ASA/PIX : Permettre le split tunneling pour des clients VPN sur l'exemple de configuration de l'ASA

Contenu

Introduction

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: Le plein Tunnellisation est considéré les la plupart configuration sécurisée parce qu'il n'active pas l'accès au périphérique simultané à l'Internet et au RÉSEAU LOCAL entreprise. Une compromission entre le pleins Tunnellisation et Segmentation de tunnel permet à des clients vpn l'accès local au LAN seulement. Référez-vous à PIX/ASA 7.x : Exemple de configuration pour permettre aux clients VPN d'accéder au réseau local pour plus d'informations.

Conditions préalables

Conditions requises

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 :

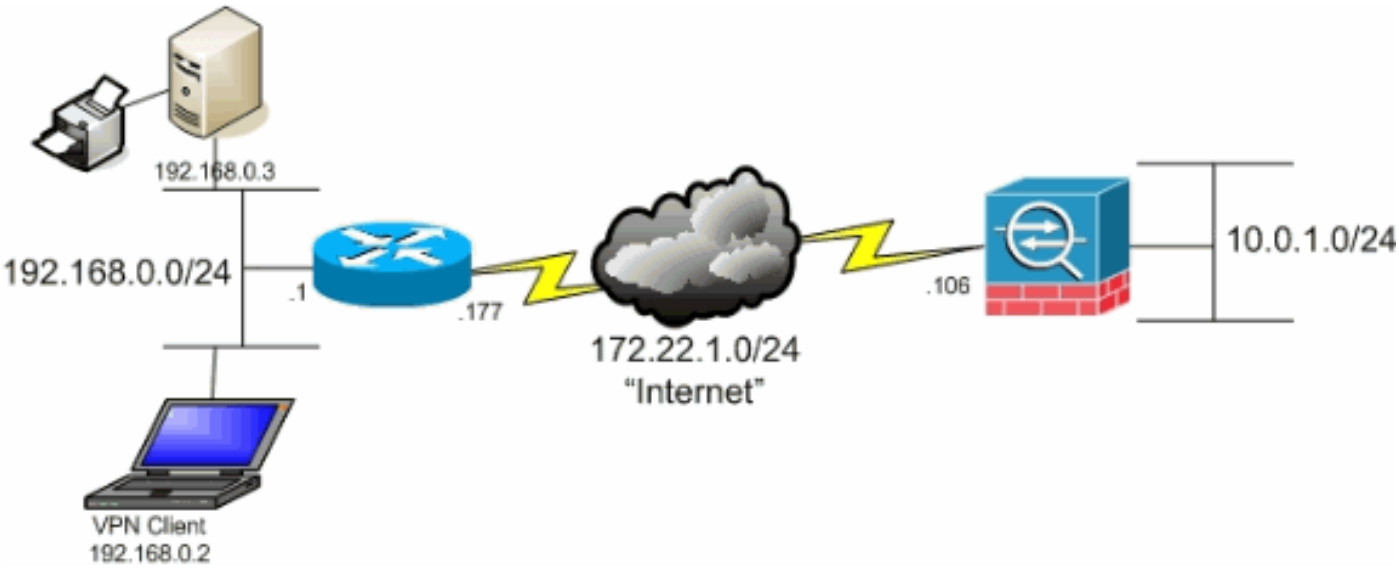
- Logiciel du dispositif de sécurité de la gamme Cisco ASA 5500 version 7.x et ultérieures
- Client VPN version 4.0.5 de Cisco Systems

Remarque: Ce document contient également la configuration CLI de PIX 6.x qui est compatible avec le Client VPN Cisco 3.x.

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

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



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 à Conventions relatives aux conseils techniques Cisco.

Informations générales

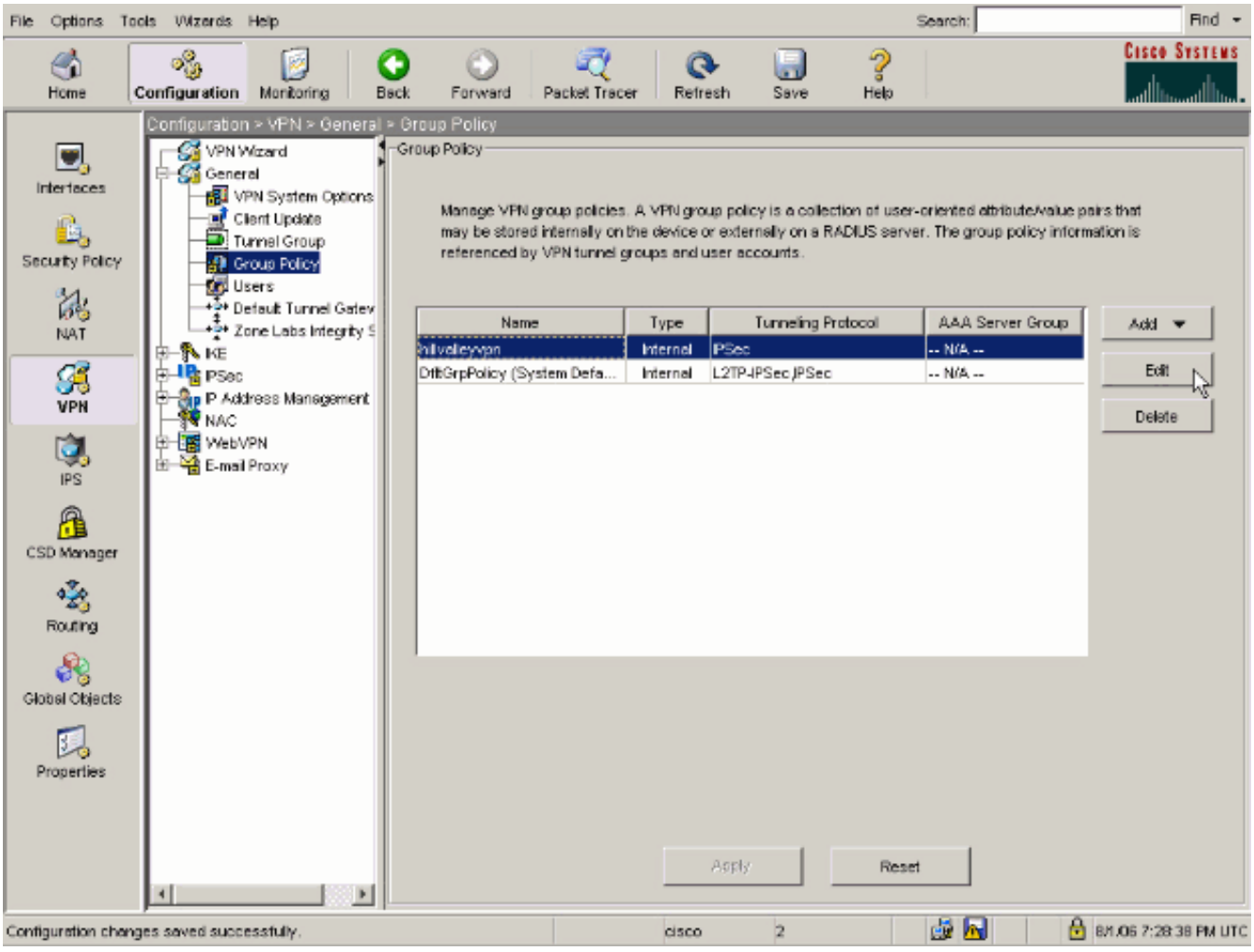
Dans un scénario de connexion de base d'un client VPN à ASA, tout le trafic provenant du client VPN est crypté et envoyé à ASA quelle que soit sa destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande passante. 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

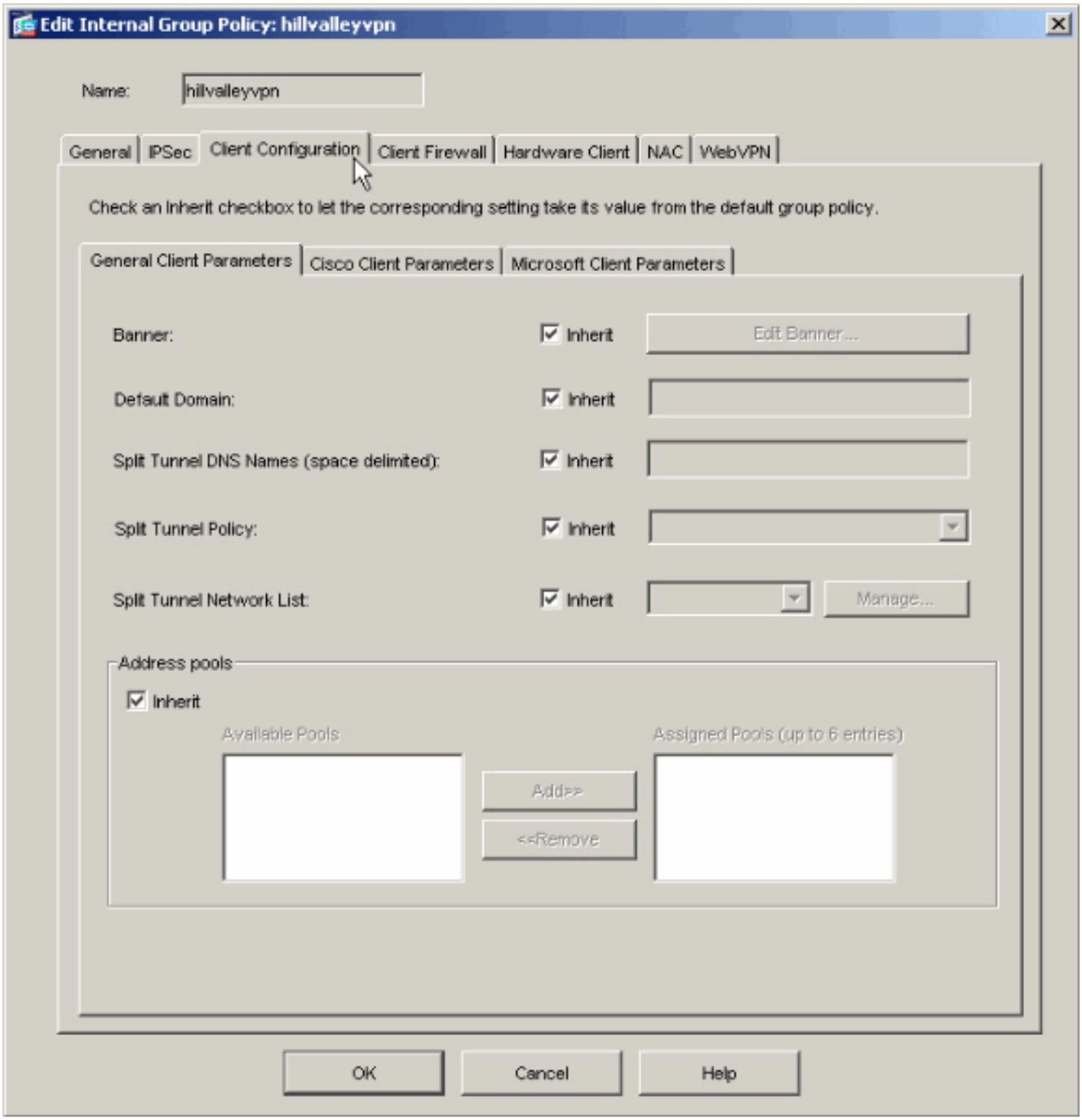
Configurer ASA 7.x avec l'Adaptive Security Device Manager (ASDM) 5.x

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

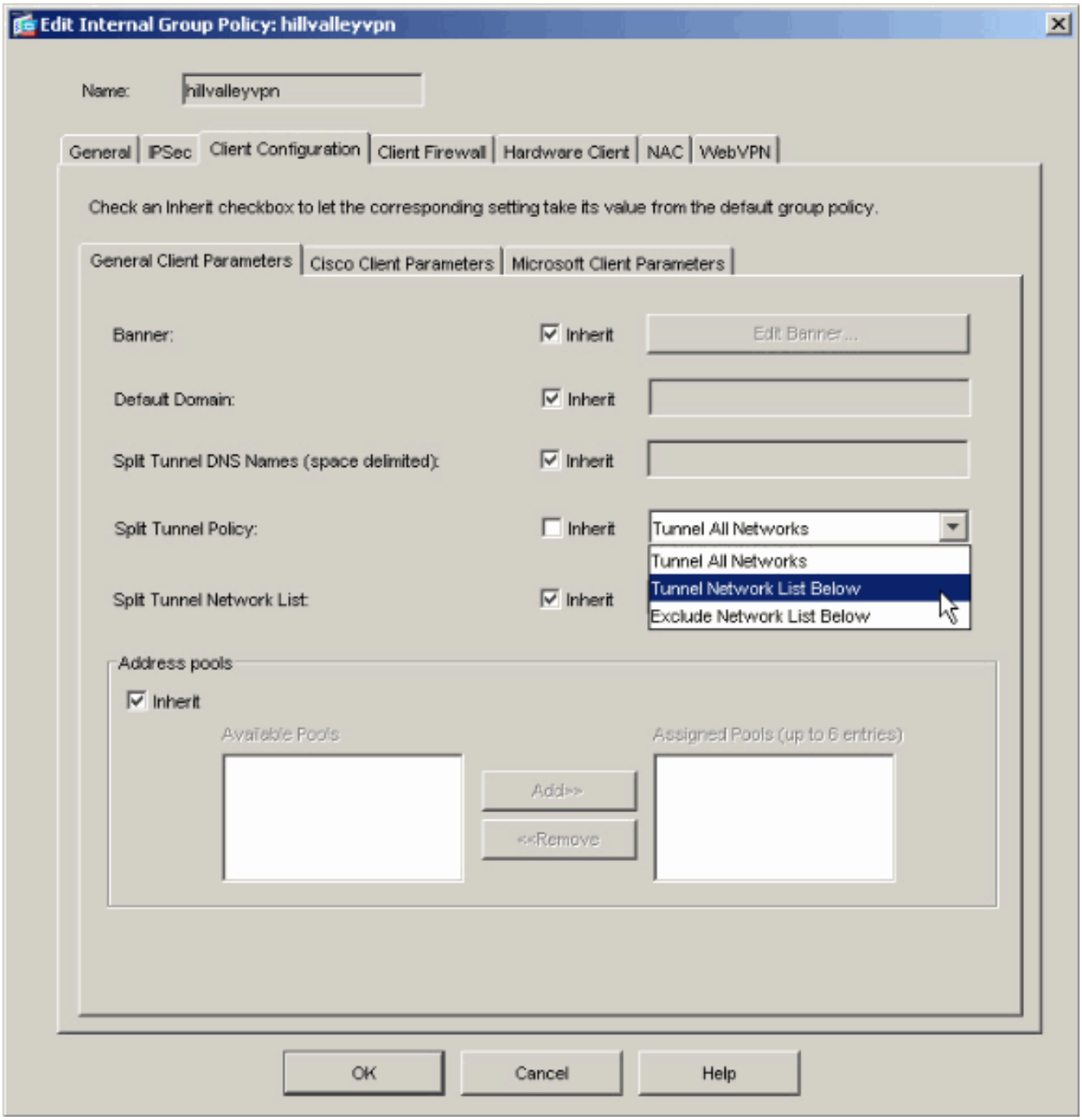
1. Choisissez **Configuration > VPN > General > Group Policy** et sélectionnez la stratégie de groupe dans laquelle vous souhaitez activer l'accès au LAN local. Cliquez alors sur **Edit**.



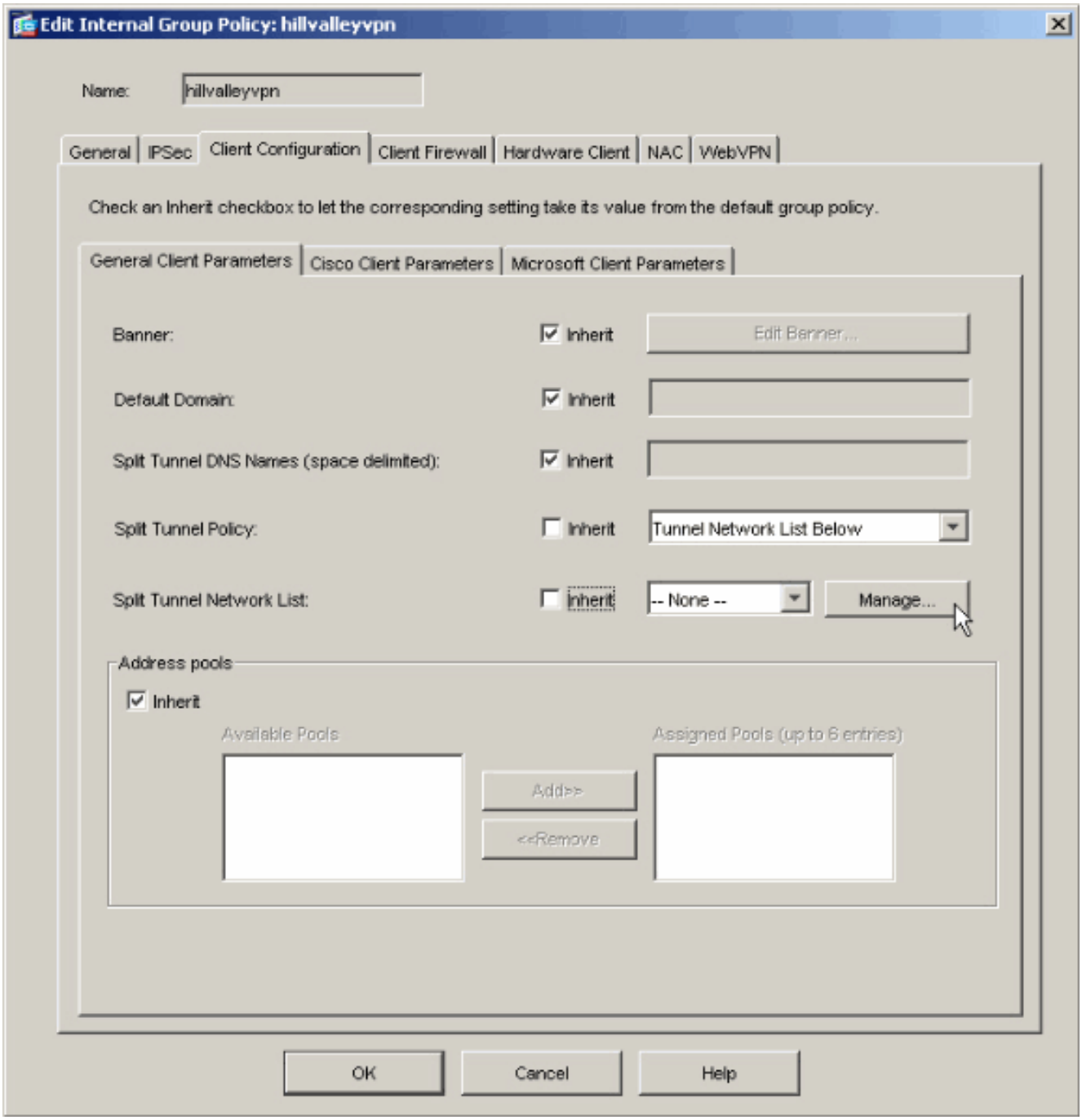
2. Accédez à l'onglet Client Configuration.



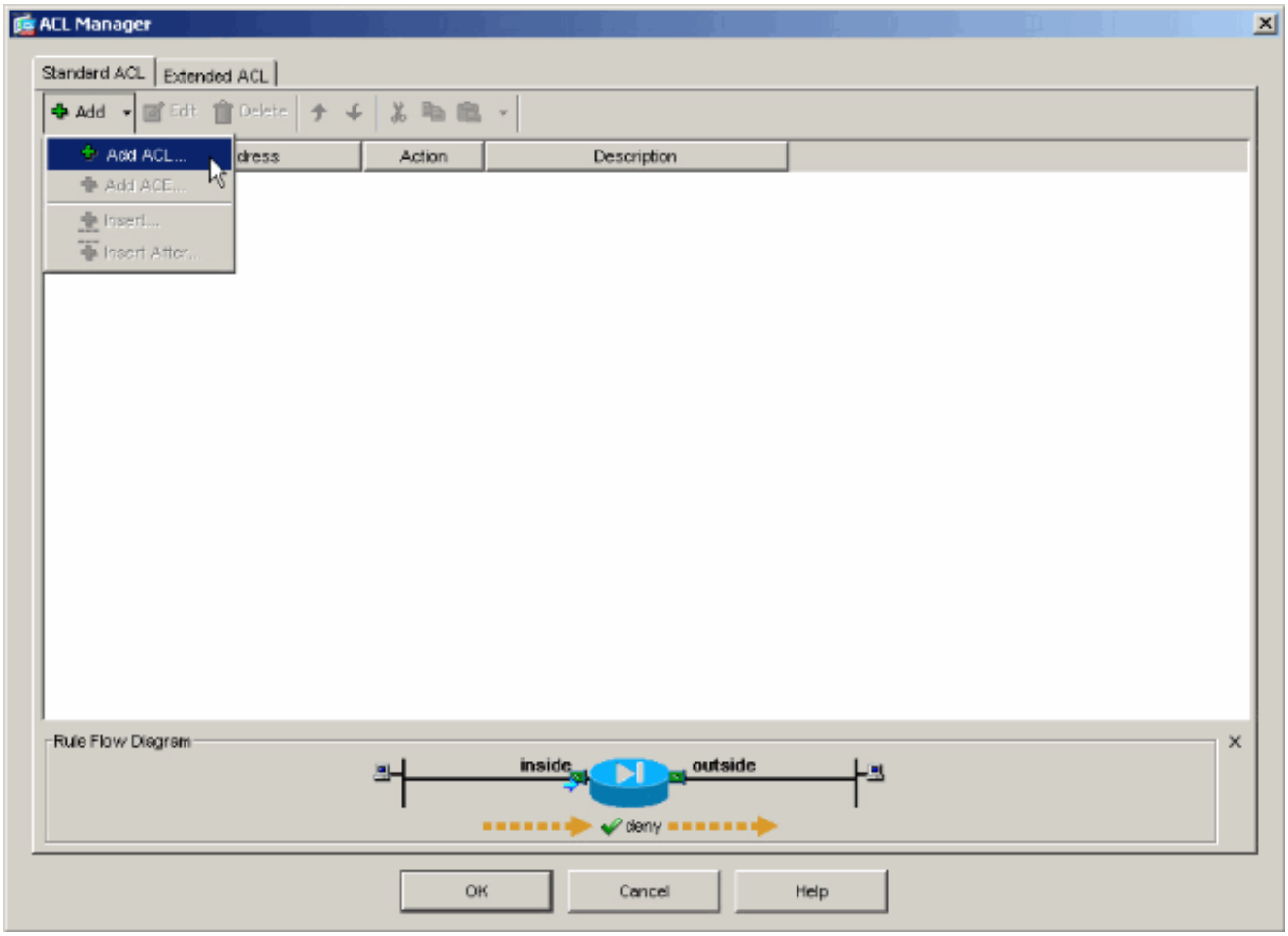
3. Désactivez la case **Inherit** pour la stratégie Split Tunnel Policy et choisissez **Tunnel Network List**
   Below.



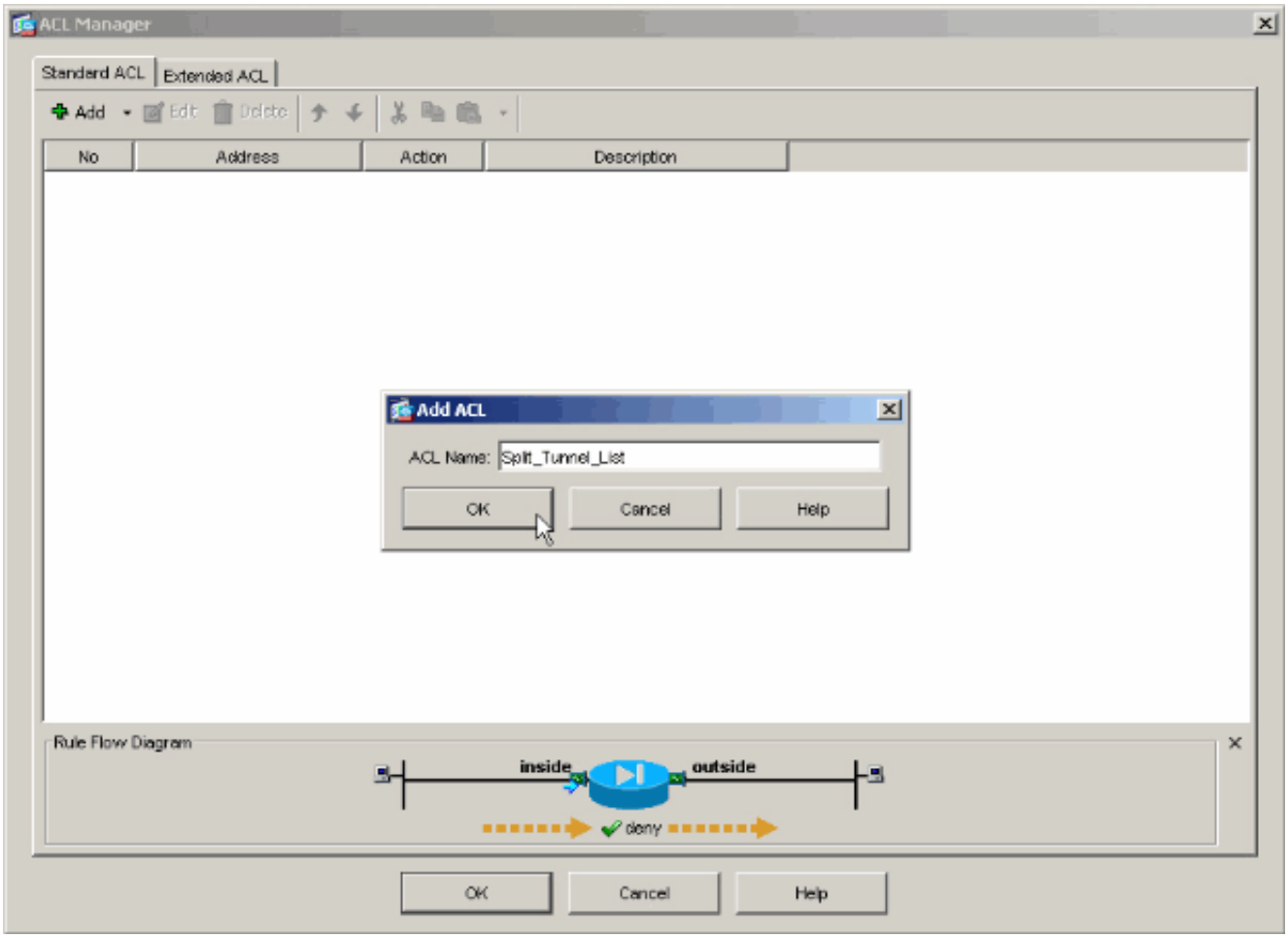
4. Désactivez la case **Inherit** pour la liste Split Tunnel Network List, puis cliquez sur **Manage** pour lancer l'ACL
   Manager.



5. Chez le gestionnaire d'ACL, choisissez **ajoutent > ajoutent l'ACL…** afin de créer une nouvelle liste
d'accès.

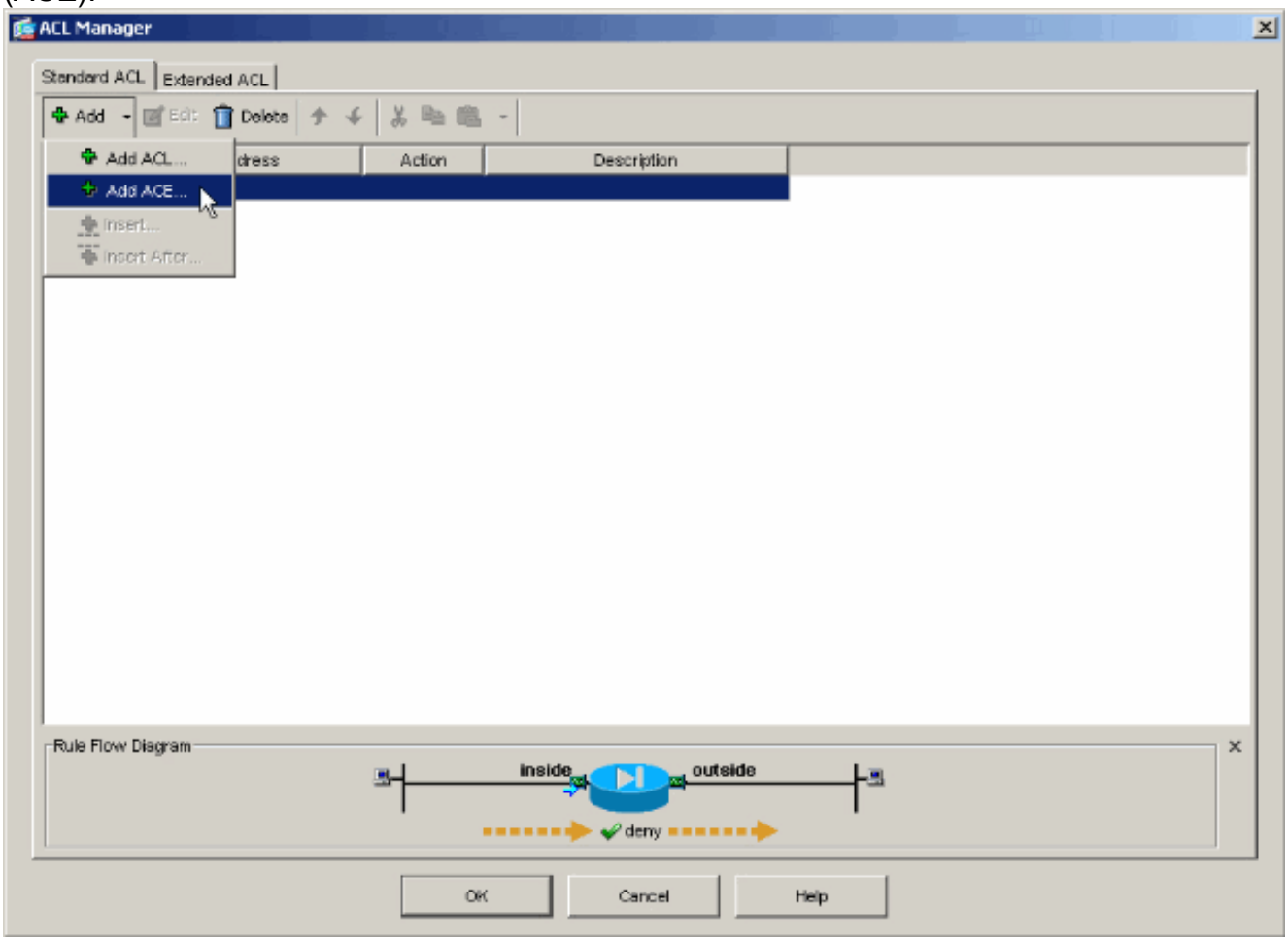


6. Fournissez un nom pour l'ACL et cliquez sur **OK**.

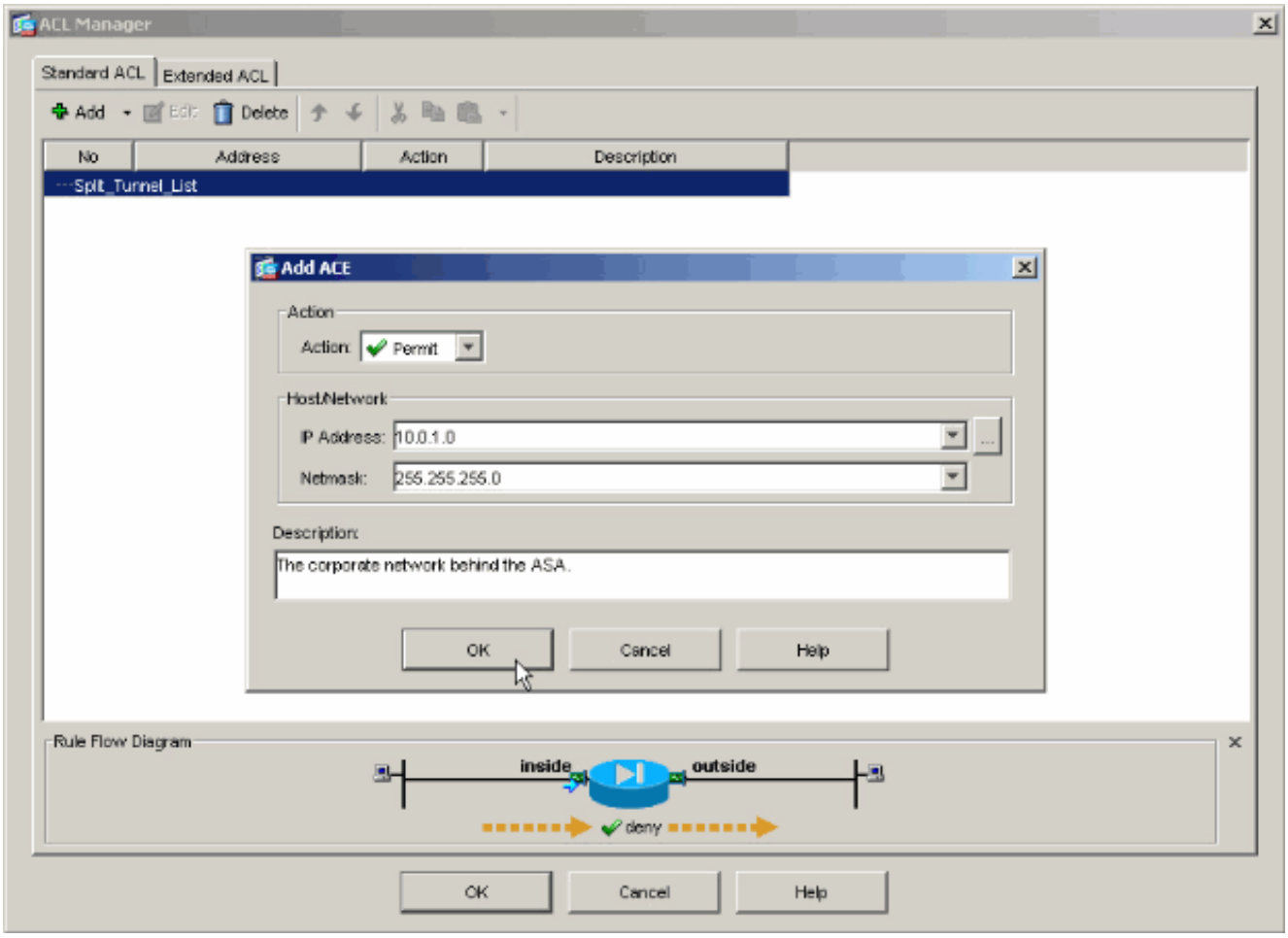


7. Une fois que l'ACL est créé, choisissez **Add > Add ACE...** afin d'ajouter une Entrée de

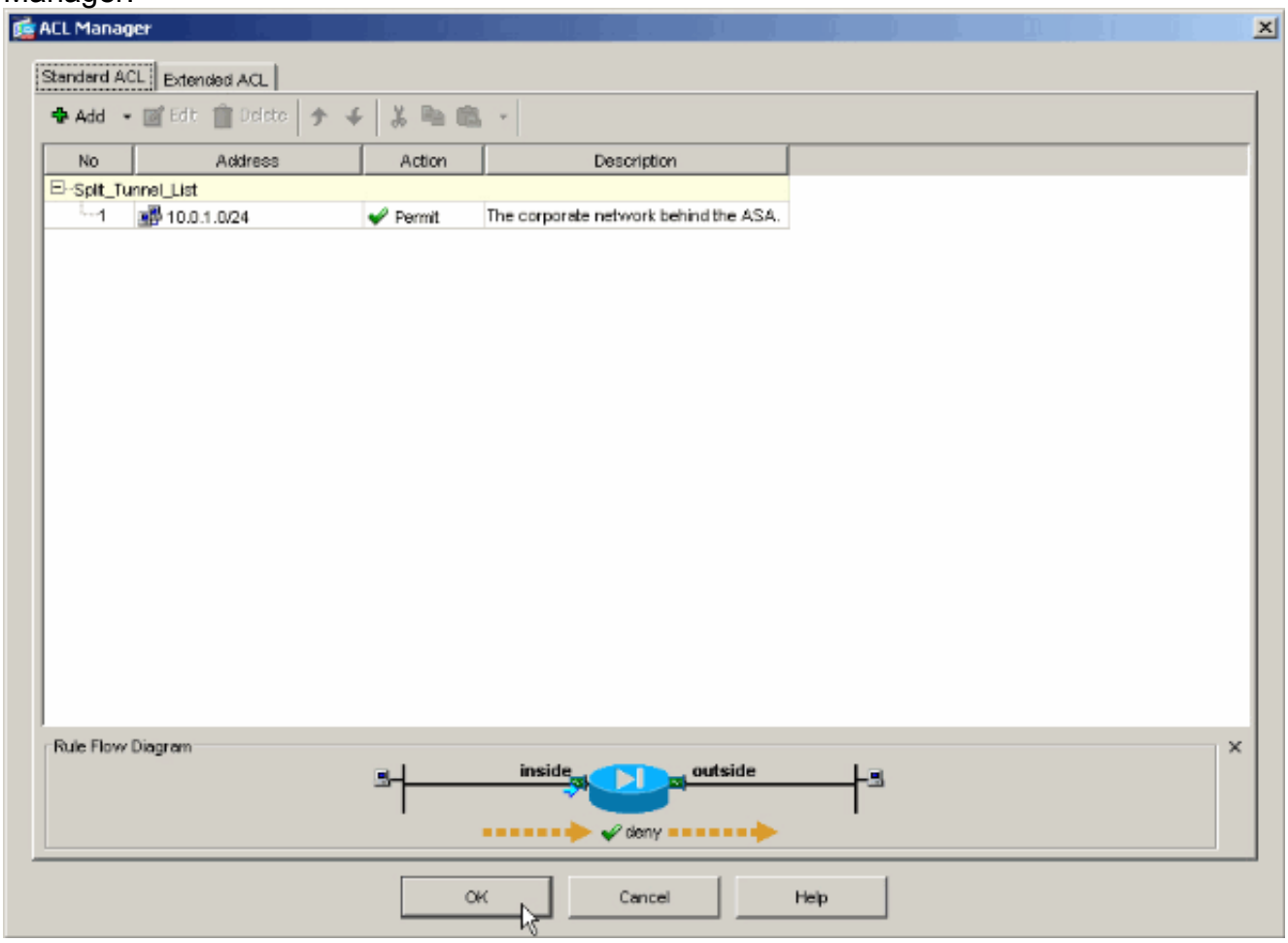
contrôle d'accès
(ACE).



8. Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est 10.0.1.0/24.Choisissez **Permit**.Choisissez une adresse IP **10.0.1.0**Choisissez un masque de réseau **255.255.255.0**.*((Facultatif)* Fournissez une description.Cliquez sur **OK**.

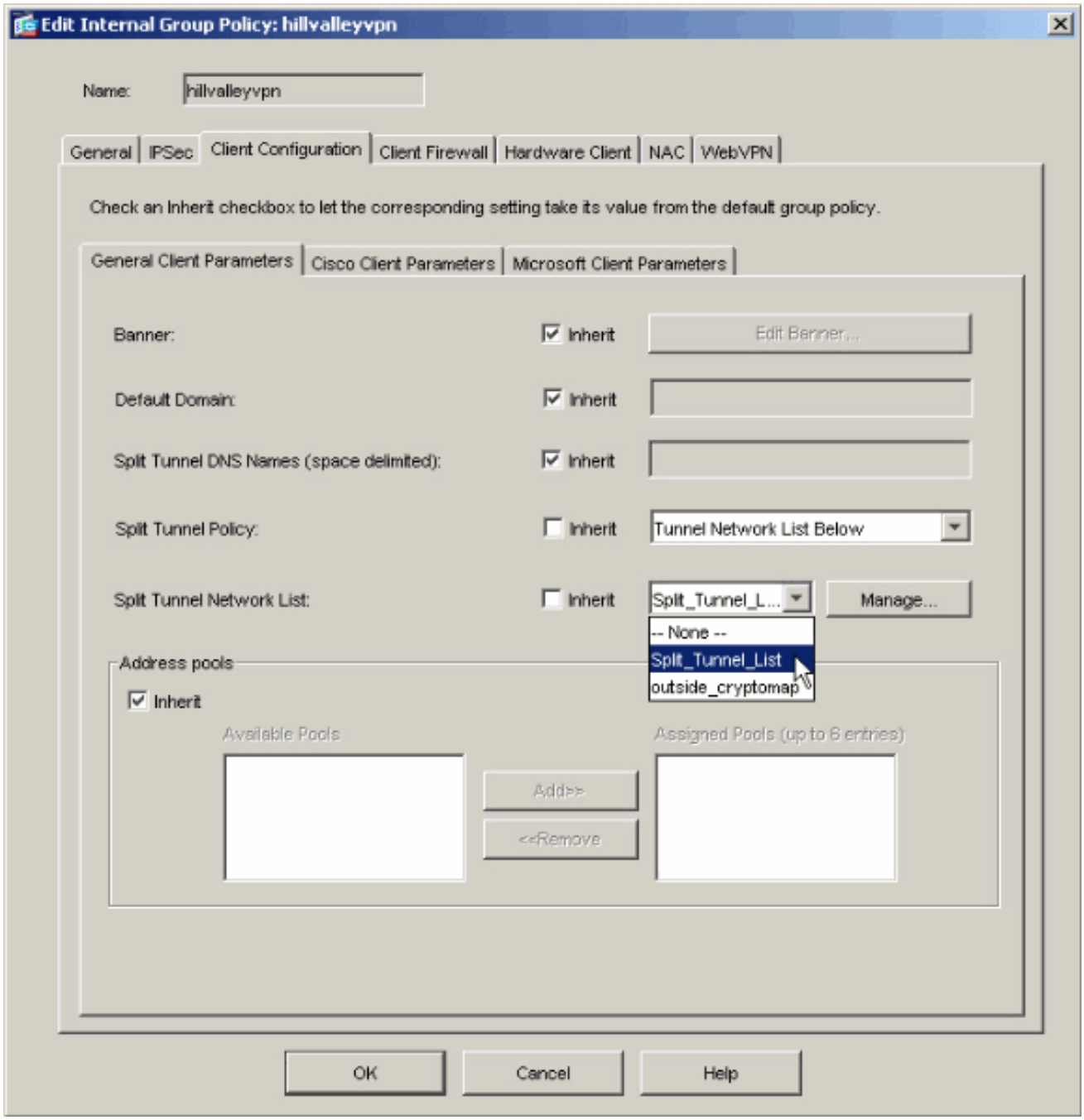


9. Cliquez sur **OK** afin de quitter l'ACL Manager.

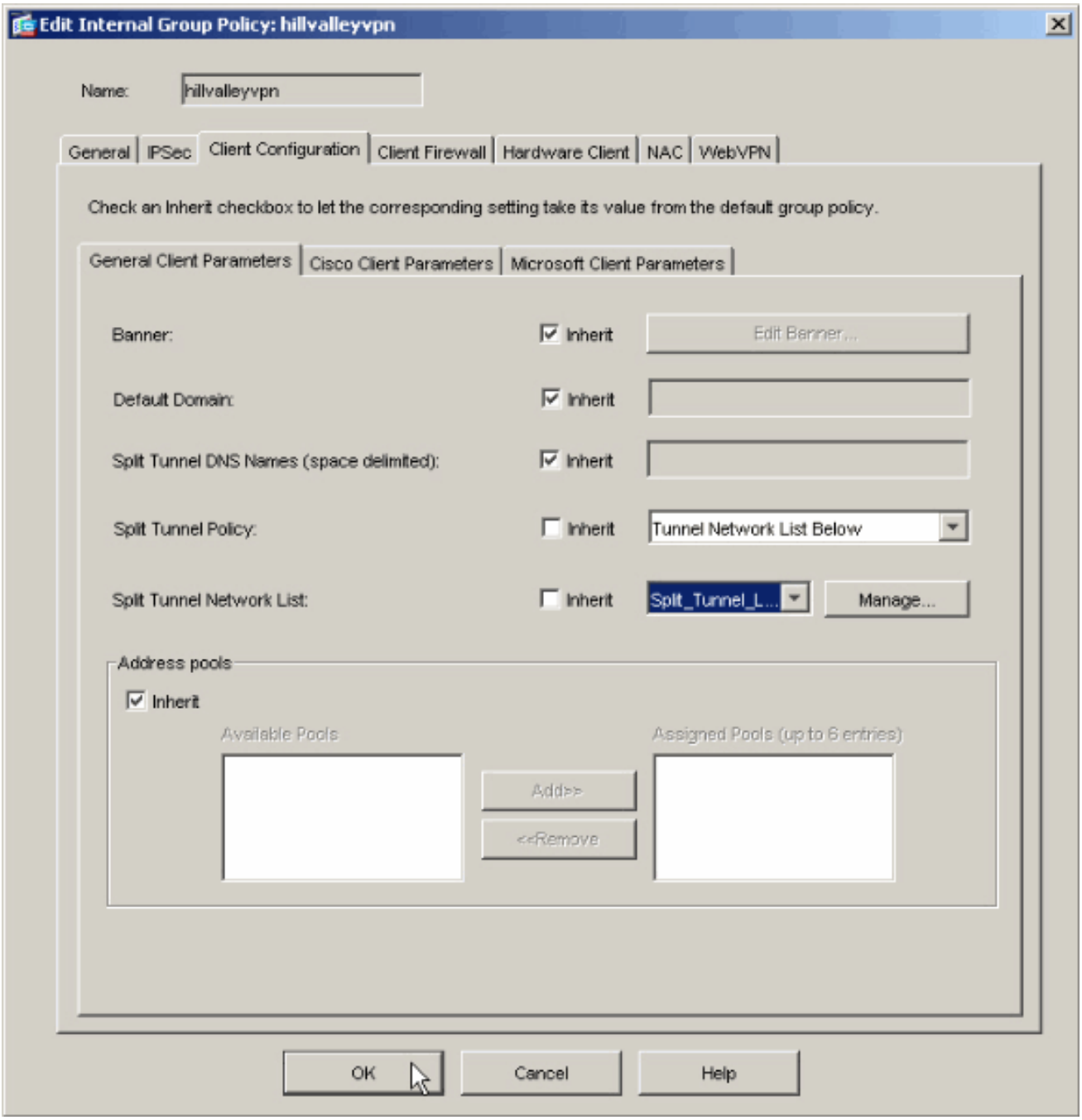


10. Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel

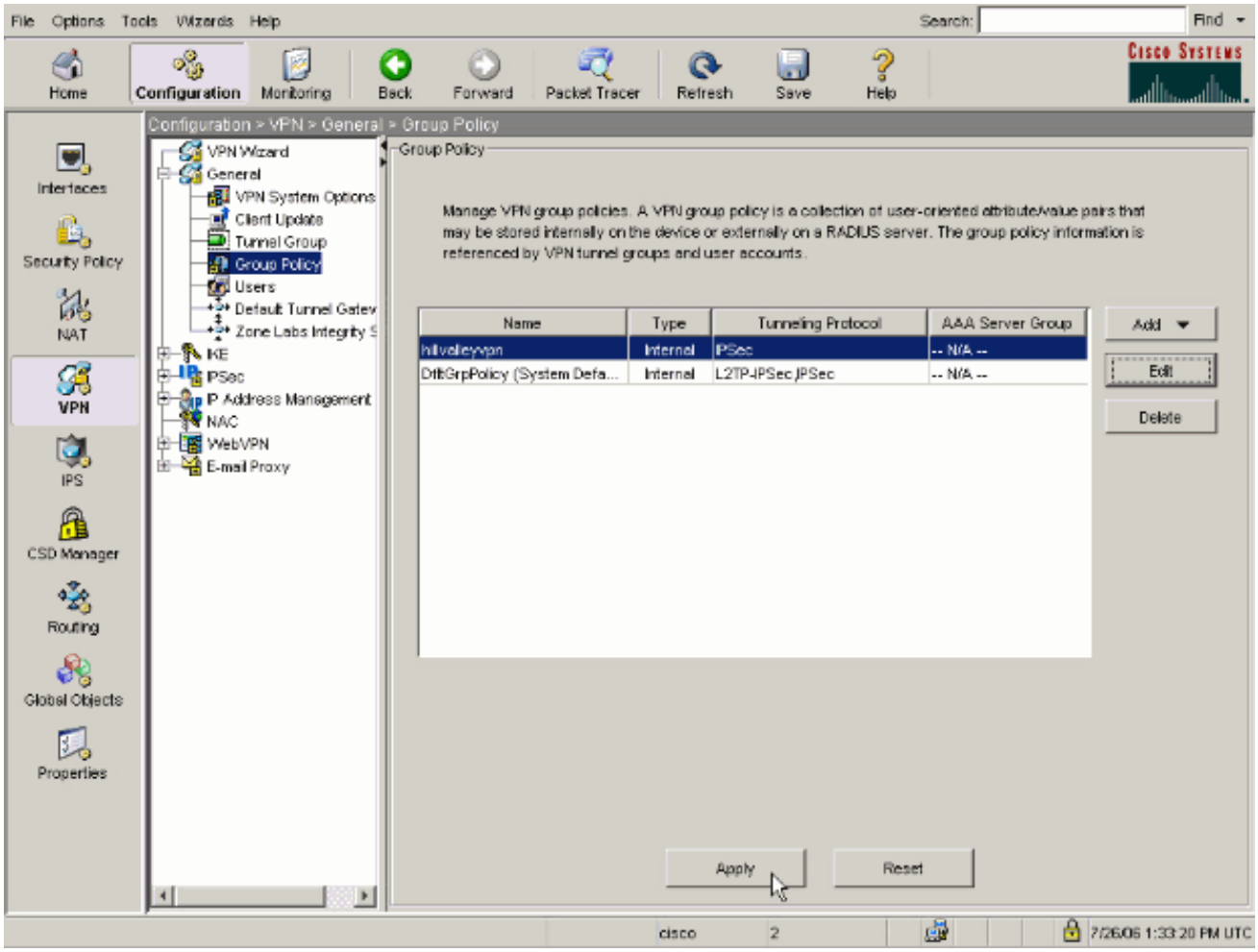
Network
List.



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



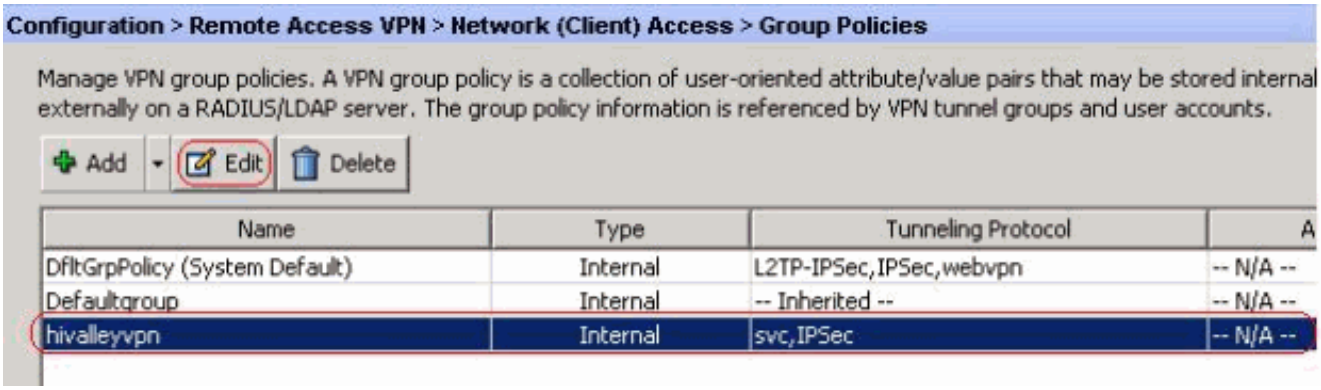
12. Cliquez sur **Apply** puis sur **Send** (s'il y a lieu) afin d'envoyer les commandes à l'ASA.



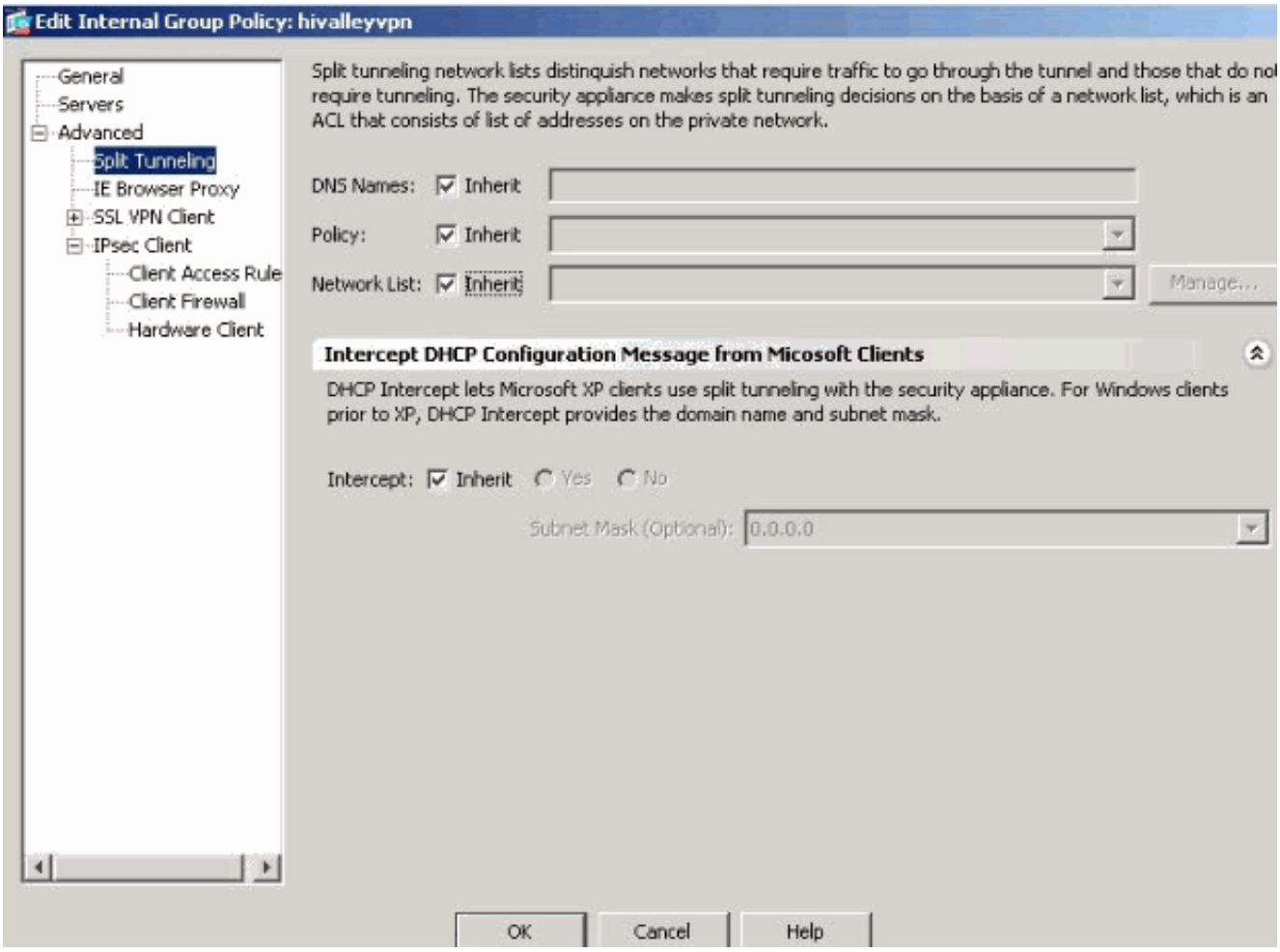
Configurer ASA 8.x avec Adaptive Security Device Manager (ASDM) 6.x

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

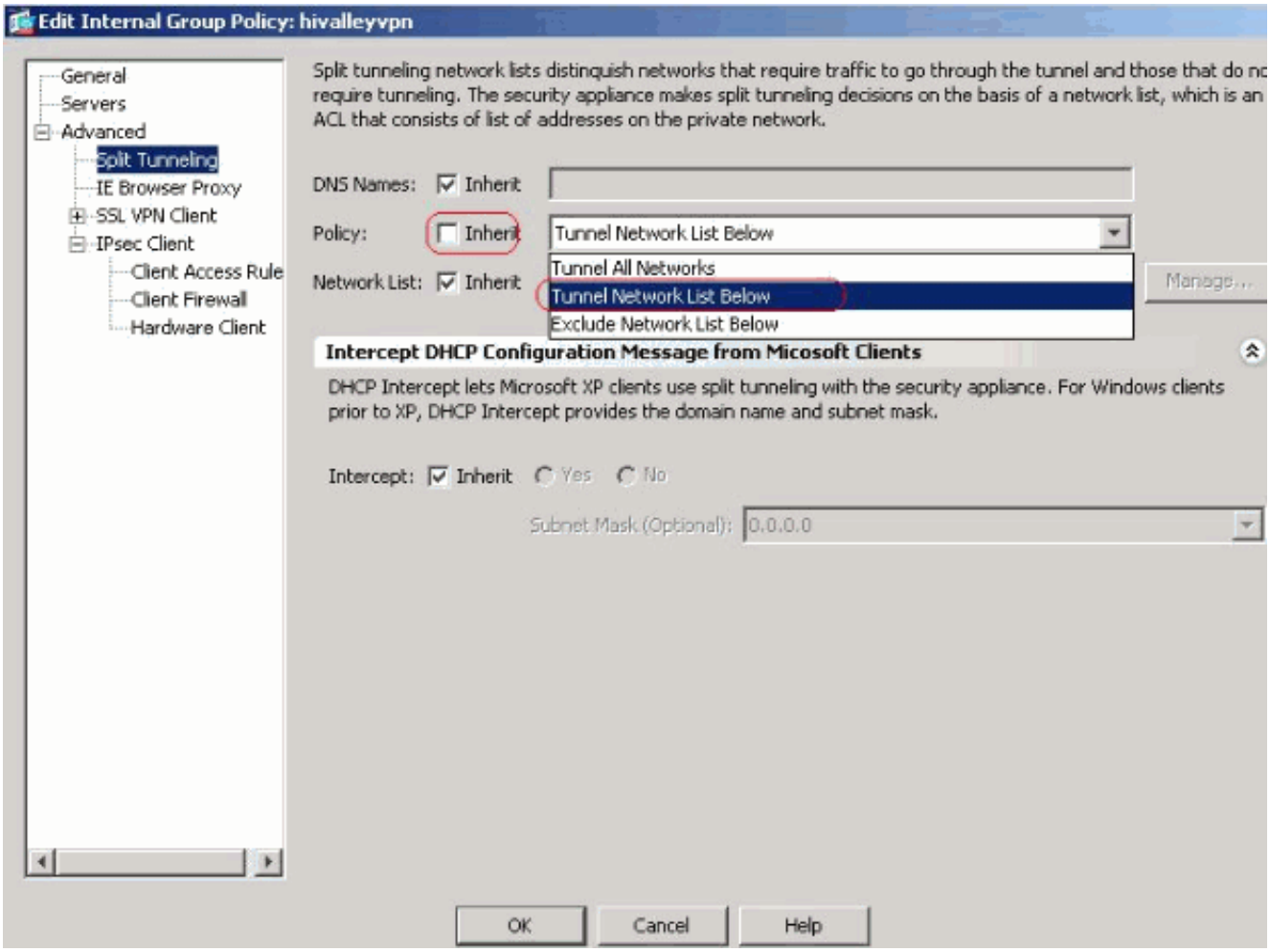
1. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**, et choisissez la stratégie de groupe dans laquelle vous souhaitez activer l'accès au LAN local. Cliquez alors sur **Edit**.



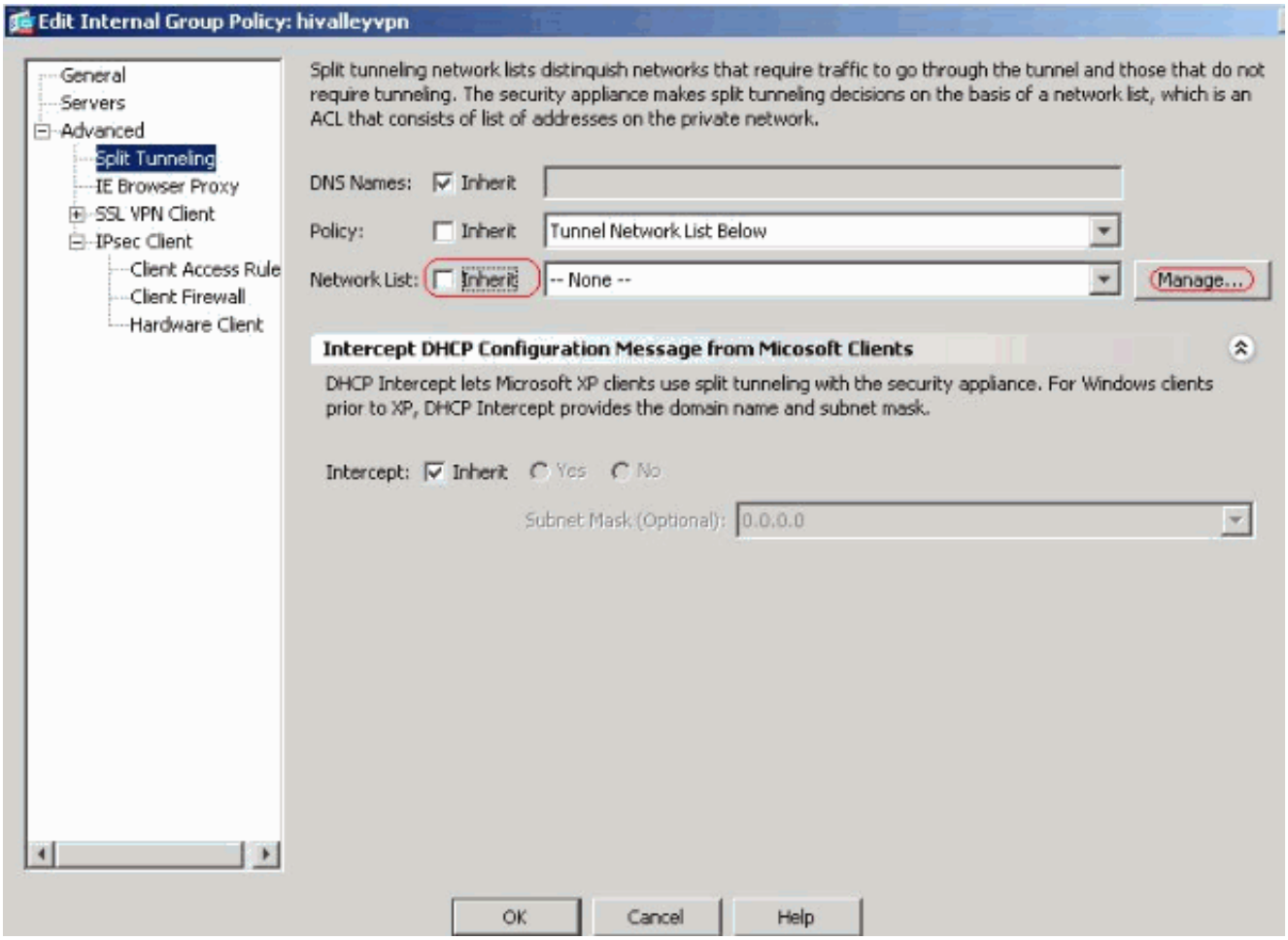
2. Cliquez sur **Split Tunneling**.



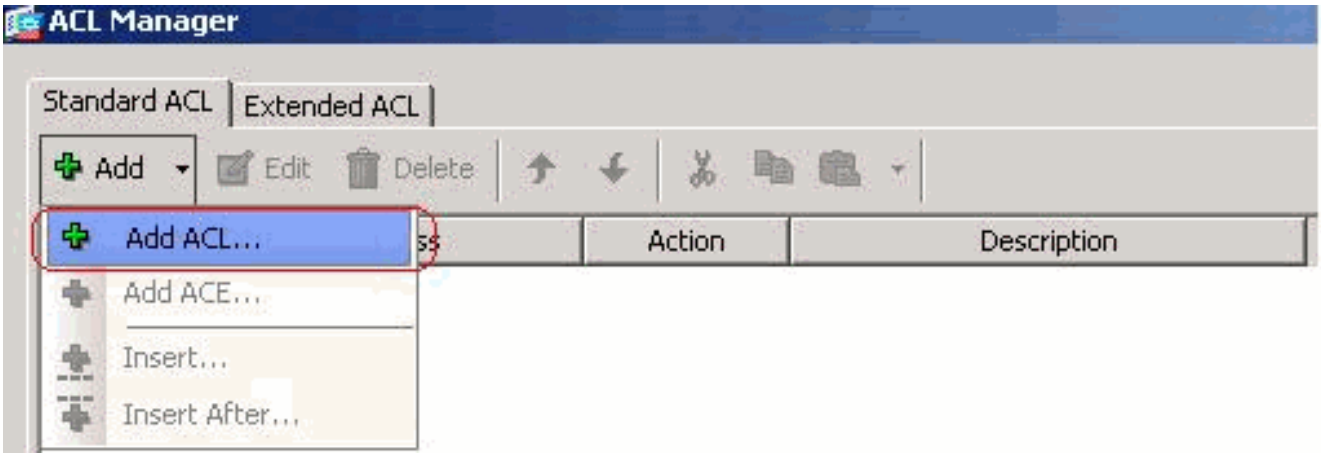
3. Désactivez la case **Inherit** pour la stratégie Split Tunnel Policy et choisissez **Tunnel Network List Below**.



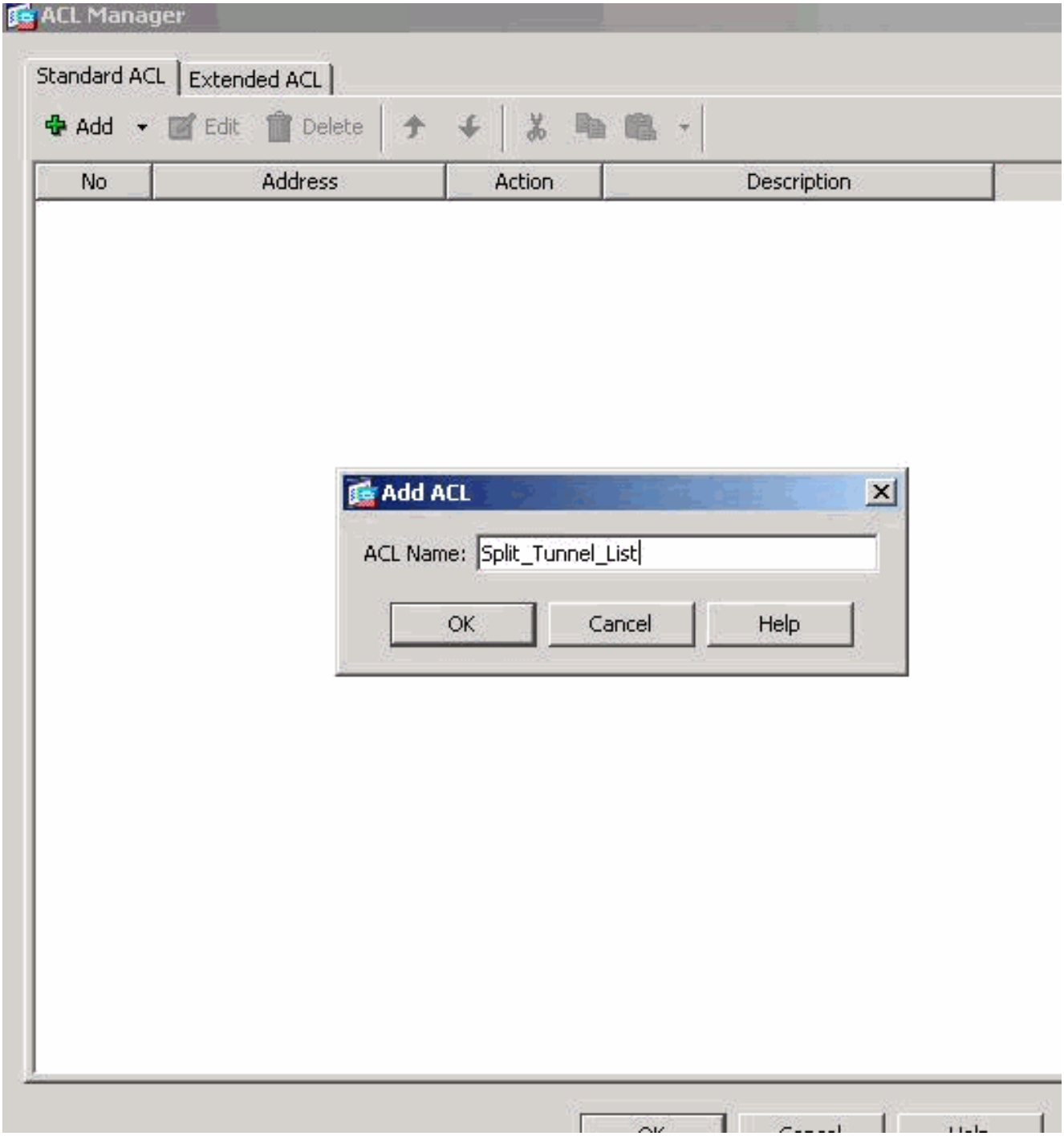
4. Désactivez la case **Inherit** pour la liste Split Tunnel Network List, puis cliquez sur **Manage** pour lancer l'ACL
   Manager.



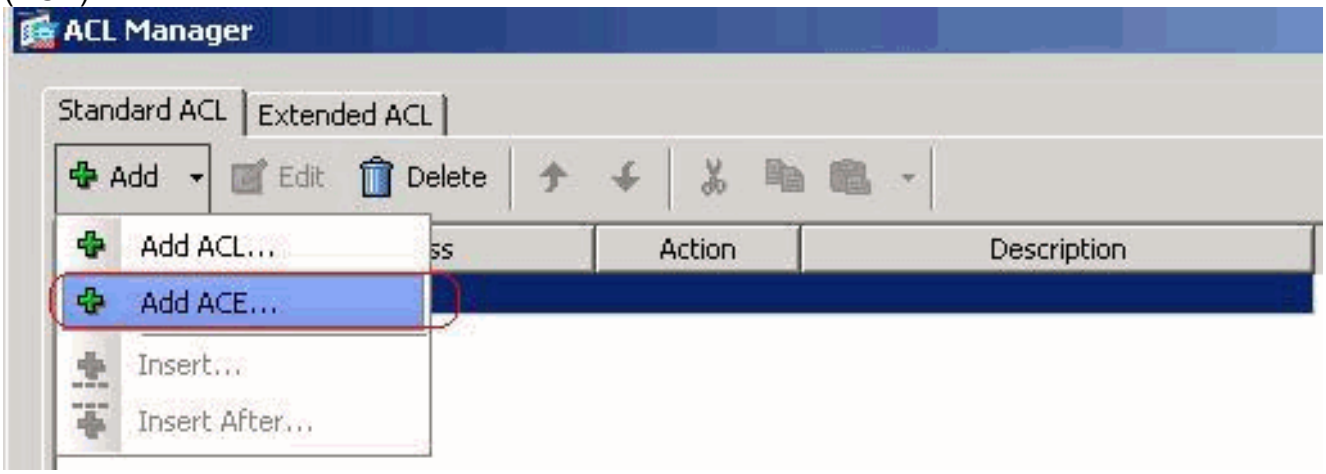
5. Chez le gestionnaire d'ACL, choisissez **ajoutent > ajoutent l'ACL…** afin de créer une nouvelle liste
d'accès.



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

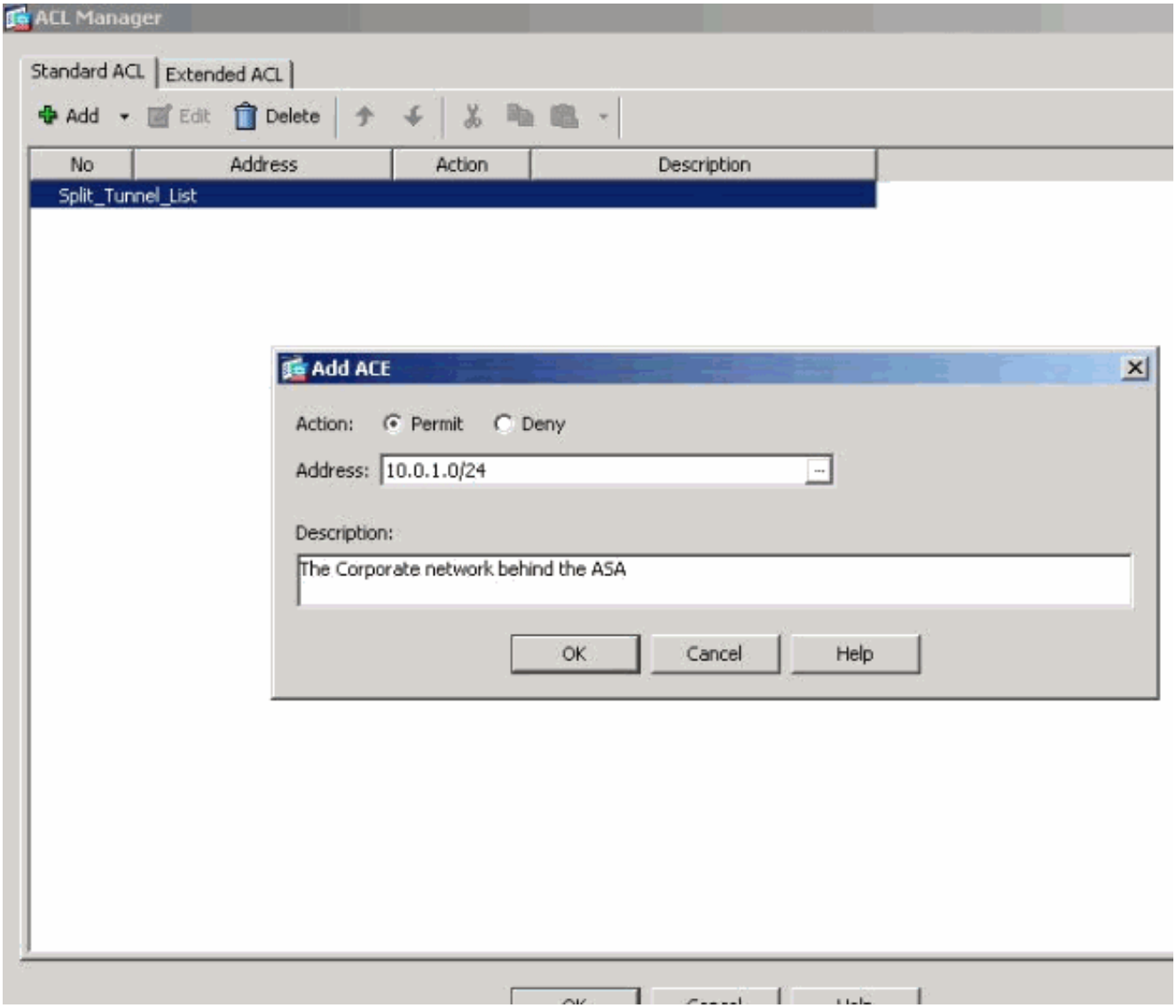


7. Une fois que l'ACL est créé, choisissez **Add > Add ACE...** afin d'ajouter une Entrée de contrôle d'accès
(ACE).

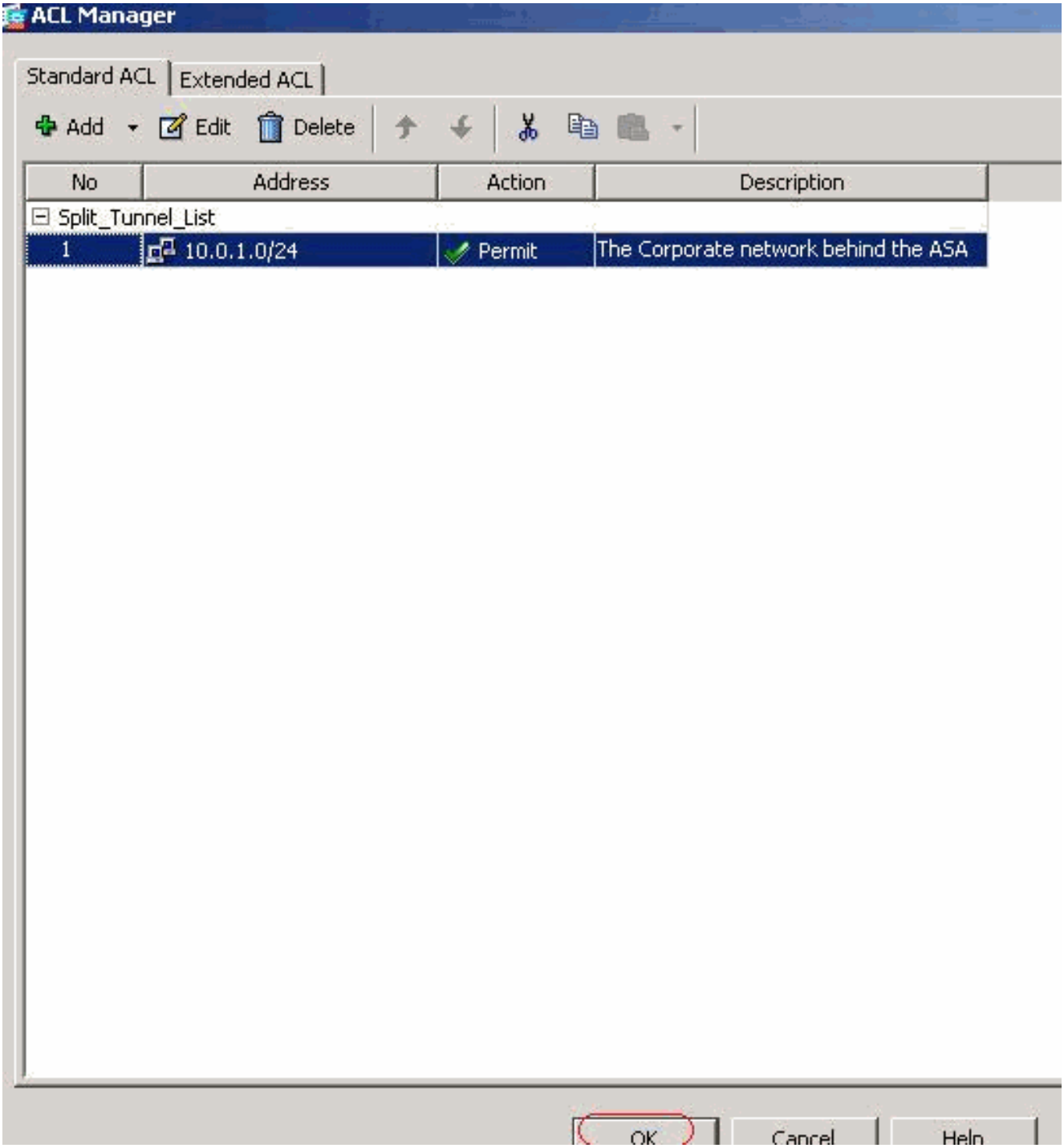


8. Définissez l'ACE qui correspond au LAN derrière l'ASA. Dans ce cas, le réseau est

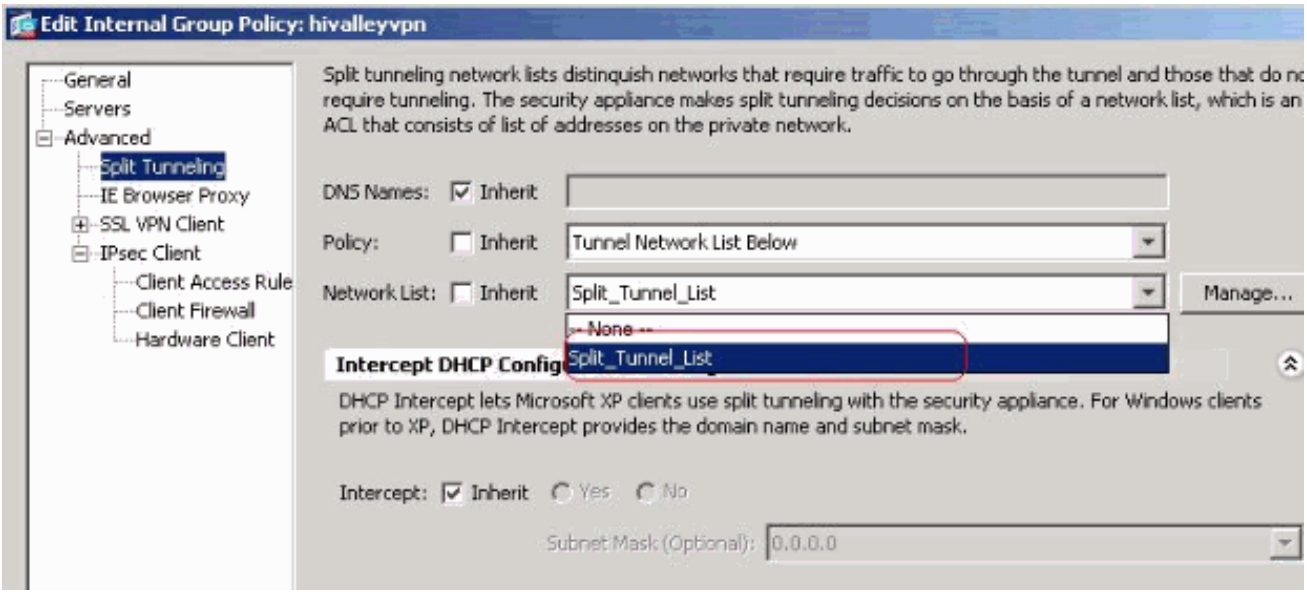
10.0.1.0/24.Cliquez sur la case d'option **Permit**.Choisissez l'adresse réseau avec le masque **10.0.1.0/24**.(Facultatif) Fournissez une description.Cliquez sur **OK**.



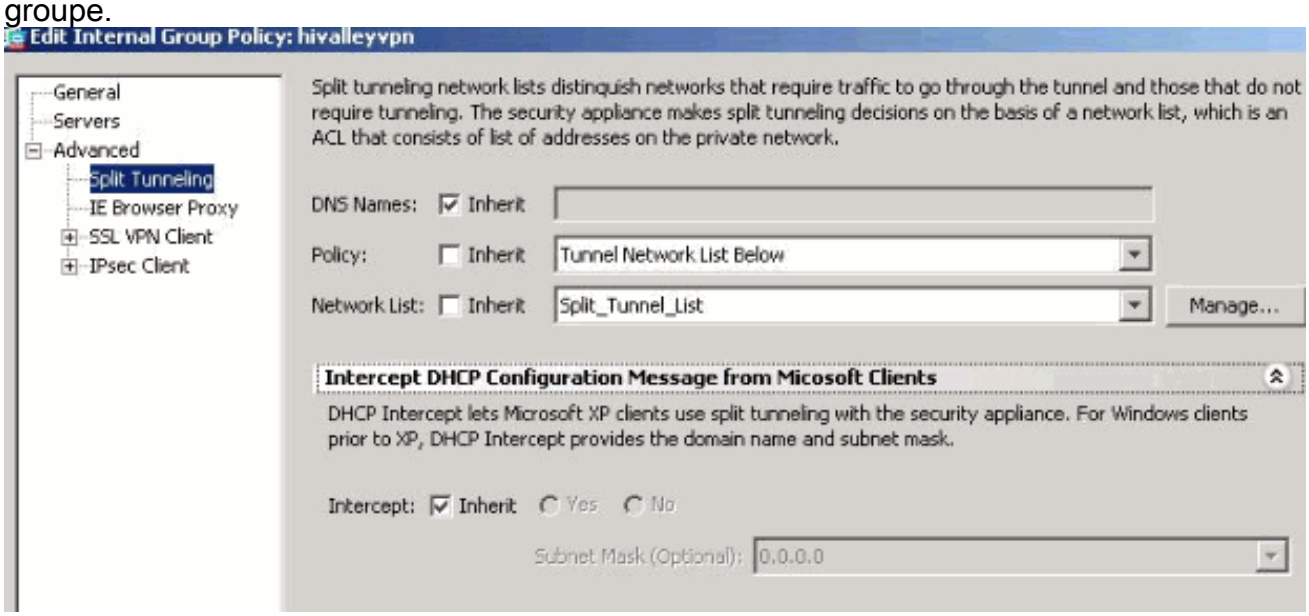
9. Cliquez sur **OK** afin de quitter l'ACL Manager.



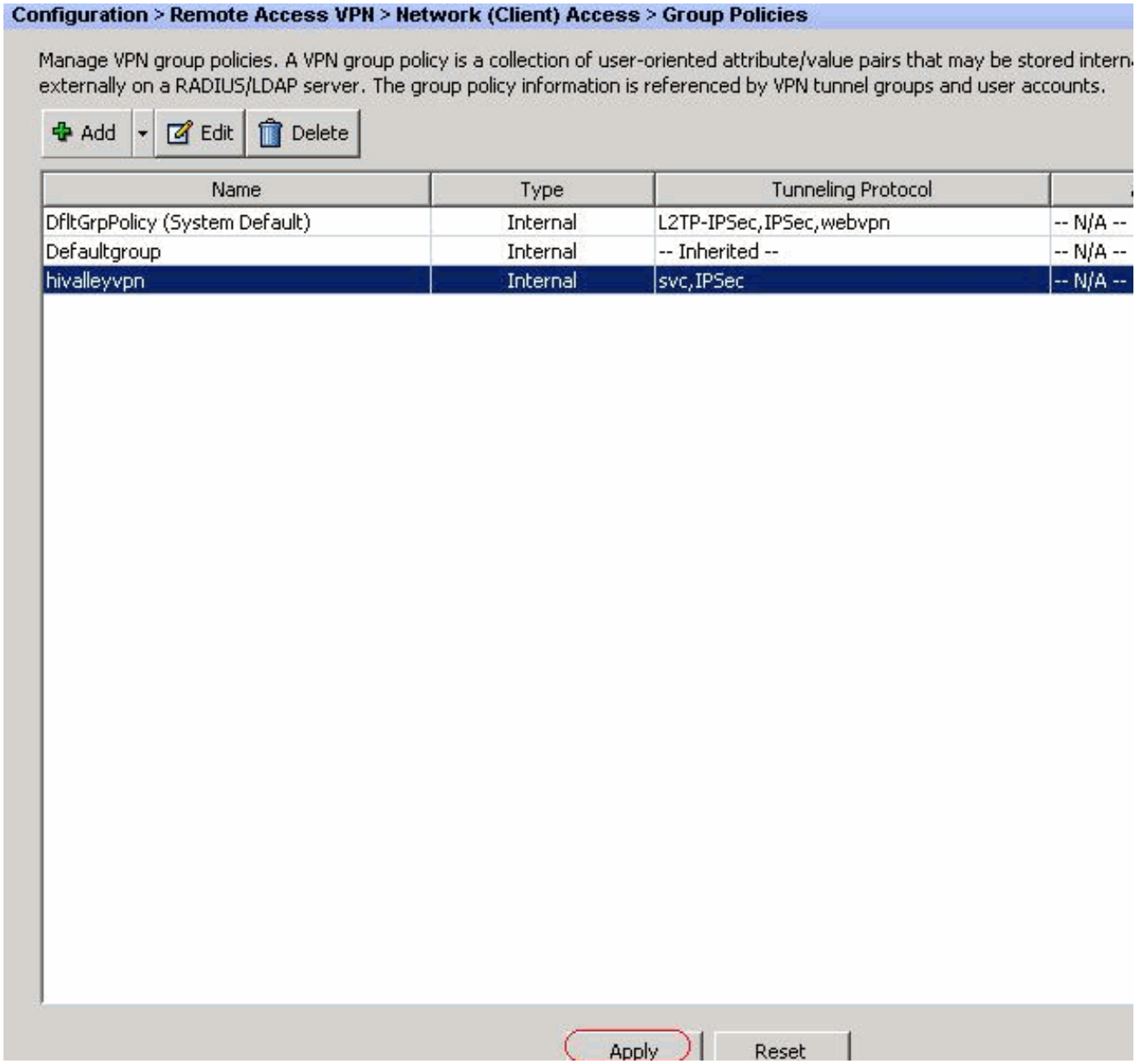
10. Assurez-vous que l'ACL que vous venez de créer est sélectionné pour la liste Split Tunnel Network
List.



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



12. 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 de la transmission tunnel partagée est identique pour ASA 7.x et 8.x.

1. Passez en mode de configuration.`ciscoasa>`**`enable`** `Password: ******** ciscoasa#`**`configure terminal`** `ciscoasa(config)#`
2. Créez la liste d'accès qui définit le réseau derrière ASA.`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`**
3. Entrez le mode de configuration Group Policy pour la stratégie que vous souhaitez modifier.`ciscoasa(config)#`**`group-policy hillvalleyvpn attributes`** `ciscoasa(config-group-policy)#`
4. Spécifiez la stratégie de transmission tunnel partagée. Dans ce cas, la stratégie est **tunnelspecified**.`ciscoasa(config-group-policy)#`**`split-tunnel-policy tunnelspecified`**
5. Spécifiez la liste d'accès de transmission tunnel partagée. Dans ce cas, la liste est **Split_Tunnel_List**.`ciscoasa(config-group-policy)#`**`split-tunnel-network-list value`**

`Split_Tunnel_List`

6. Émettez la commande suivante :`ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes`
7. Associez la stratégie de groupe au groupe de tunnels`ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn`
8. Quittez les deux modes de configuration.`ciscoasa(config-group-policy)#exit ciscoasa(config)#exit ciscoasa#`
9. Sauvegardez la configuration dans une mémoire vive non volatile (NVRAM) et appuyez **Enter** lorsqu'on vous invite à spécifier le nom de fichier source.`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 :

1. Créez la liste d'accès qui définit le réseau derrière PIX.
   `PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0`
2. Créez un groupe vpn *vpn3000* et spécifiez l'ACL de transmission tunnel partagée pour ce groupe comme illustré :`PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List`
   Remarque: Référez-vous au Cisco Secure PIX Firewall 6.x et Client VPN Cisco 3.5 pour Windows avec l'authentification RADIUS IAS de Microsoft Windows 2000 et 2003 pour plus d'informations sur la configuration du VPN d'accès à distance pour PIX 6.x.

Vérifiez

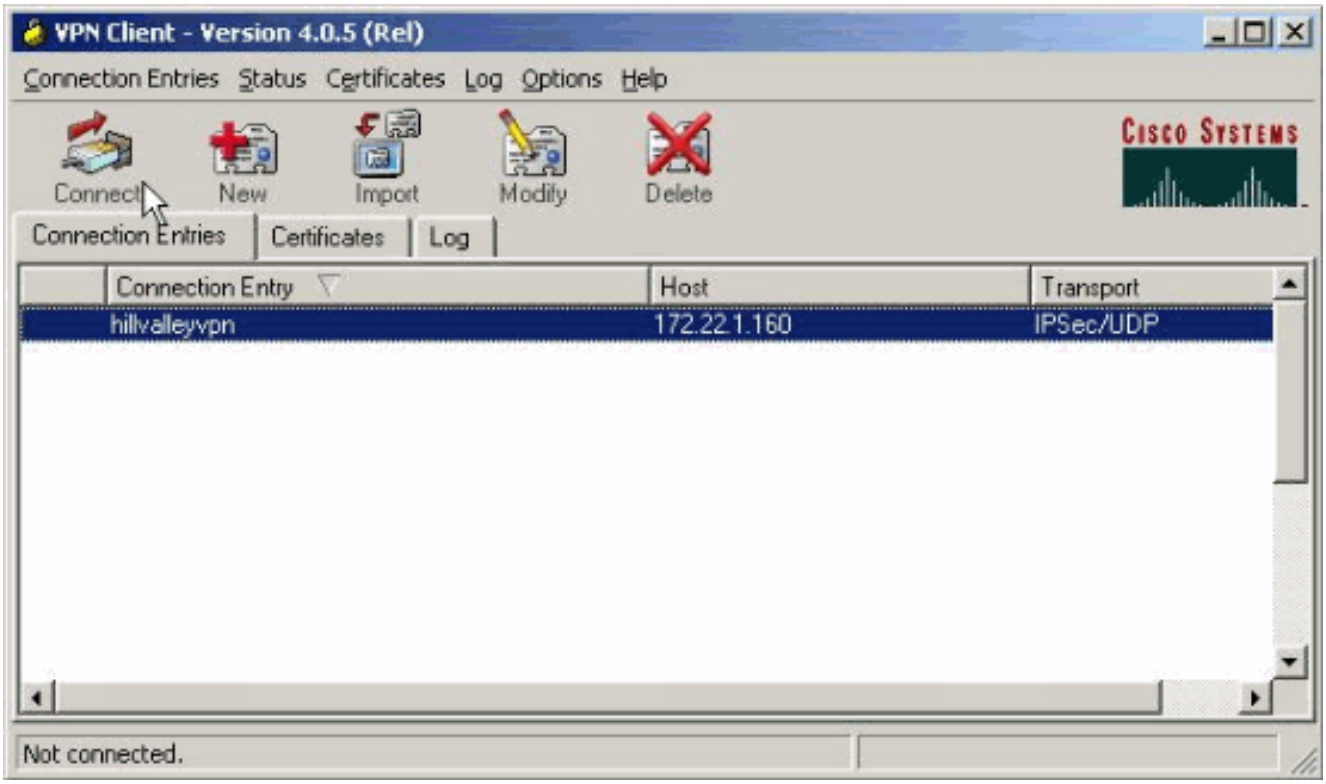
Suivez les étapes décrites dans ces sections afin de vérifier votre configuration.

- 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

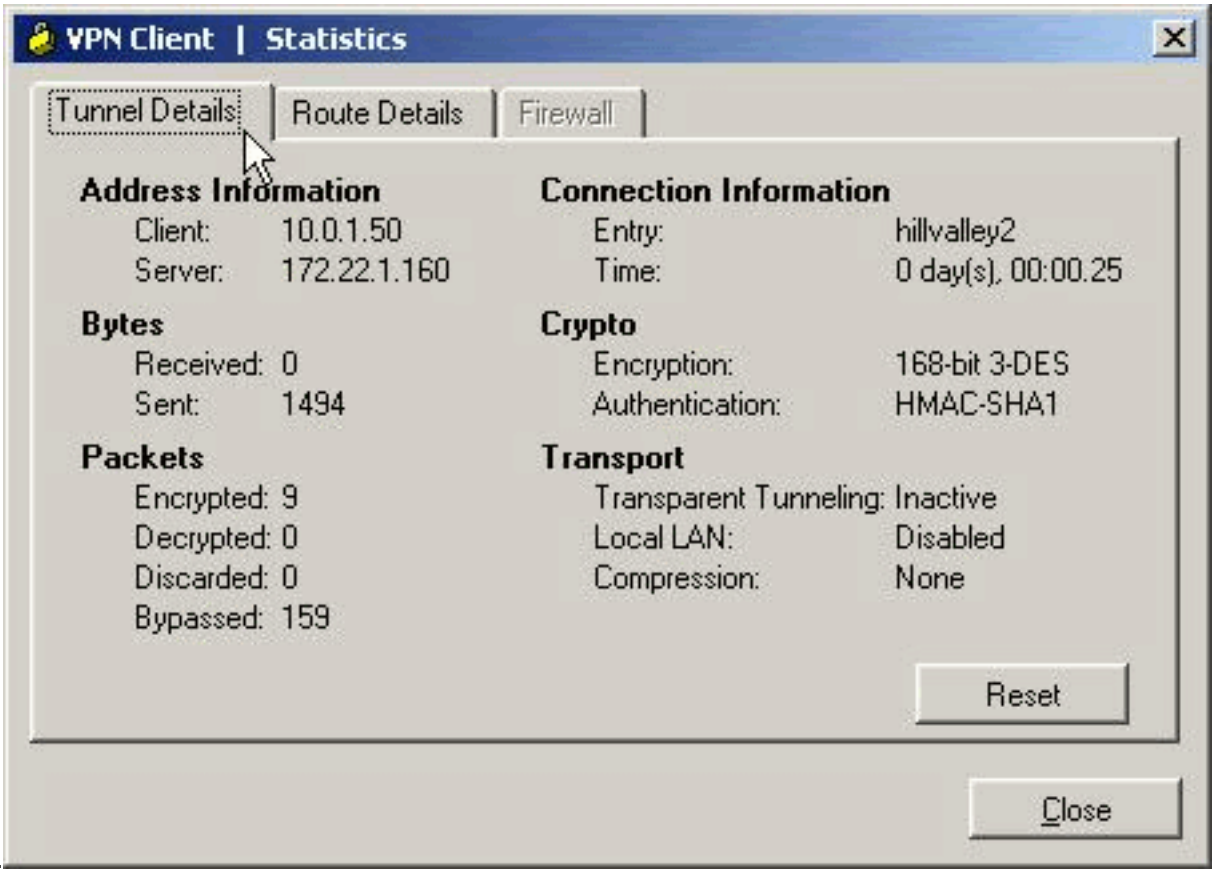
Connectez votre client VPN au concentrateur VPN afin de vérifier votre configuration.

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



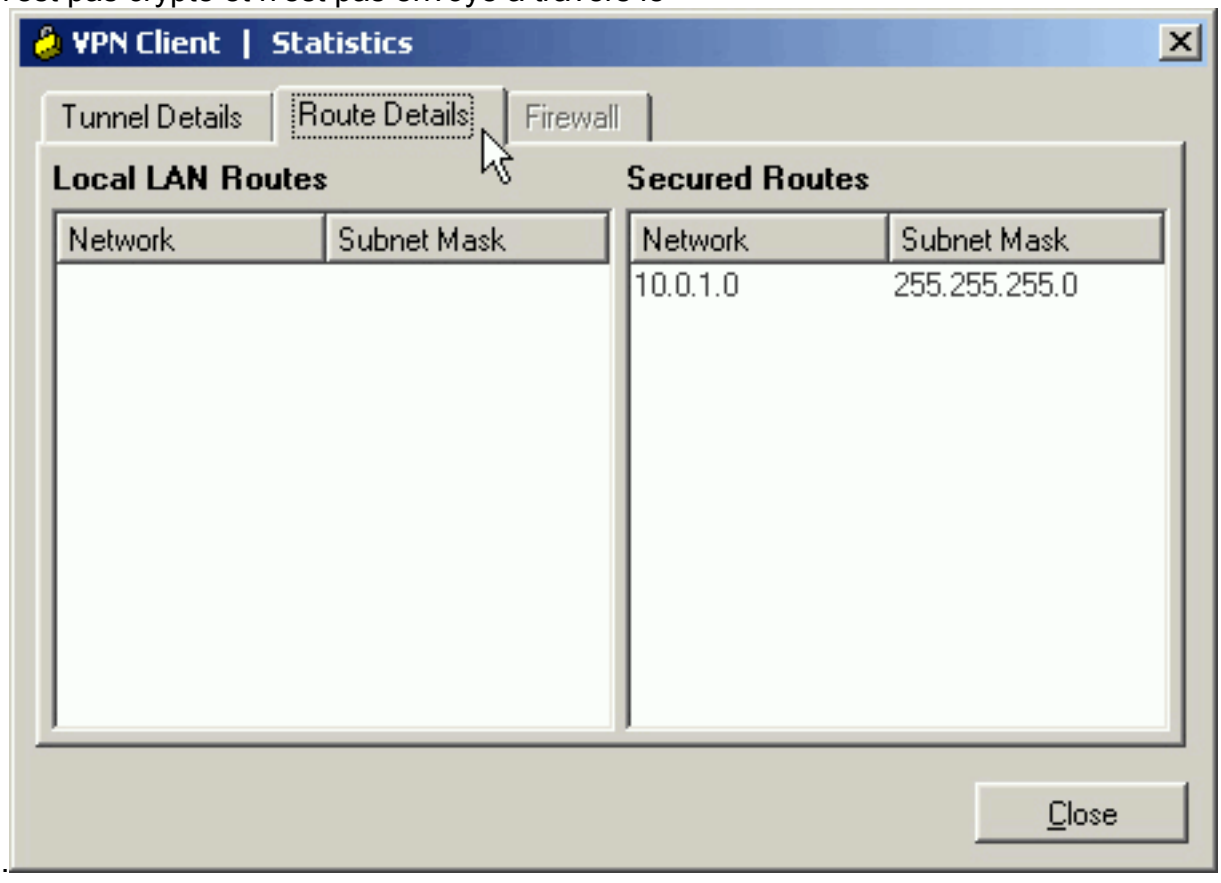
2. Entrez dans vos informations d'identification.

3. 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.

4. 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

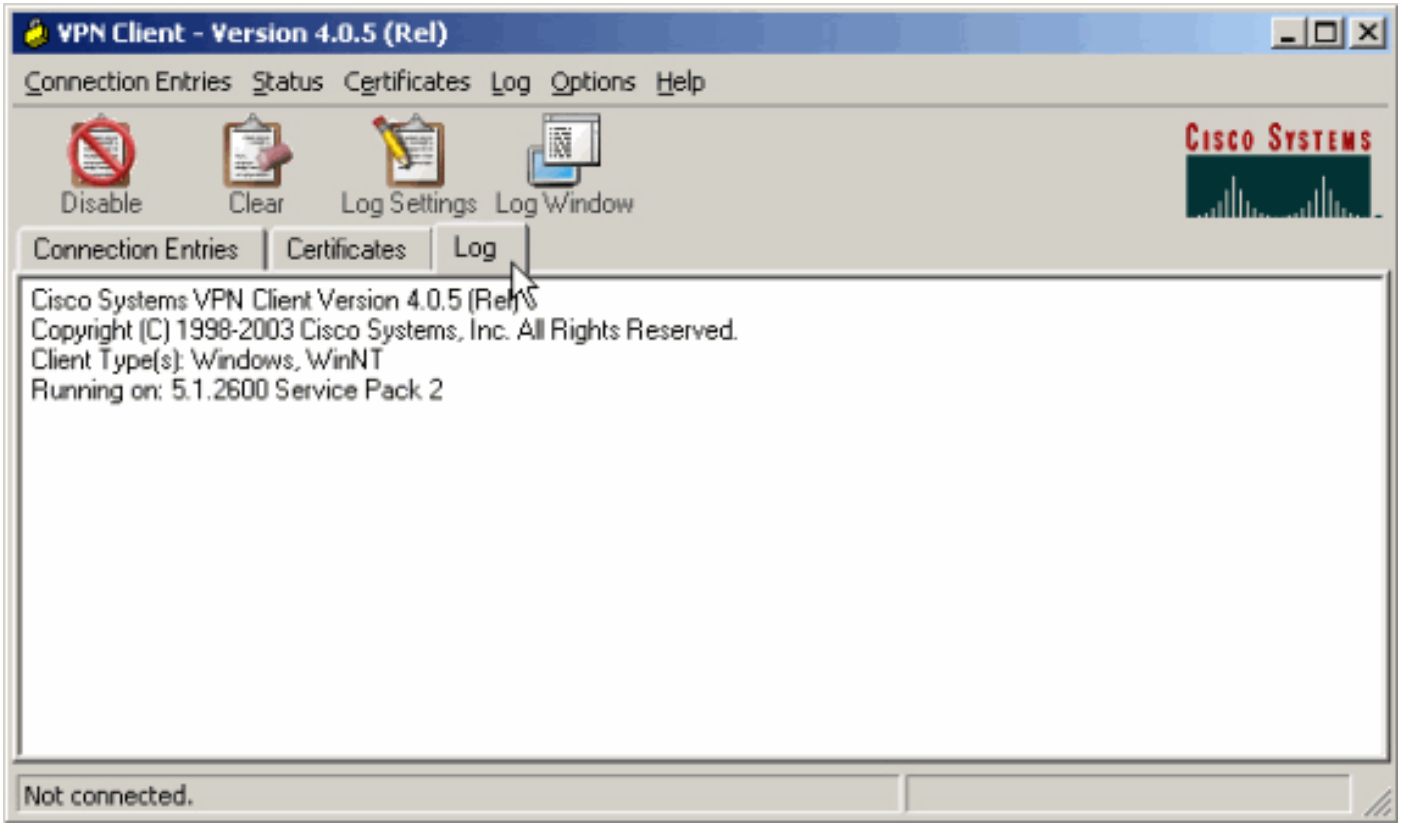


tunnel.

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/6IKE/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.

```
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
```

Dépannez

Limite avec le nombre des entrées dans un ACL de tunnel partagé

Il y a une restriction avec le nombre d'entrées dans un ACL utilisé pour le tunnel partagé. Il est recommandé pour ne pas utiliser plus de 50-60 entrées d'ACE pour la fonctionnalité satisfaisante. Vous êtes informé implémenter la caractéristique de sous-réseautage pour couvrir une plage des 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
- Support et documentation techniques - Cisco Systems