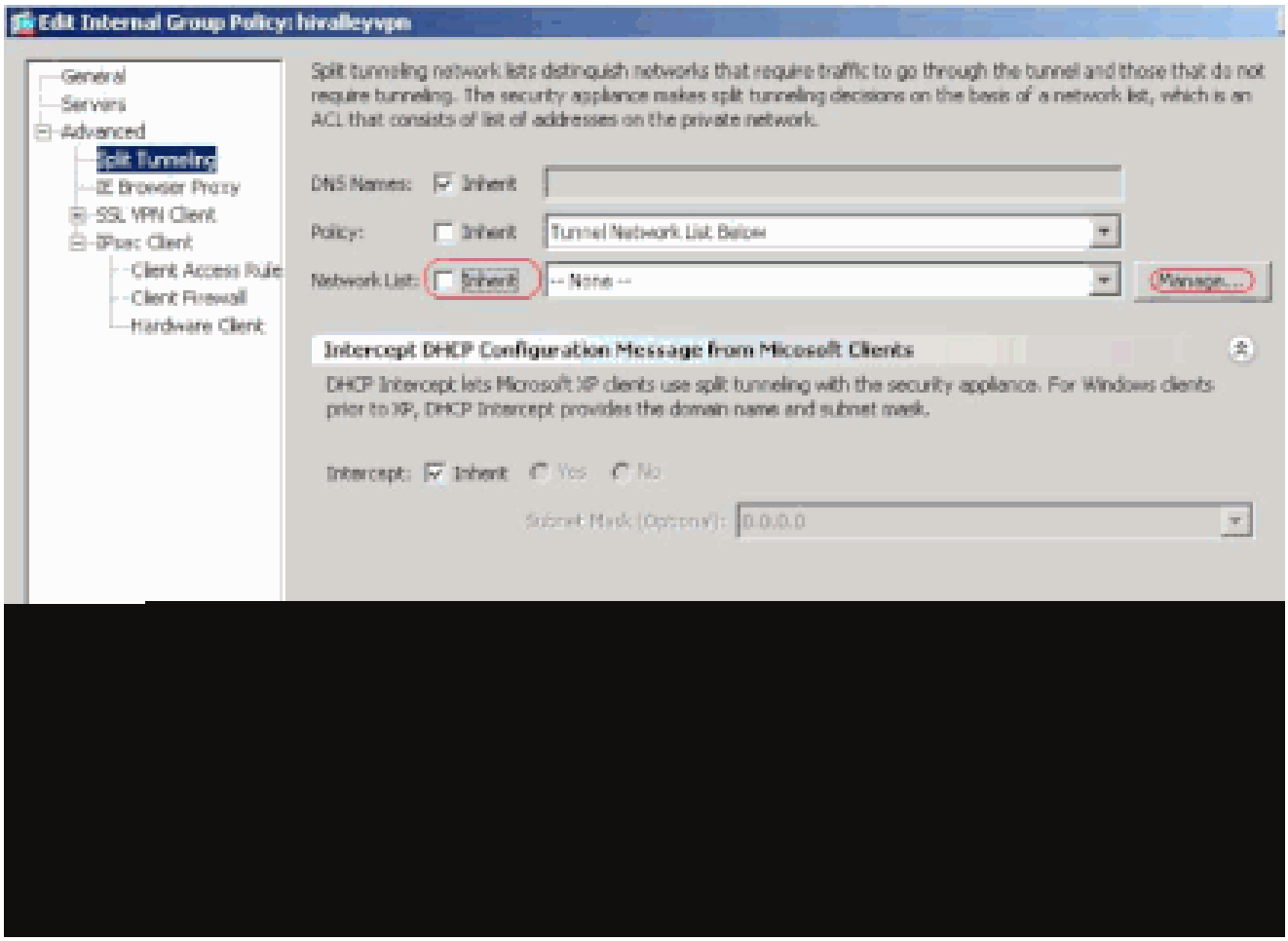

•

Désactivez la case Inherit pour la stratégie Split Tunnel Policy et choisissez Tunnel Network List Below.



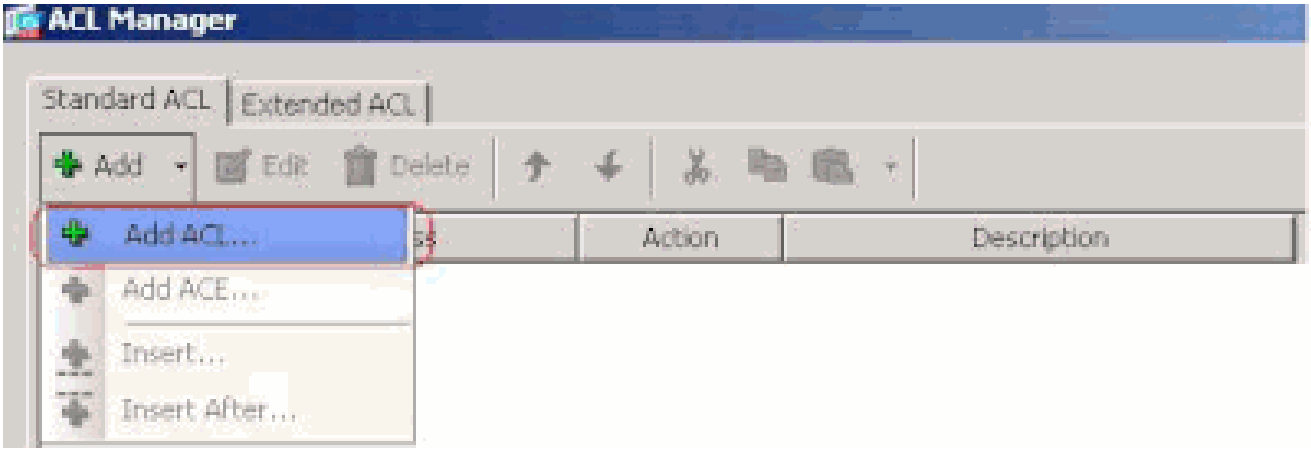

•

Désactivez la case Inherit pour la liste Split Tunnel Network List, puis cliquez sur Manage pour lancer l'ACL Manager.



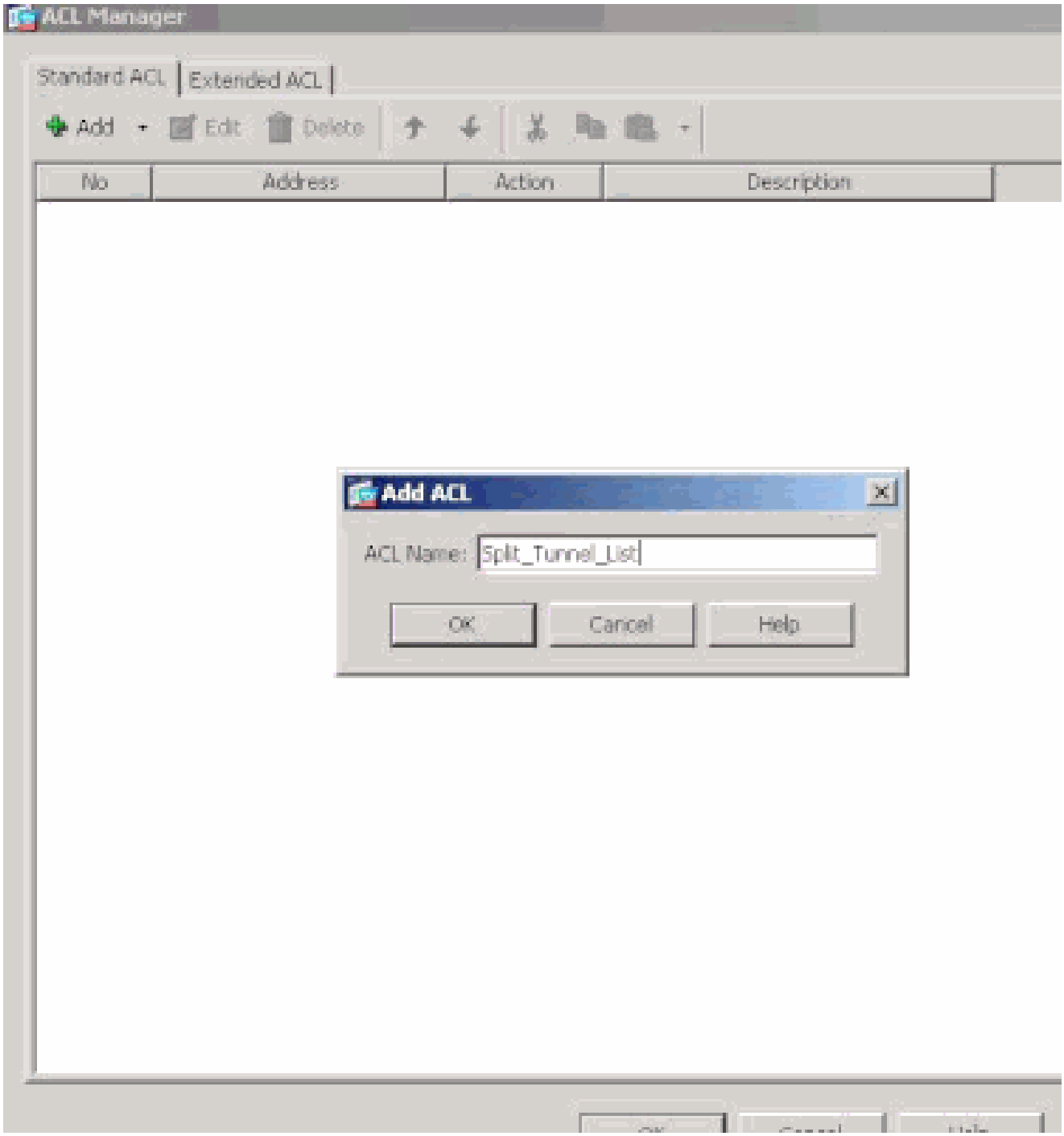

•

Dans le gestionnaire de listes de contrôle d'accès (ACL), choisissez « Add > Add ACL... » (ajouter > ajouter une ACL...) pour créer une nouvelle liste d'accès.



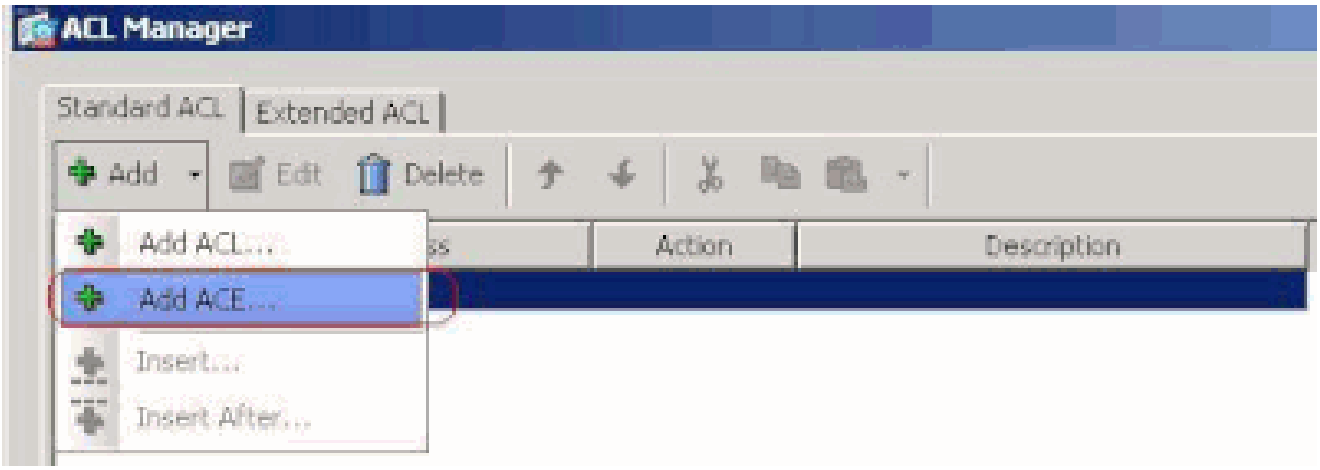

•

Fournissez un nom pour l'ACL et cliquez sur OK.




•

Une fois que l'ACL est créé, choisissez Add > Add ACE... afin d'ajouter une Entrée de contrôle d'accès (ACE).




- 

Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.0.1.0/24.

a. 

Cliquez sur la case d'option Permit.

b. 

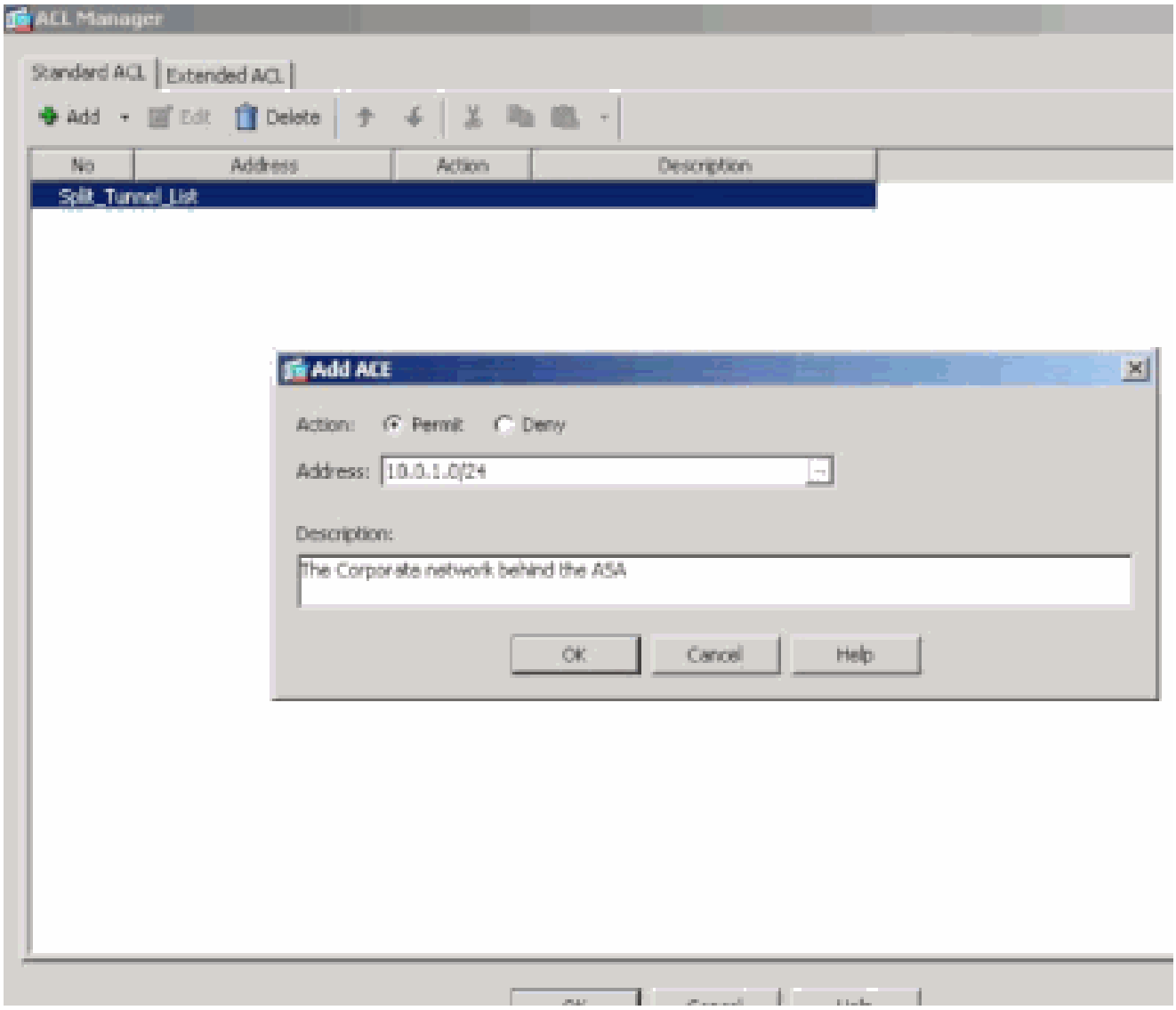
Choisissez l'adresse réseau avec le masque 10.0.1.0/24.

c. 

(Facultatif) Fournissez une description.

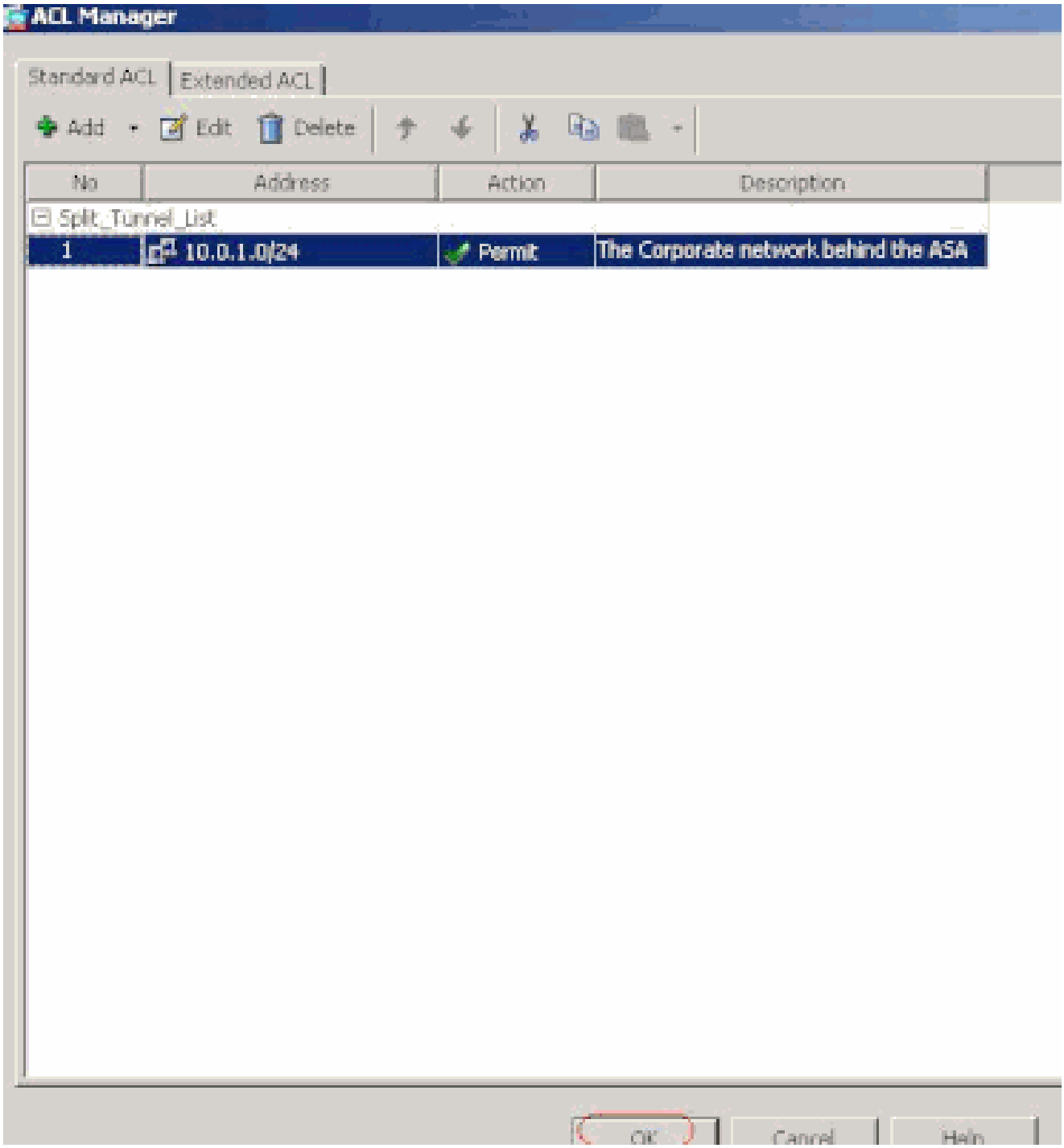
d. 

Click OK.



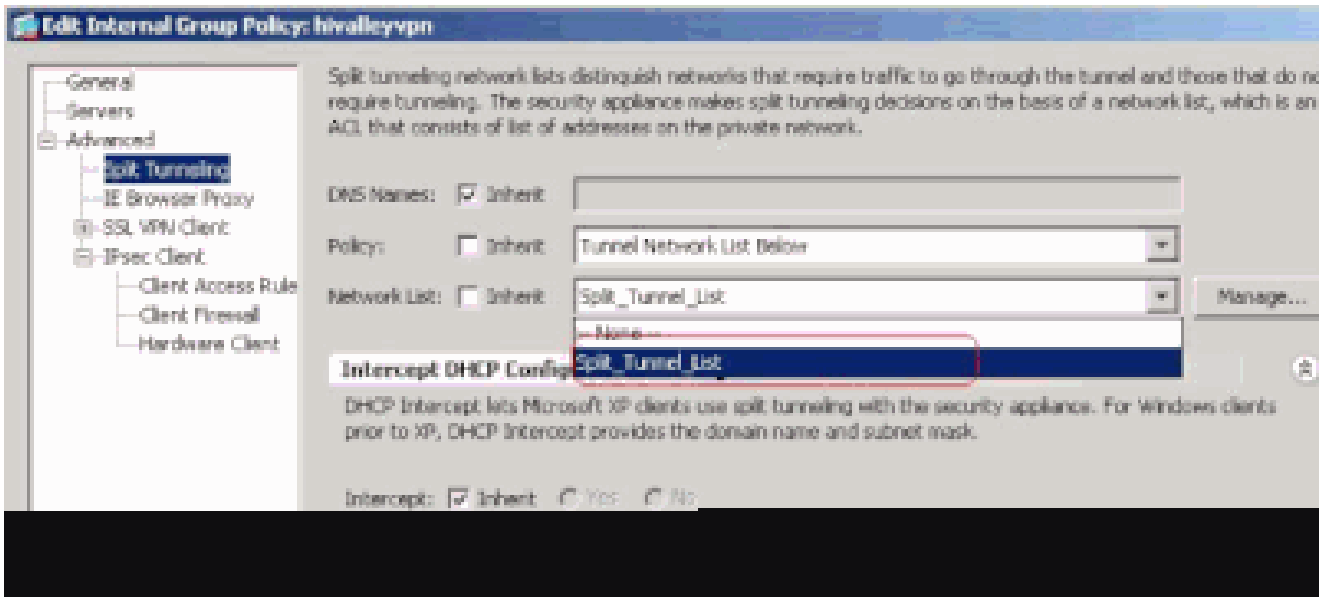

•

Cliquez sur OK afin de quitter l'ACL Manager.



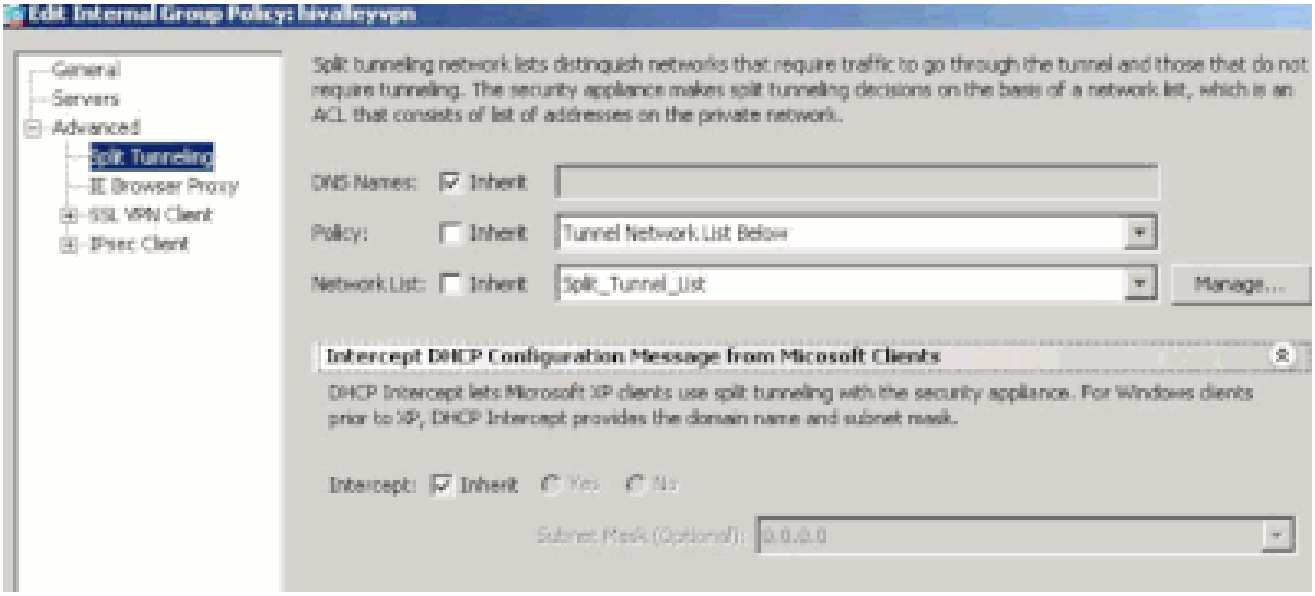

•

Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network List.



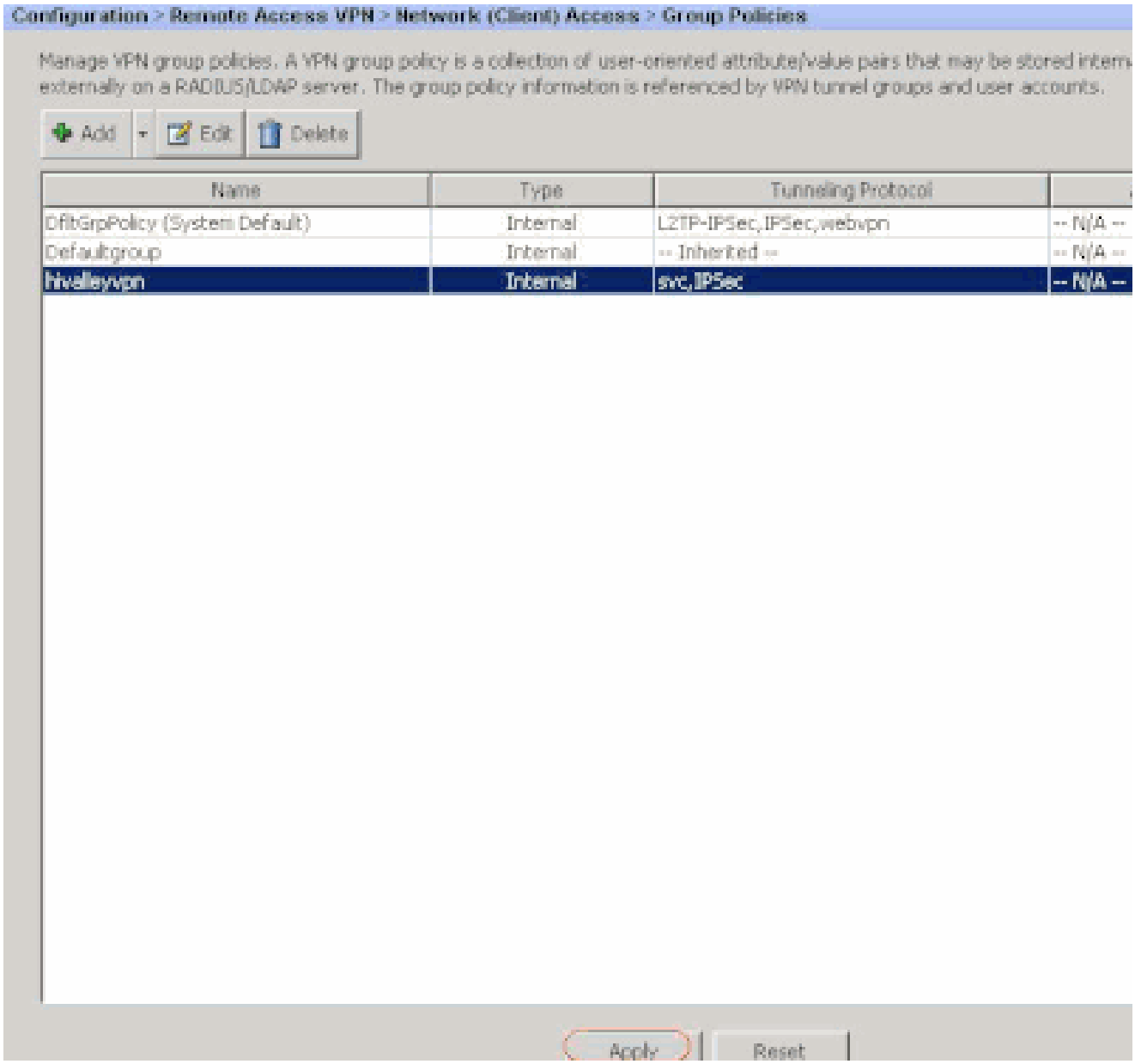

•

Cliquez sur OK afin de retourner à la configuration de la stratégie de groupe.



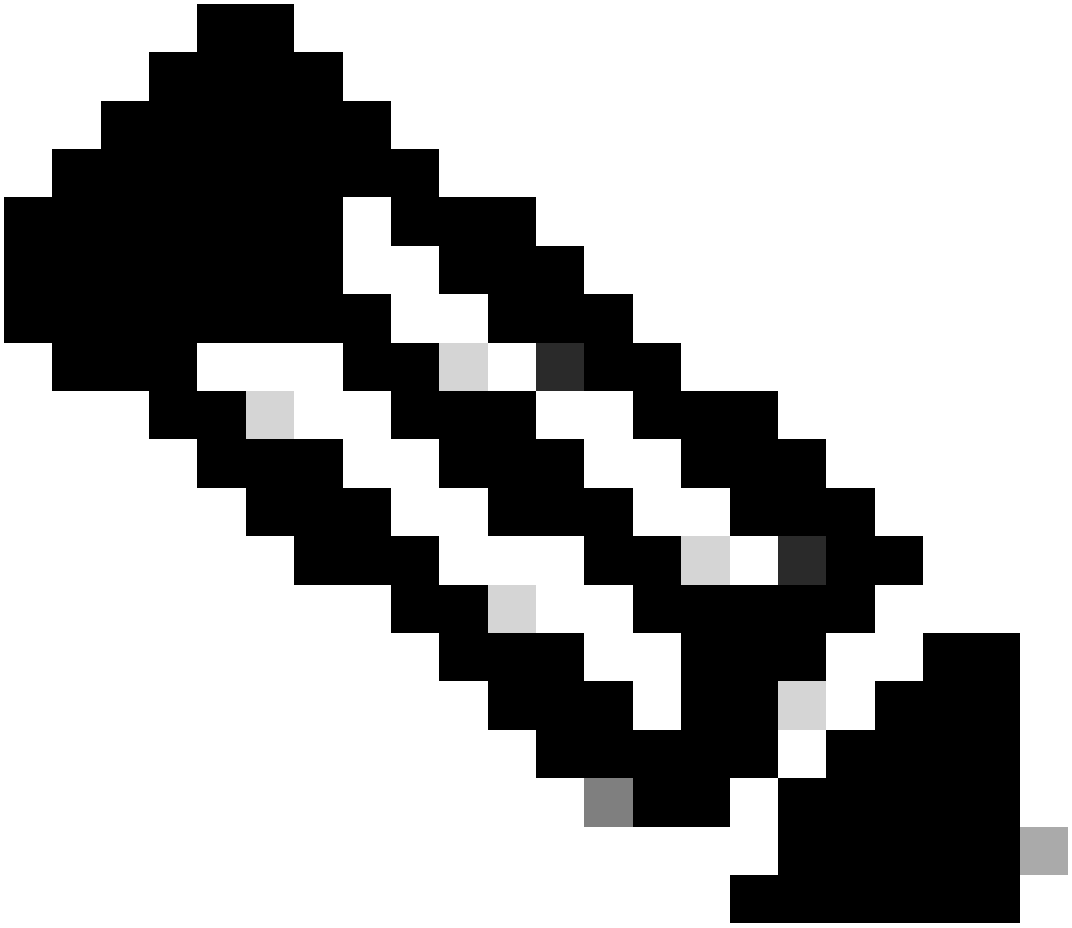

•

Cliquez sur Apply puis sur Send (s'il y a lieu) afin d'envoyer les commandes à l'ASA.




Configurer ASA 7.x et ultérieures via l'interface de ligne de commande (CLI)

Au lieu d'utiliser l'ASDM, vous pouvez compléter ces étapes dans l'interface de ligne de commande CLI d'ASA afin d'autoriser la transmission tunnel partagée sur ASA :



**Remarque** : la configuration CLI Split Tunneling est la même pour ASA 7.x et 8.x.

- 

Passez en mode de configuration.

```
<#root>

ciscoasa>
```

```
enable
```

```
Password: ********
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

- 

Créez la liste d'accès qui définit le réseau derrière ASA.

```
    <#root>

ciscoasa(config)#

 access-list Split_Tunnel_List remark The corporate network behind the ASA.

ciscoasa(config)#

 access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- 

Entrez le mode de configuration Group Policy pour la stratégie que vous souhaitez modifier.

```
    <#root>

ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

- 

Spécifiez la stratégie de transmission tunnel partagée. Dans ce cas, la stratégie est tunnelspecified.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

- 

Spécifiez la liste d'accès de transmission tunnel partagée. Dans ce cas, la liste est Split_Tunnel_List.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

- 

Émettez la commande suivante :

<#root>

```
ciscoasa(config)#
```

**tunnel-group hillvalleyvpn general-attributes**

- 

Associez la stratégie de groupe au groupe de tunnels

<#root>

```
ciscoasa(config-tunnel-ipsec)#
```

**default-group-policy hillvalleyvpn**

- 

Quittez les deux modes de configuration.

<#root>

```
ciscoasa(config-group-policy)#
```

**exit**

```
ciscoasa(config)#
```

**exit**

```
ciscoasa#
```

- Sauvegardez la configuration dans une mémoire vive non volatile (NVRAM) et appuyez Enter lorsqu'on vous invite à spécifier le nom de fichier source.

```
<#root>

ciscoasa#

 copy running-config startup-config


Source filename [running-config]?
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec)
ciscoasa#
```

Configurer PIX 6.x via l'interface de ligne de commande (CLI)

Procédez comme suit :

- Créez la liste d'accès qui définit le réseau derrière PIX.

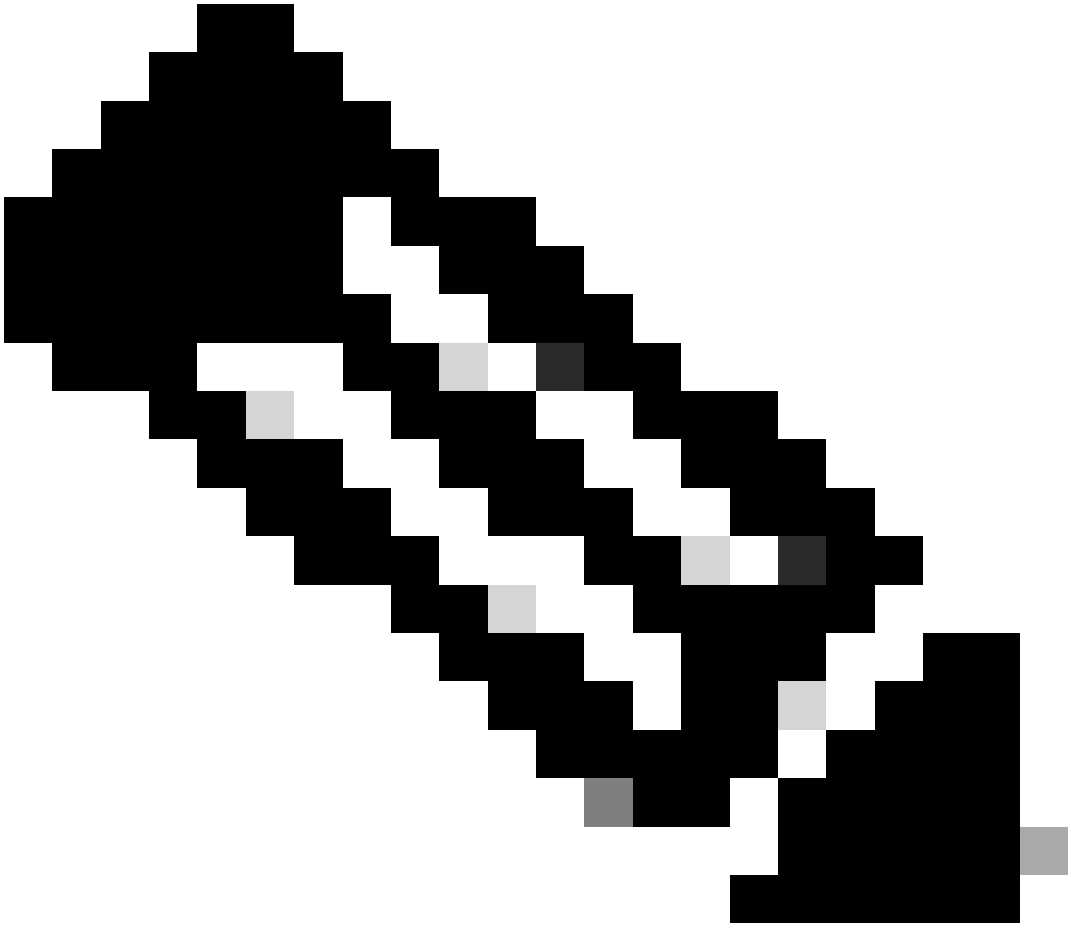
```
<#root>

 PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- Créez un groupe vpn vpn3000 et spécifiez l'ACL de transmission tunnel partagée pour ce groupe comme illustré :

**<#root>**

**PIX(config)#**

**vpngroup vpn3000 split-tunnel Split_Tunnel_List**



**Remarque** : référez-vous à Cisco Secure PIX Firewall 6.x et Cisco VPN Client 3.5 pour Windows avec authentification RADIUS IAS Microsoft Windows 2000 et 2003 pour plus d'informations sur la configuration VPN d'accès à distance pour PIX 6.x.

---

Vérifier

Exécutez les étapes décrites dans ces parties afin de vérifier votre configuration.

- Se connecter avec le client VPN

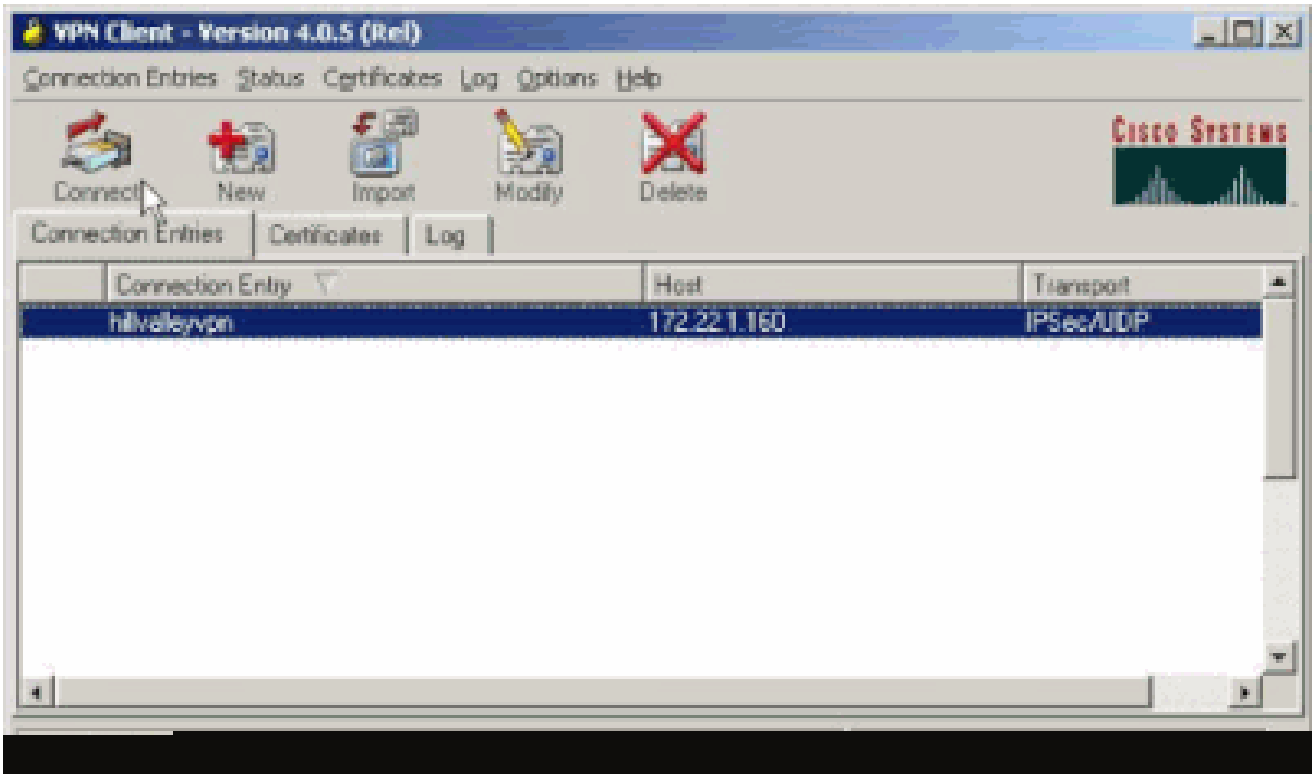
- Afficher le journal du client VPN

- Tester l'accès local au LAN avec un ping

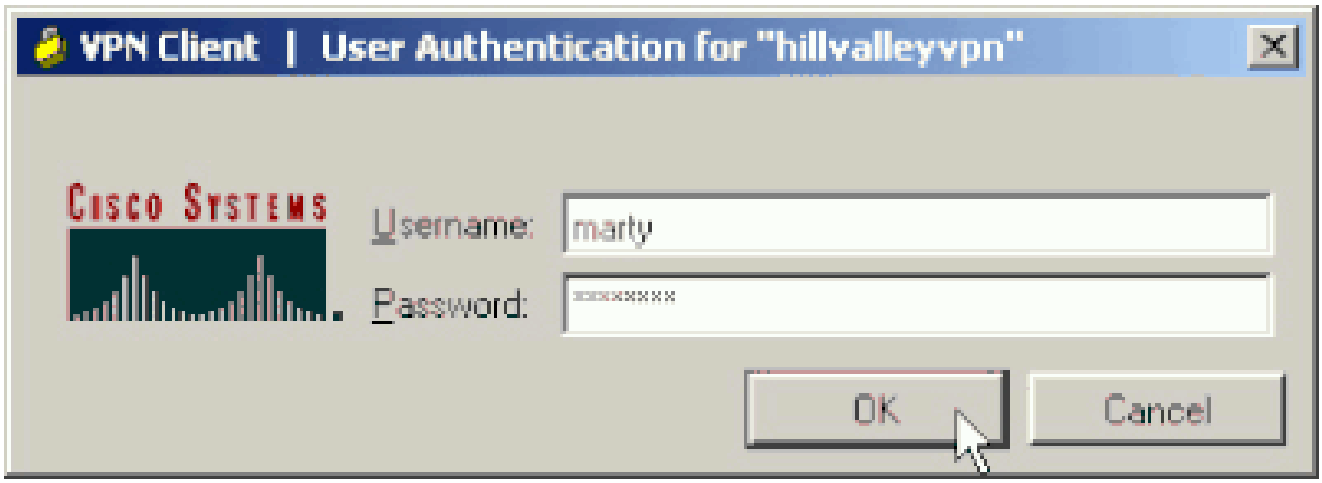
Se connecter avec le client VPN

Connectez votre client VPN au concentrateur VPN afin de vérifier votre configuration.

- Choisissez votre entrée de connexion dans la liste et cliquez sur **Connect.**

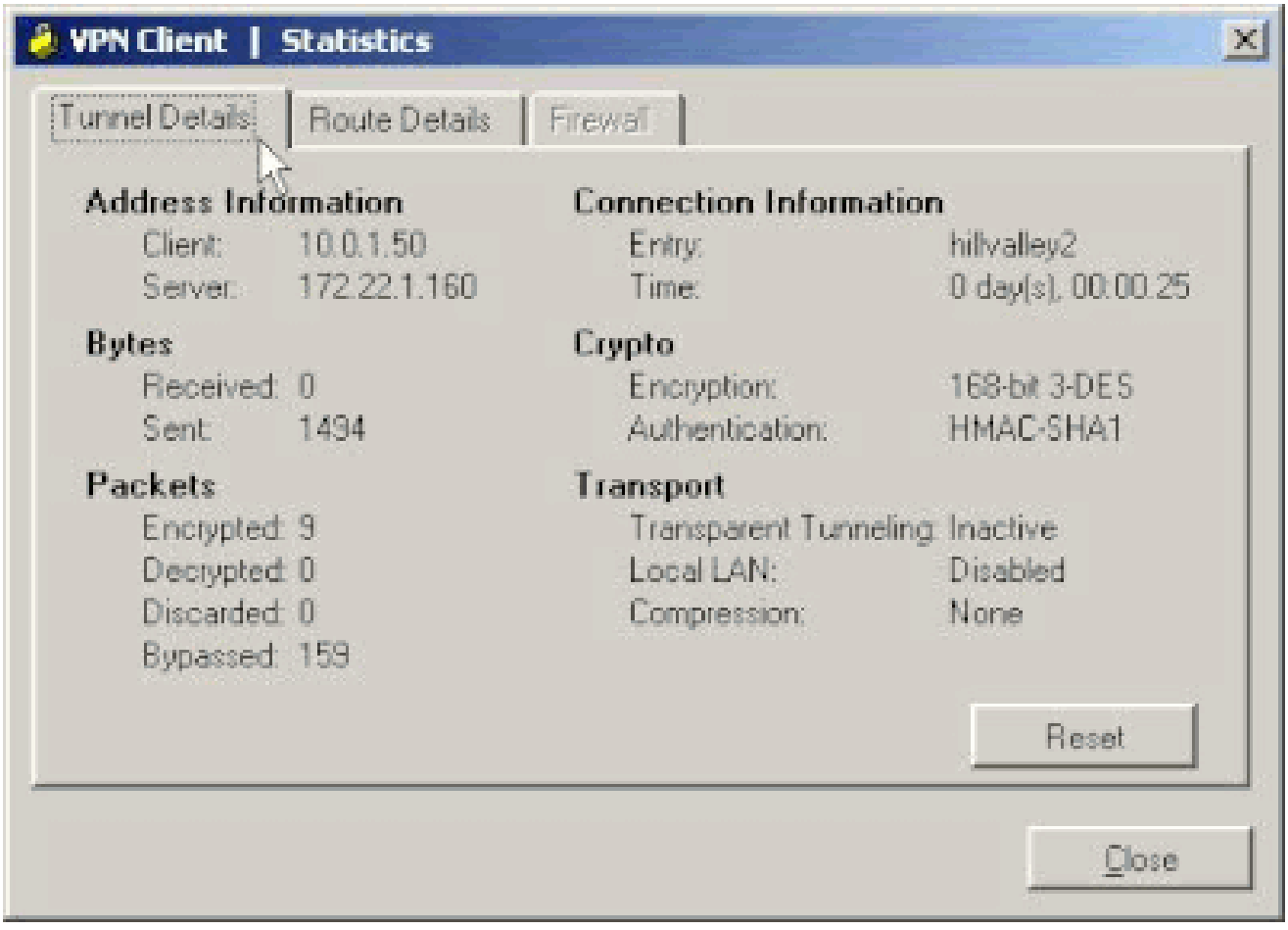



- Entrez dans vos informations d'identification.




•

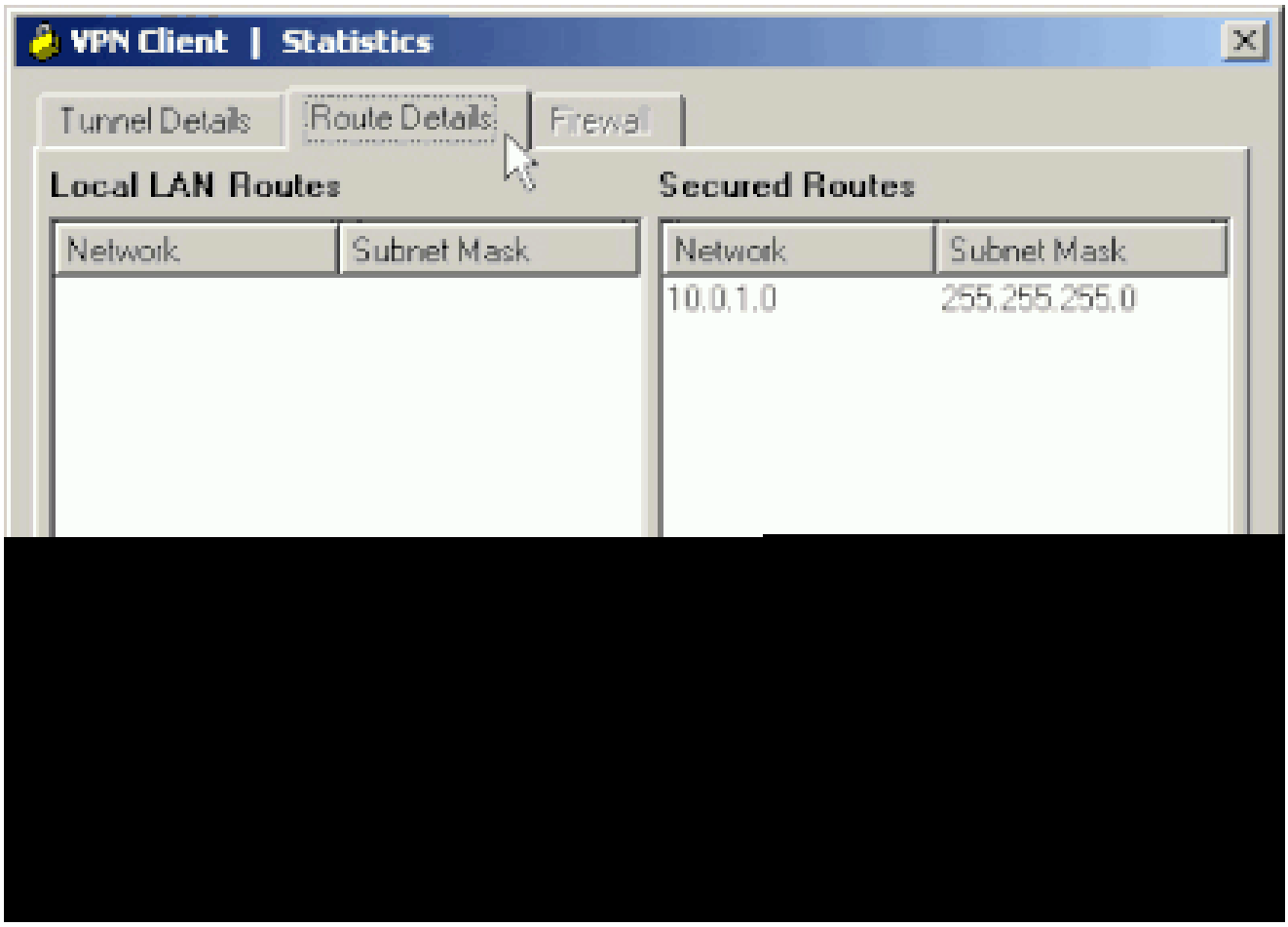
Choisissez **Status > Statistics... afin d'afficher la fenêtre de détails de tunnel où vous pouvez inspecter les conditions particulières du tunnel et consulter le flux du trafic.**




•

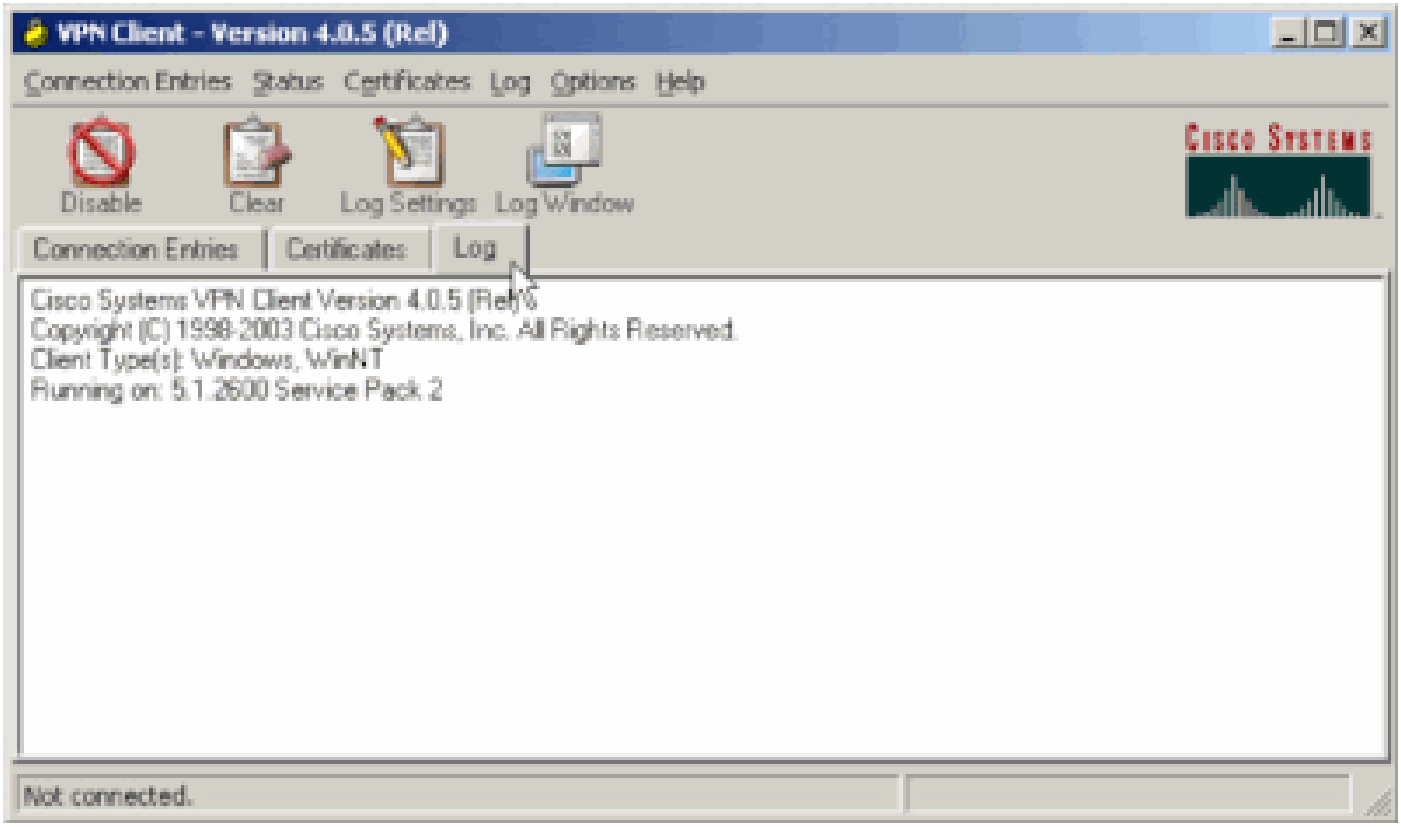
Accédez à l'onglet Route Details pour afficher les routes que le client VPN sécurise vers ASA.

Dans cet exemple, le client VPN sécurise l'accès à 10.0.1.0/24, tandis que tout autre trafic n'est pas crypté et n'est pas envoyé à travers le tunnel.




Afficher le journal du client VPN

Quand vous examinez le journal du client VPN, vous pouvez déterminer si le paramètre qui spécifie la transmission tunnel partagée est défini. Afin d'afficher le journal, accédez à l'onglet Log dans le client VPN. Cliquez alors sur **Log Settings afin d'ajuster ce qui est enregistré.** Dans cet exemple, IKE est défini sur **3 - High** tandis que tous les autres éléments du journal sont définis sur 1 - Low.




```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:20:09.532  07/27/06  Sev=Info/6    IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.


!--- Output is supressed


18     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005D
Client sending a firewall request to concentrator

19     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).

20     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005C
Firewall Policy: Product=Cisco Intrusion Prevention Security Agent,
Capability= (Are you There?).

21     14:20:14.208  07/27/06  Sev=Info/4    IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160

22     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300002F
Received ISAKMP packet: peer = 172.22.1.160

23     14:20:14.208  07/27/06  Sev=Info/4    IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.160

24     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x63000010
```

```
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50

25     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0

26     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000

27     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000

28     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems,
Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45

!--- Split tunneling is permitted and the remote LAN is defined.

29     14:20:14.238  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

30     14:20:14.238  07/27/06  Sev=Info/5    IKE/0x6300000F
SPLIT_NET #1
    subnet = 10.0.1.0
    mask = 255.255.255.0
    protocol = 0
    src port = 0
    dest port=0

!--- Output is supressed.
```

Tester l'accès local au LAN avec un ping

Un moyen supplémentaire de tester si le client VPN est configuré pour la transmission tunnel partagée, tout en étant relié par tunnel à ASA, est d'utiliser la commande ping sur la ligne de commande Windows. Le réseau local du client VPN est 192.168.0.0/24 et un autre hôte est présent sur le réseau avec une adresse IP 192.168.0.3.

```
   <#root>

C:\>

 ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Dépannage

Limitation avec le nombre d'entrées dans une ACL de tunnel partagé

Il existe une restriction avec le nombre d'entrées dans une liste de contrôle d'accès utilisée pour le split tunnel. Il est recommandé de ne pas utiliser plus de 50-60 entrées ACE pour une fonctionnalité satisfaisante. Il est conseillé de mettre en oeuvre la fonction de création de sous-réseaux pour couvrir une plage d’adresses IP.

Informations connexes

- **Exemple de configuration de PIX/ASA 7.x comme serveur de VPN distant avec l'ASDM**
- **Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500**
- **Assistance technique de Cisco et téléchargements**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.