Exemple de configuration d'accès client VPN et client AnyConnect au LAN local

Contenu

Introduction

Ce document décrit comment autoriser le client VPN Cisco ou le client de mobilité sécurisée Cisco AnyConnect à **seulement** accéder à son réseau local tout en le connectant à un appareil de sécurité adaptatif Cisco (ASA) 5500 ou à la gamme ASA 5500-X. Cette configuration permet aux clients VPN Cisco ou au client Cisco AnyConnect Secure Mobility d'accéder en toute sécurité aux ressources de l'entreprise via IPsec, SSL (Secure Sockets Layer) ou IKEv2 (Internet Key Exchange Version 2), tout en permettant au client d'effectuer des activités telles que l'impression à l'emplacement du client. Si c'est autorisé, le trafic destiné à l'Internet est encore tunnelisé vers l'ASA.

> Remarque: Ce n'est pas une configuration pour la Transmission tunnel partagée, où le client de routage a l'accès à Internet décrypté tandis qu'il est connecté à l'ASA ou au PIX. Référez-vous à PIX/ASA 7.x : Autoriser la transmission tunnel partagée pour les clients VPN dans l'exemple de configuration ASA pour des informations sur la configuration de la transmission tunnel partagée sur l'ASA.

Conditions préalables

Conditions requises

Ce document suppose qu'une configuration VPN fonctionnelle d'Accès à distance existe déjà sur l'ASA.

Référez-vous à Exemple de configuration de PIX/ASA 7.x en tant que serveur VPN distant utilisant ASDM pour le client VPN Cisco si l'un d'eux n'est pas déjà configuré.

Référez-vous à Exemple de configuration d'un accès VPN ASA 8.x avec le client VPN SSL AnyConnect pour le client Cisco AnyConnect Secure Mobility si l'un d'eux n'est pas déjà configuré.

Components Used

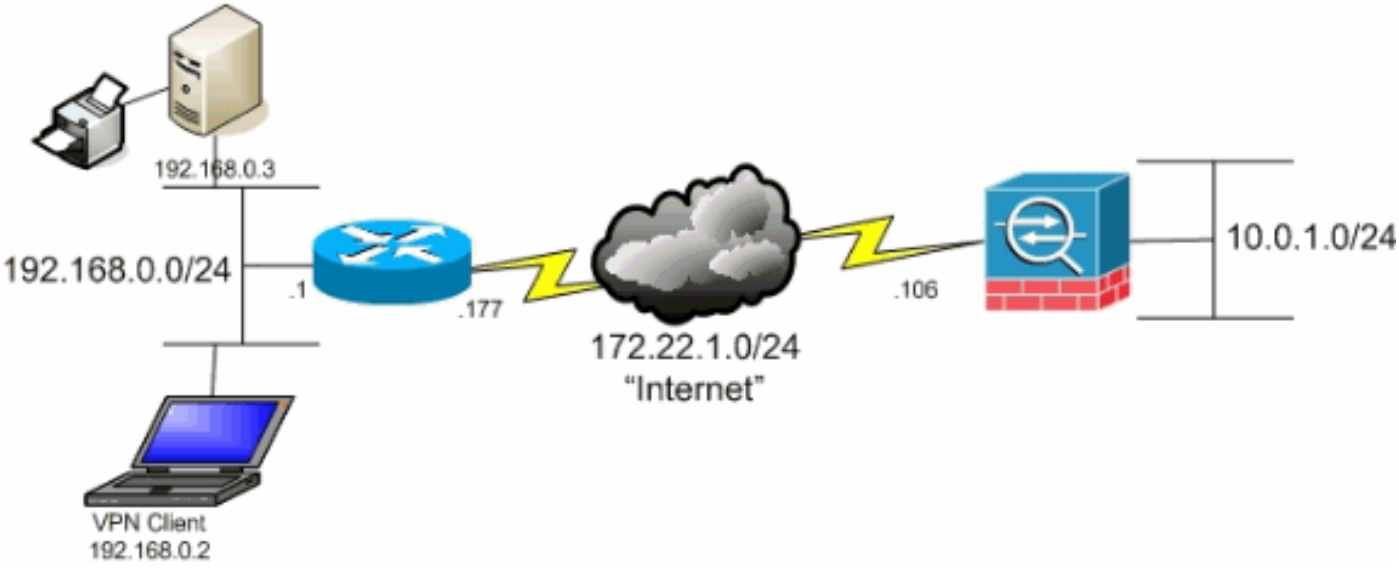
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme Cisco ASA 5500 Version 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) version 7.1(6)
- Client VPN Cisco version 5.0.07.0440
- Client Cisco AnyConnect Secure Mobility Version 3.1.05152

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Le client se trouve sur un réseau SOHO (Small Office / Home Office) classique et se connecte via Internet au bureau central.



Informations générales

Contrairement à un scénario classique de fractionnement en canaux dans lequel tout le trafic Internet est envoyé sans cryptage, lorsque vous activez l'accès LAN local pour les clients VPN, il permet à ces clients de communiquer sans cryptage avec uniquement les périphériques du réseau sur lequel ils se trouvent. Par exemple, un client qui est autorisé à accéder au LAN local alors qu'il est connecté à l'ASA à partir de son domicile peut imprimer sur sa propre imprimante,

mais ne peut pas accéder à Internet sans envoyer d'abord le trafic via le tunnel.

Une liste d'accès est utilisée afin de permettre l'accès de réseau local LAN plus ou moins de la même façon que la Transmission tunnel partagée est configurée sur l'ASA. Cependant, au lieu de définir quels réseaux *doivent être* cryptés, la liste d'accès dans ce cas définit quels réseaux *ne doivent pas être* cryptés. En outre, à la différence du scénario de Transmission tunnel partagée, les réseaux réels dans la liste n'ont pas besoin d'être connus. Au lieu de cela, l'ASA fournit un réseau par défaut de 0.0.0.0/255.255.255.255, ce qui signifie le réseau local du client.

> Remarque: Lorsque le client est connecté et configuré pour l'accès LAN local, vous *ne pouvez pas imprimer ou parcourir par nom* sur le LAN local. Cependant, vous pouvez naviguer ou imprimer par adresse IP. Consultez la section Dépannage de ce document pour plus d'informations ainsi que les solutions de contournement de cette situation.

Configurer l'accès LAN local pour les clients VPN ou le client AnyConnect Secure Mobility

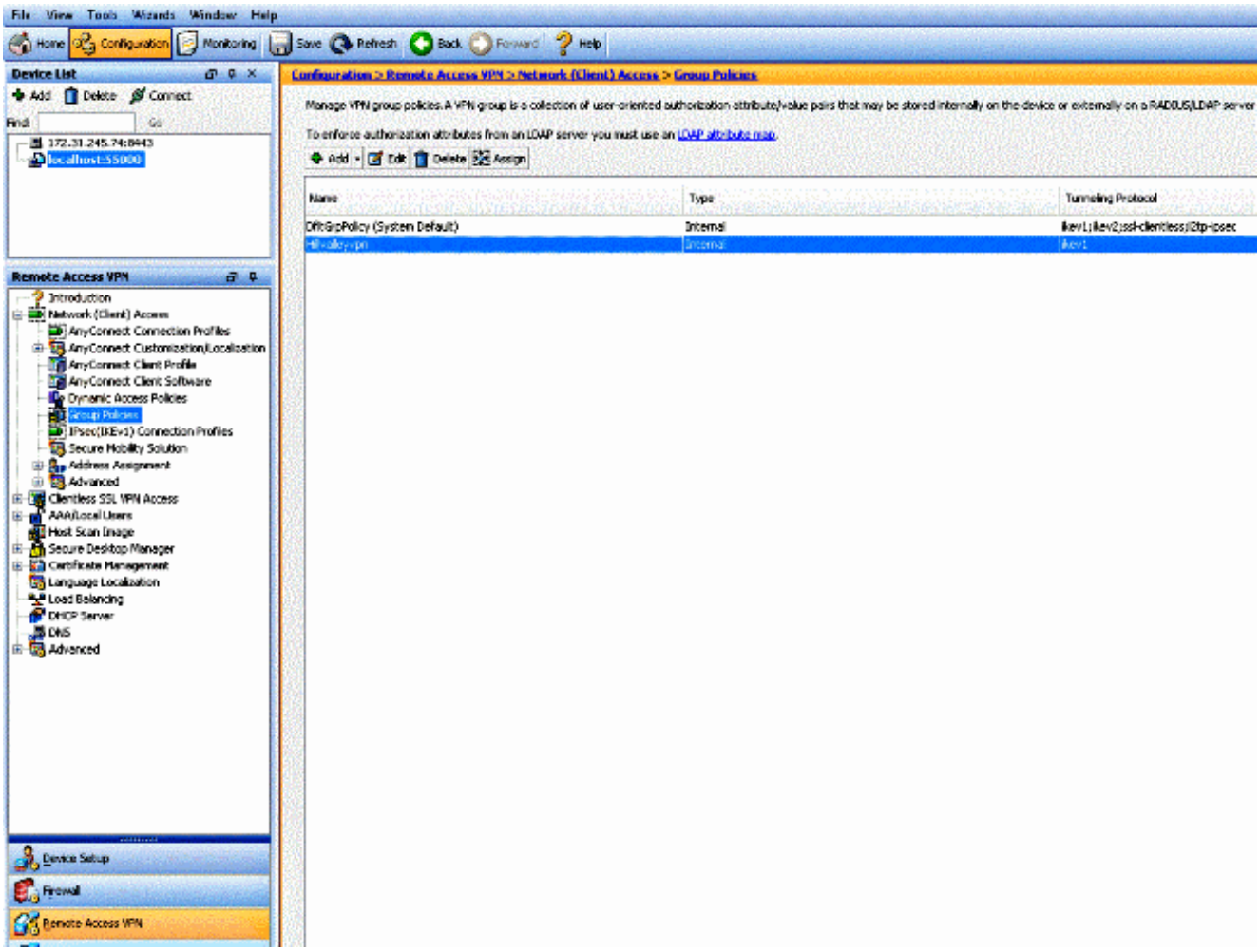
Effectuez ces tâches afin de permettre aux clients VPN Cisco ou aux clients de mobilité sécurisée Cisco AnyConnect d'accéder à leur LAN local lors de leur connexion à l'ASA :

- Configurer l'ASA via l'ASDM ou Configurer l'ASA via l'interface de ligne de commande
- Configurer le client Cisco AnyConnect Secure Mobility

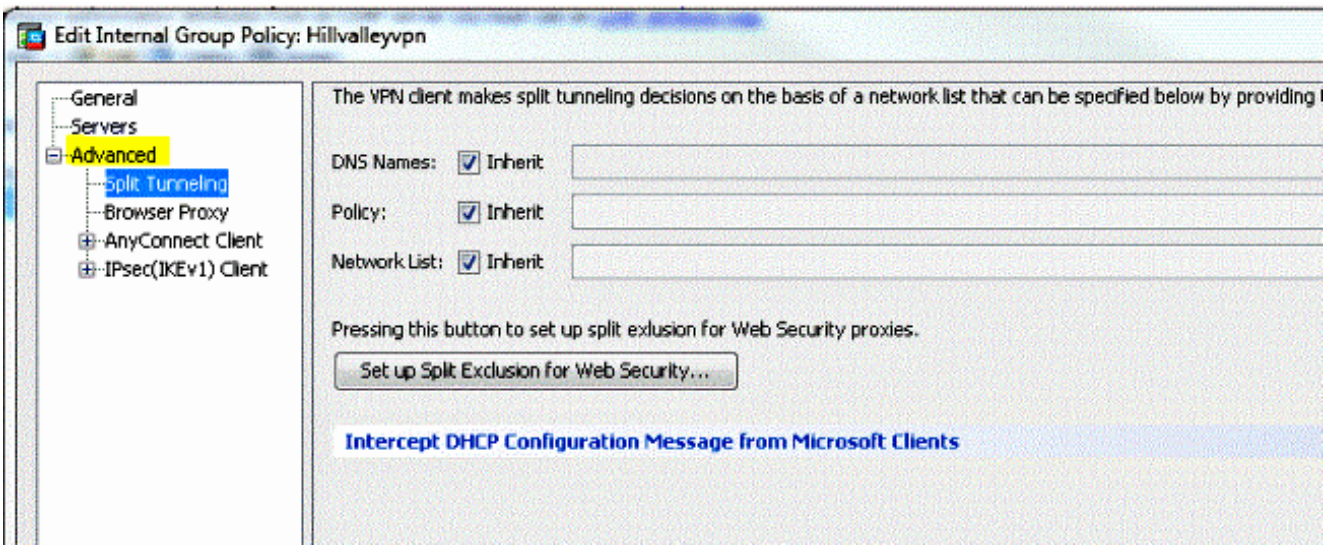
Configurez l'ASA par l'intermédiaire de l'ASDM

Complétez ces étapes dans l'ASDM afin de permettre aux clients VPN d'avoir un accès LAN local lors de leur connexion à l'ASA :

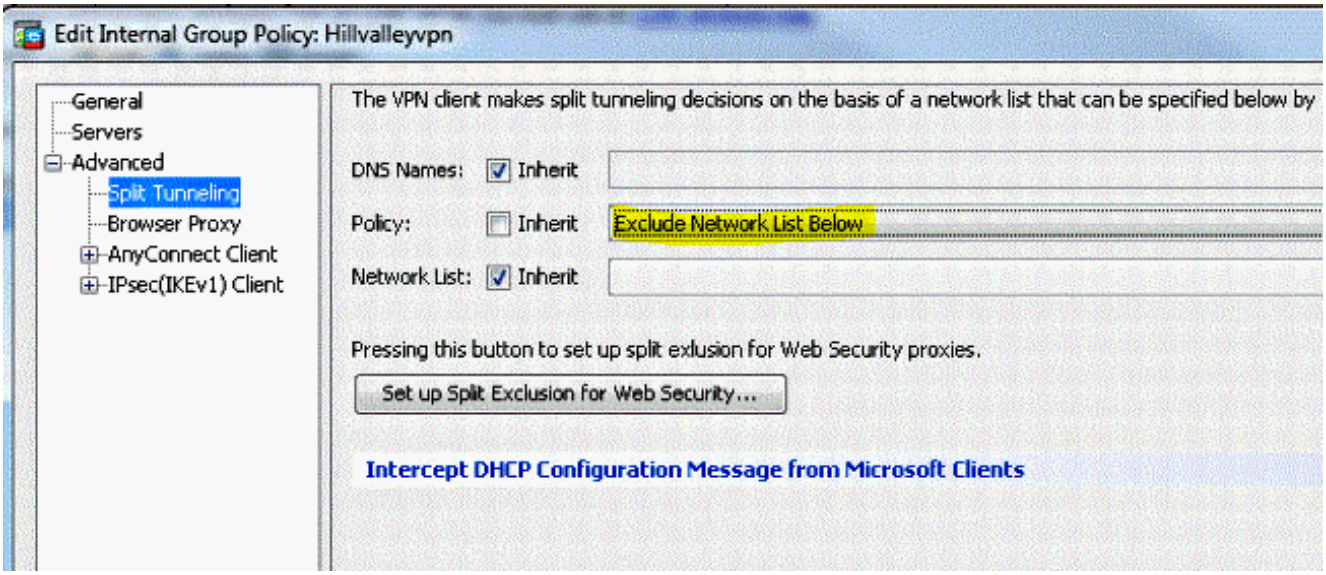
1. Choisissez **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** et sélectionnez la stratégie de groupe dans laquelle vous souhaitez activer l'accès LAN local. Cliquez alors sur Edit.



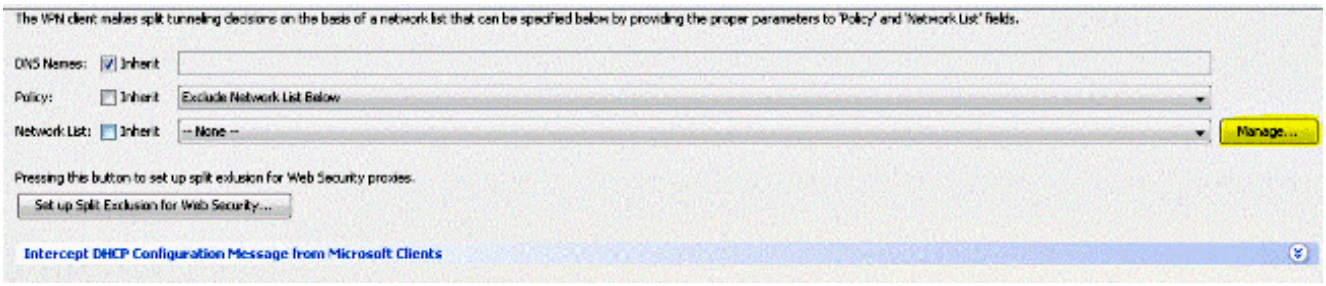
2. Accédez à **Advanced > Split Tunneling**.



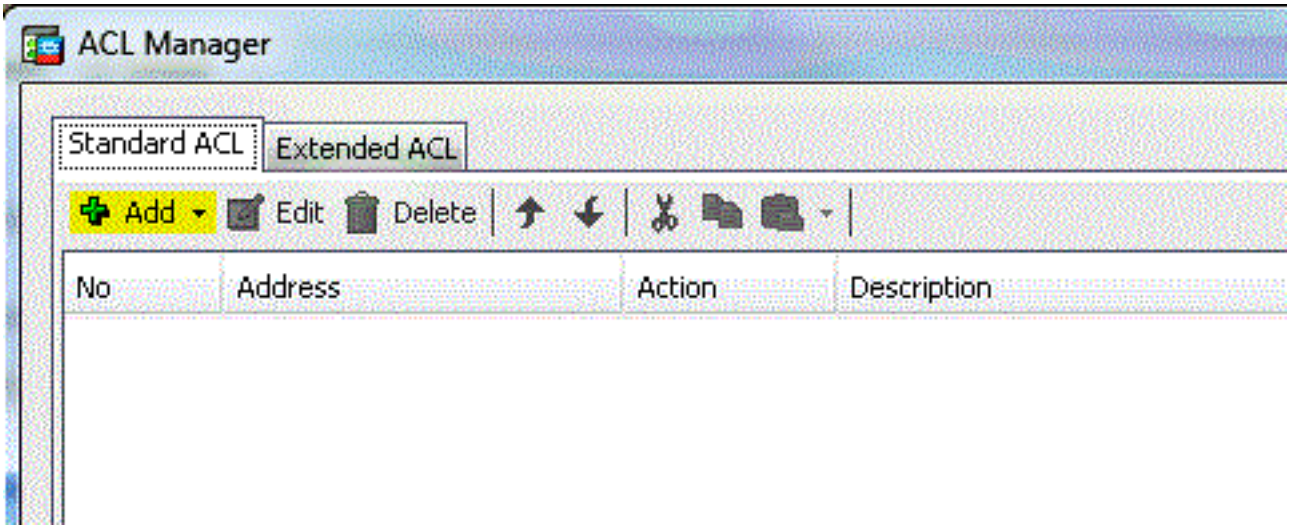
3. Décochez la case **Hériter** de la stratégie et sélectionnez **Exclure la liste réseau ci-dessous**.



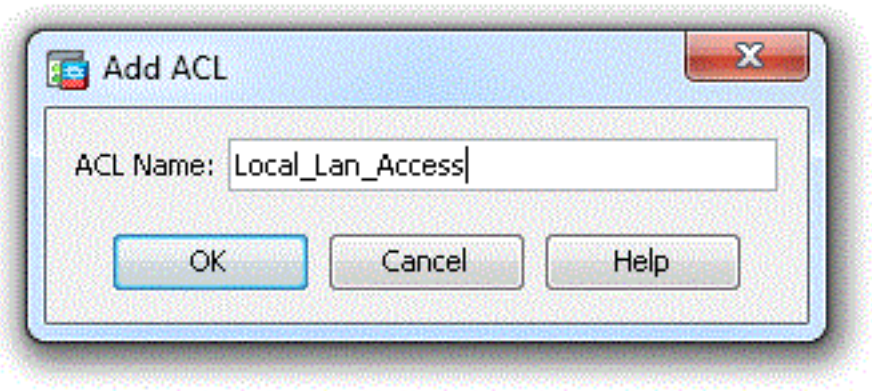
4. Décochez la case **Hériter** de la liste réseau, puis cliquez sur **Gérer** afin de lancer le gestionnaire de liste de contrôle d'accès (ACL).



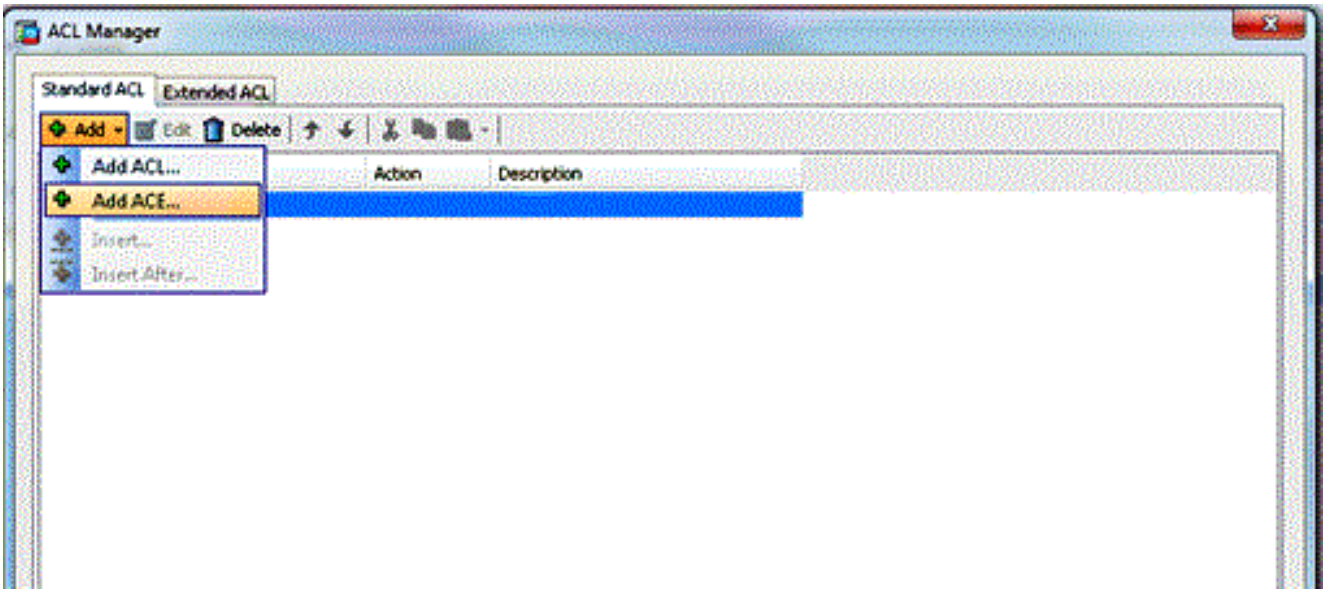
5. Dans le gestionnaire ACL, choisissez **Ajouter > Ajouter une ACL...** afin de créer une nouvelle liste d'accès.



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

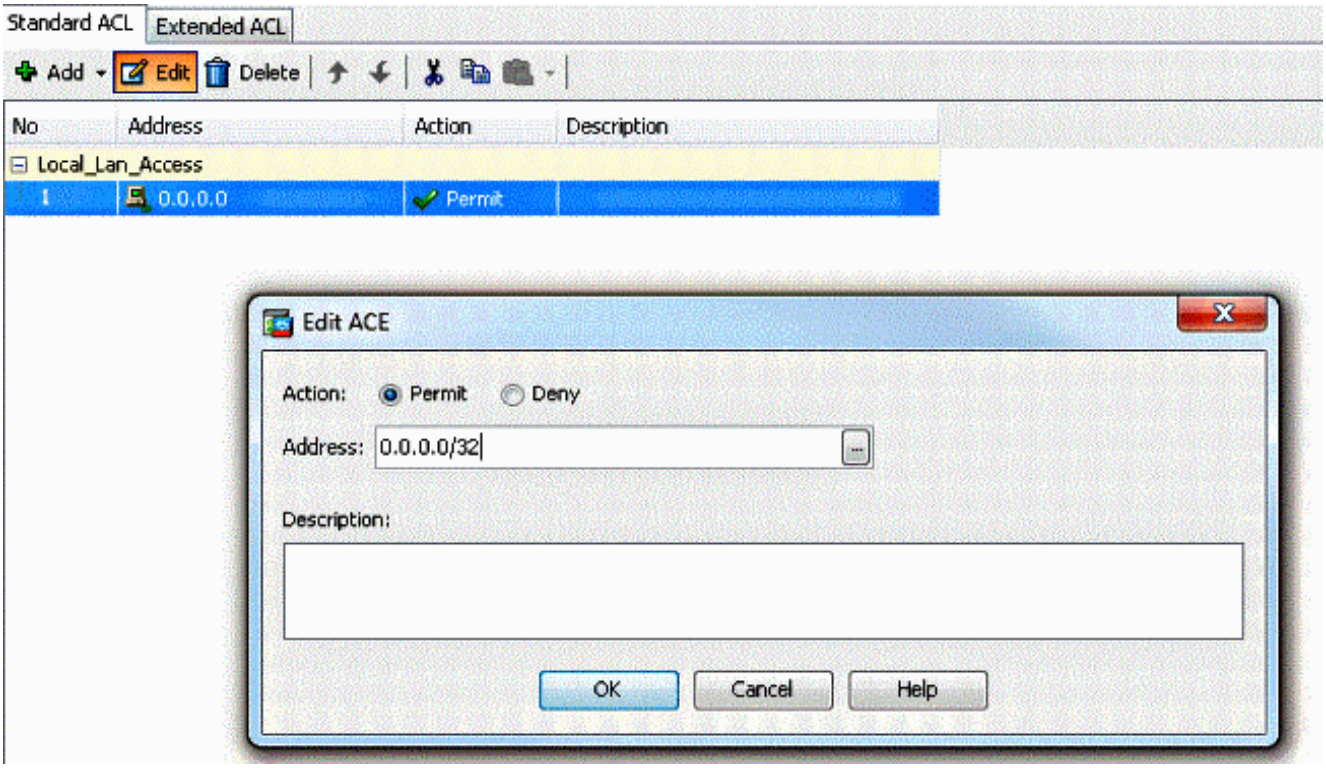


7. Une fois la liste de contrôle d'accès créée, choisissez **Ajouter > Ajouter ACE...** afin d'ajouter une entrée de contrôle d'accès (ACE).

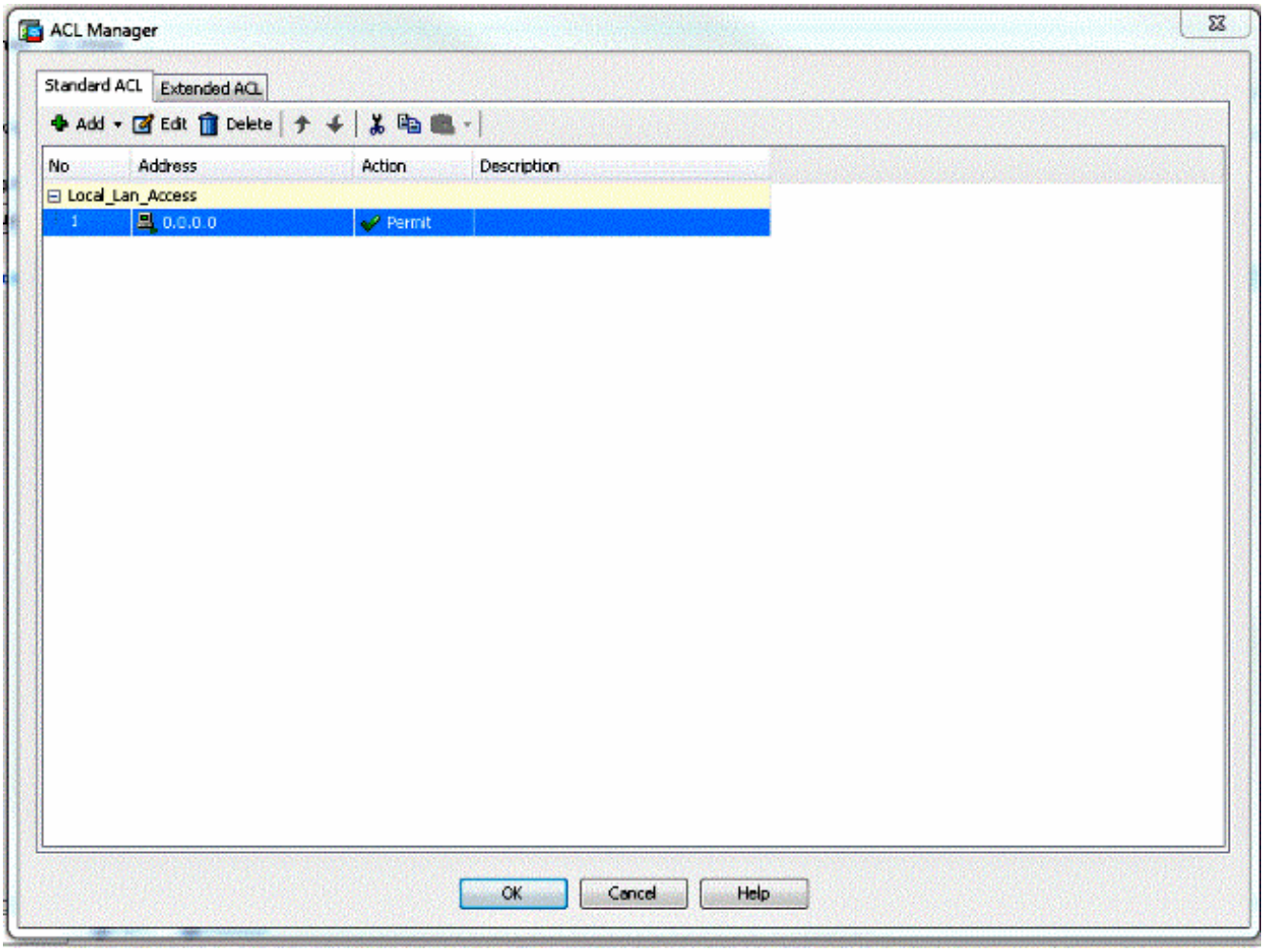


8. Définissez l'ACE qui correspond au réseau local LAN du client de routage.

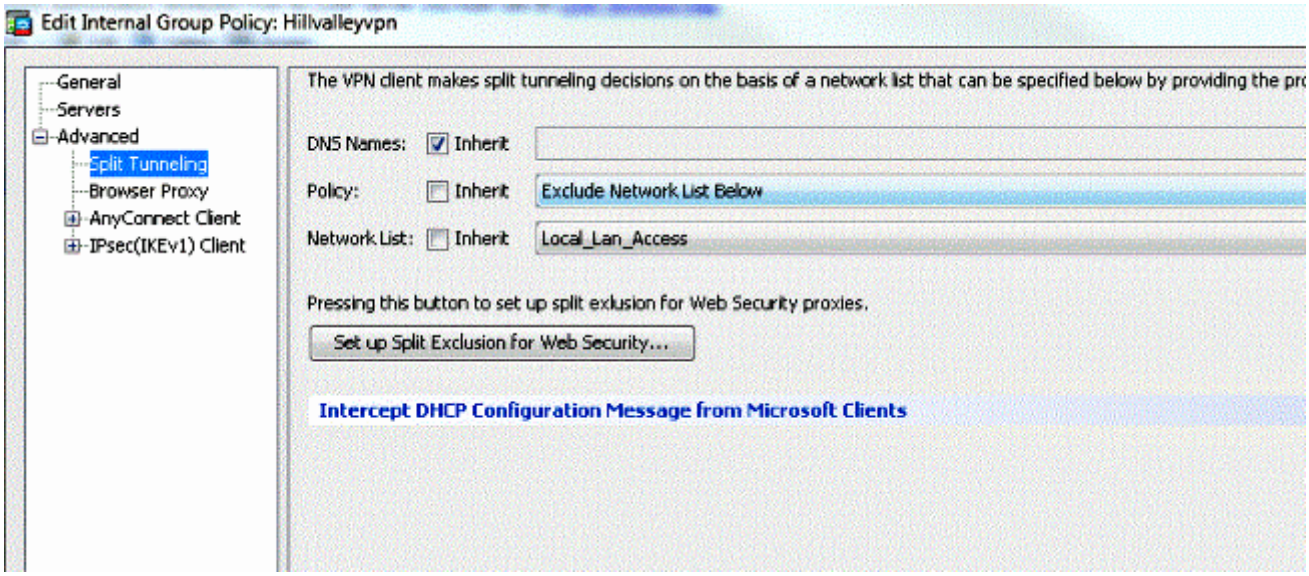
   Choisissez Permit.Choisissez une adresse IP 0.0.0.0Choisissez un masque de réseau de **/32**.(Facultatif) Fournissez une description.Click OK.



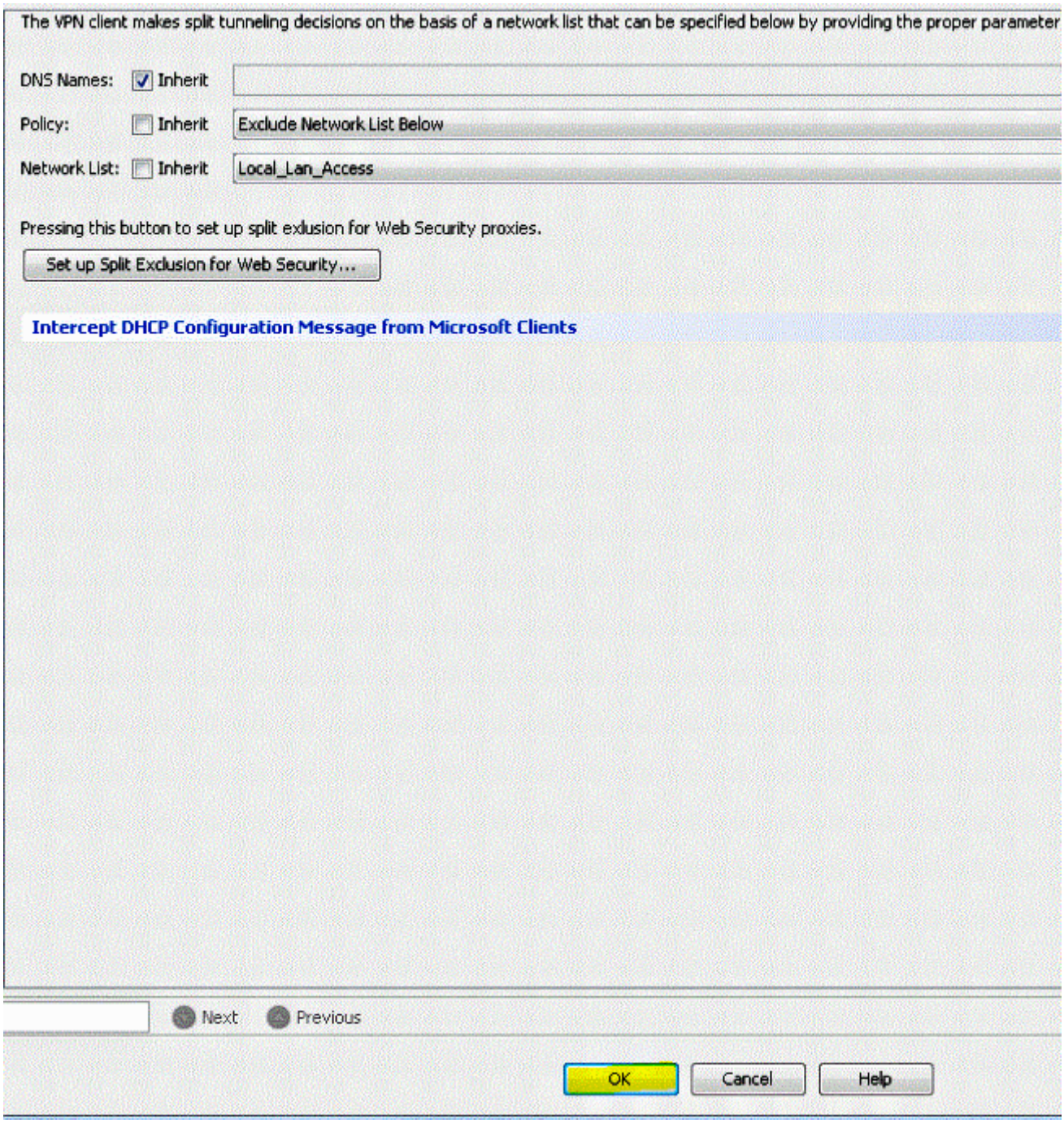
9. Cliquez sur OK afin de quitter l'ACL Manager.



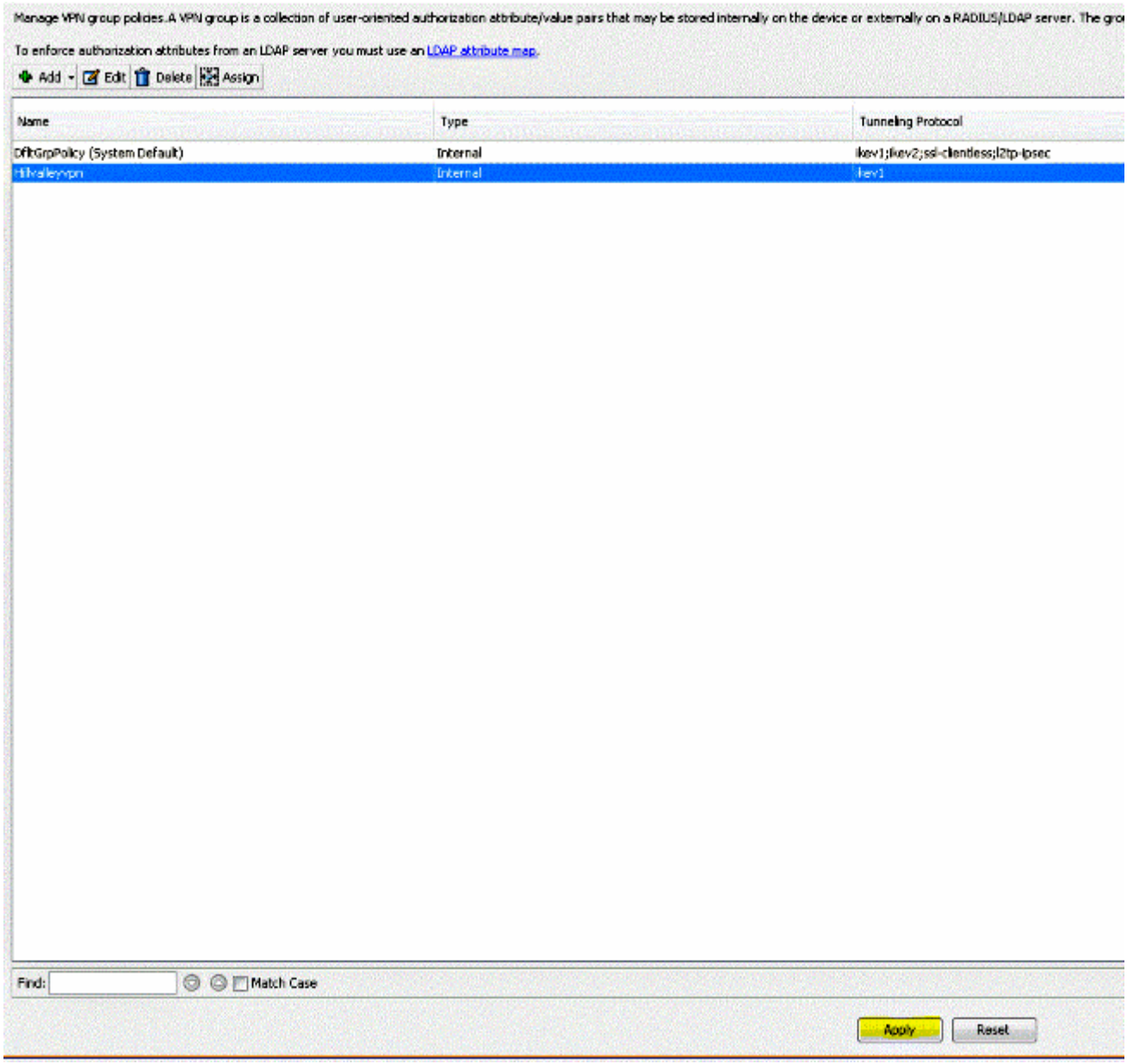
10. Assurez-vous que la liste de contrôle d'accès que vous venez de créer est sélectionnée pour la liste de réseaux à tunnels fractionnés.



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 l'ASA via l'interface de ligne de commande

Au lieu d'utiliser l'ASDM, vous pouvez exécuter ces étapes dans l'ASA CLI afin de permettre à des clients VPN d'avoir un accès au réseau local LAN tandis qu'ils sont connectés à l'ASA:

1. Passez en mode de configuration.

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#
```

2. Créez la liste d'accès afin d'autoriser l'accès au réseau local.

```
ciscoasa(config)#access-list Local_LAN_Access remark Client Local LAN Access
ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0
```

Attention : En raison de modifications apportées à la syntaxe des listes de contrôle d'accès entre les versions logicielles ASA 8.x et 9.x, cette liste de contrôle d'accès n'est plus

autorisée et les administrateurs verront ce message d'erreur lorsqu'ils essaieront de la configurer :

```
rtpvpnoutbound6(config)# access-list test standard permit host
0.0.0.0
ERREUR : adresse IP non valide
```

La seule chose autorisée est :

```
rtpvpnoutbound6(config)# access-list test standard permit any4
```

Il s'agit d'un problème connu qui a été résolu par l'ID de bogue Cisco CSCut3131. Passez à une version avec la correction de ce bogue afin de pouvoir configurer l'accès local au LAN.

3. Passez en mode de configuration Stratégie de groupe 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 politique est **exclue**.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

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

```
ciscoasa(config-group-policy)#split-tunnel-network-list value Local_LAN_Access
```

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 le client Cisco AnyConnect Secure Mobility

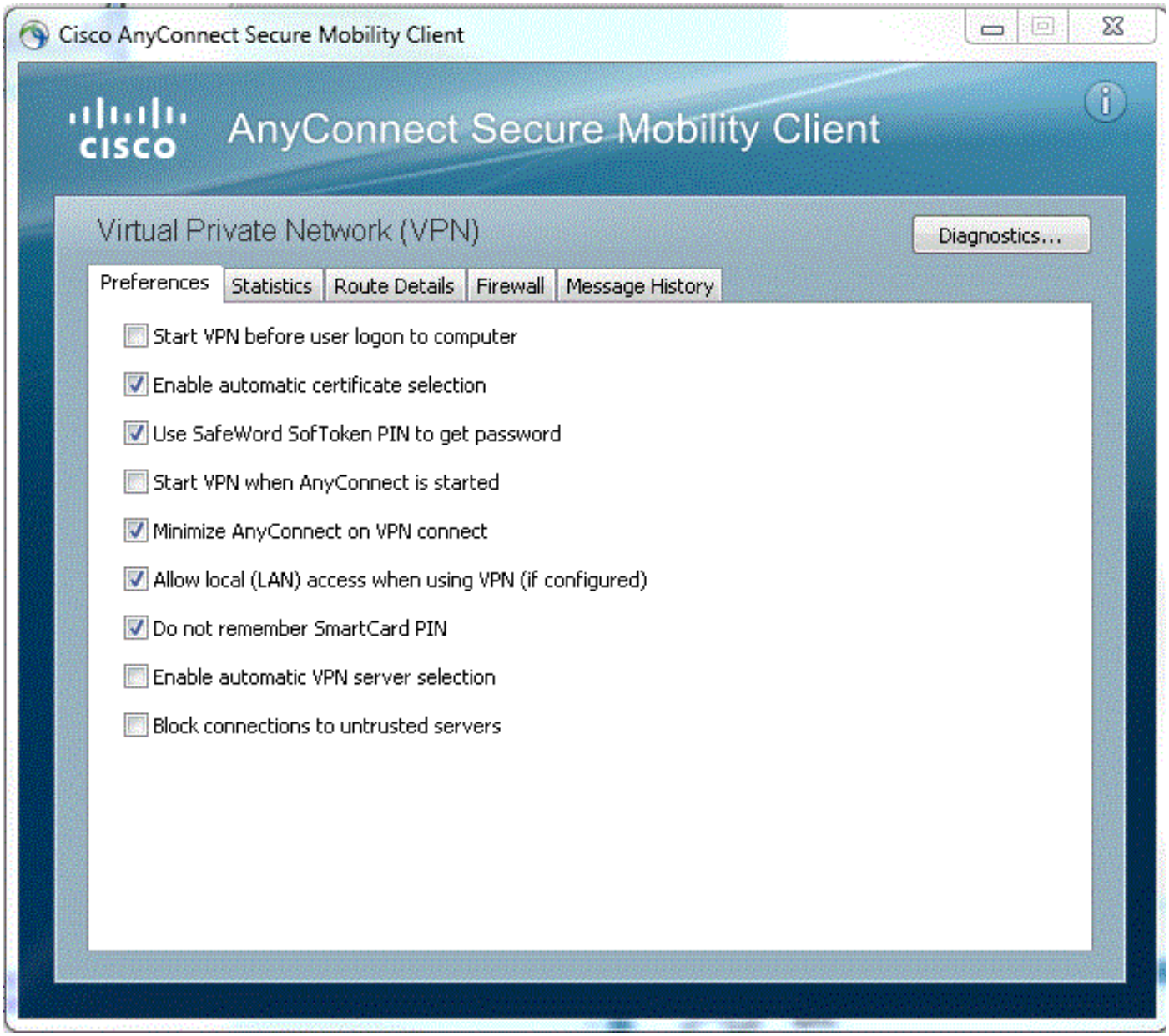
Afin de configurer le client Cisco AnyConnect Secure Mobility, référez-vous à la section Établir la connexion VPN SSL avec SVC de **ASA 8.x :** Exemple de configuration d'autorisation de la Transmission tunnel partagée pour un client VPN AnyConnect sur le dispositif ASA

Pour une Transmission tunnel non partagée, il faut que vous activiez AllowLocalLanAccess dans le client de routage d'AnyConnect. Toute Transmission tunnel non partagée est considérée comme un accès au réseau local LAN. Afin d'utiliser la fonctionnalité de l'exclusion de la transmission tunnel partagée, vous devez activer la préférence AllowLocalLanAccess dans les préférences de client VPN d'AnyConnect. Par défaut, l'accès de réseau local LAN est désactivé.

Afin d'autoriser l'accès LAN local, et donc la transmission tunnel à exclusion partagée, un administrateur réseau peut l'activer dans le profil ou les utilisateurs peuvent l'activer dans leurs paramètres de préférences (voir l'image dans la section suivante). Afin de permettre l'accès au réseau local LAN, un utilisateur sélectionne la case à cocher Allow Local LAN access si la transmission tunnel partagée est activée sur la passerelle sécurisée et si elle est configurée avec la stratégie indiquée de transmission tunnel partagée exclue. En outre, vous pouvez configurer le profil de client VPN si l'accès au réseau local LAN est autorisé avec **<LocalLanAccess UserControllable=« true »>true</LocalLanAccess>**.

Préférences utilisateur

Voici les sélections que vous devez effectuer dans l'onglet Préférences du client Cisco AnyConnect Secure Mobility afin d'autoriser l'accès LAN local.



Exemple de profil XML

Voici un exemple de configuration du profil de client VPN avec XML.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">true</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
```

```
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
</AnyConnectProfile>
```

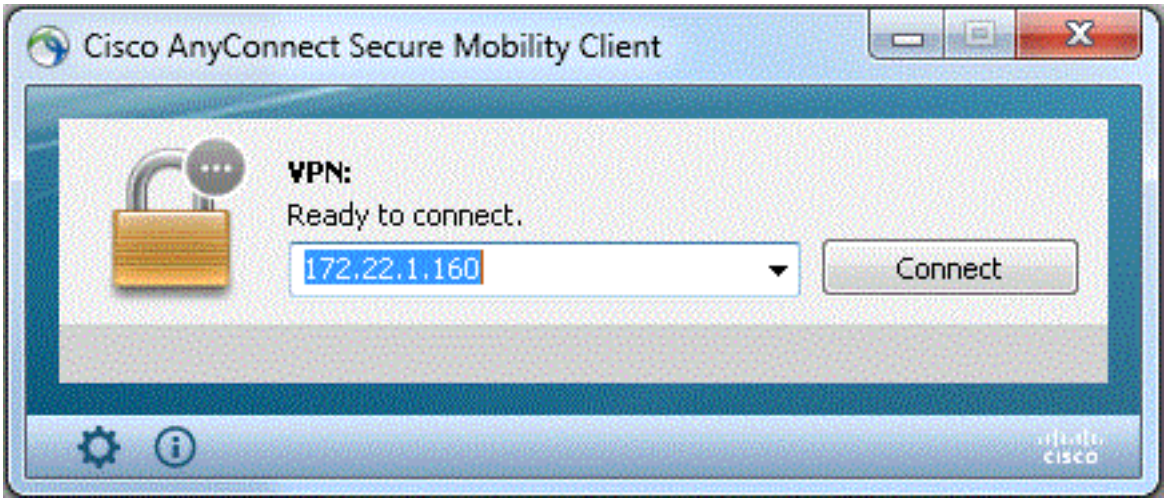
Vérification

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

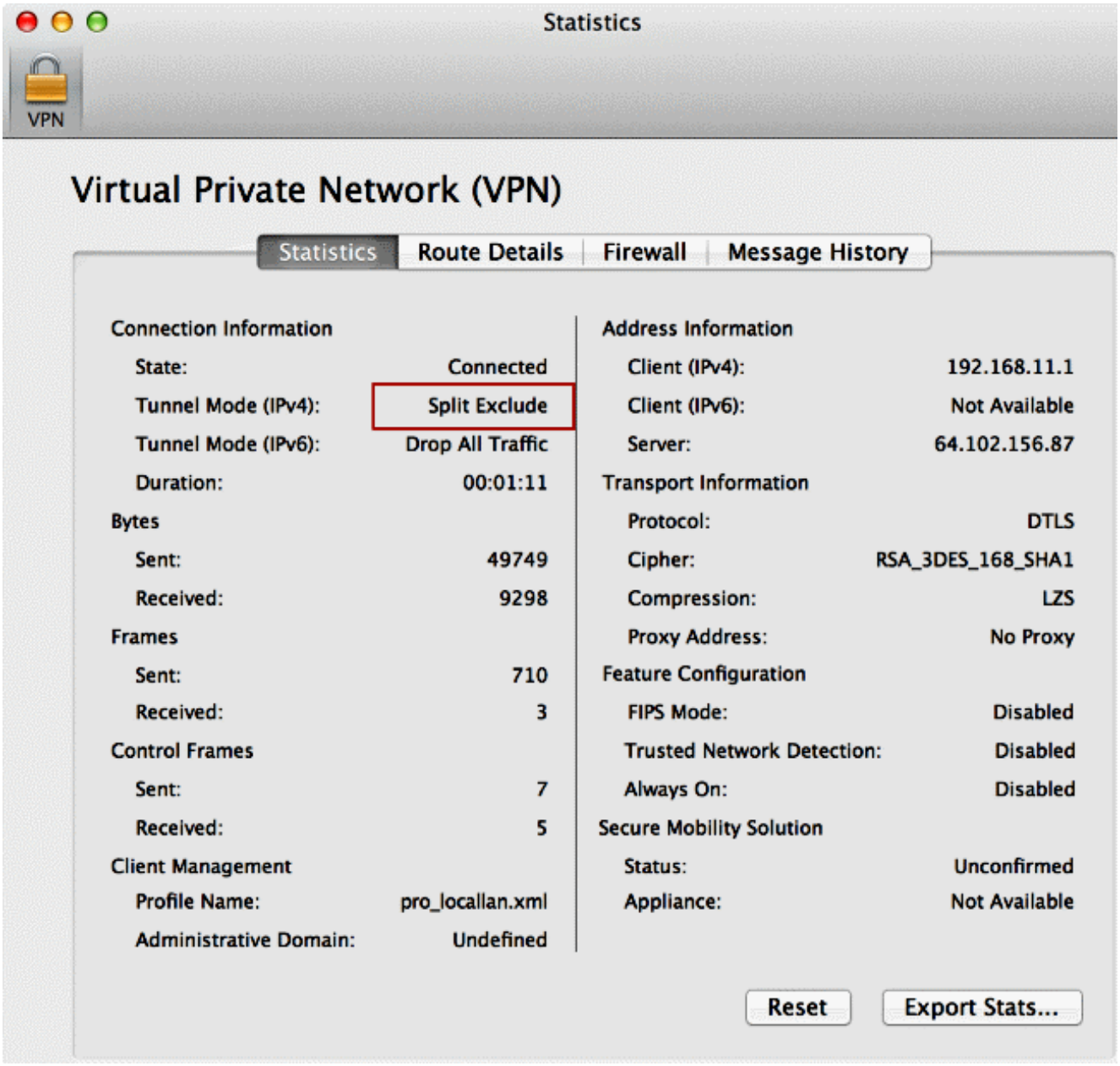
- Afficher le DART
- Tester l'accès local au LAN avec un ping

Connectez votre client Cisco AnyConnect Secure Mobility à l'ASA afin de vérifier votre configuration.

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

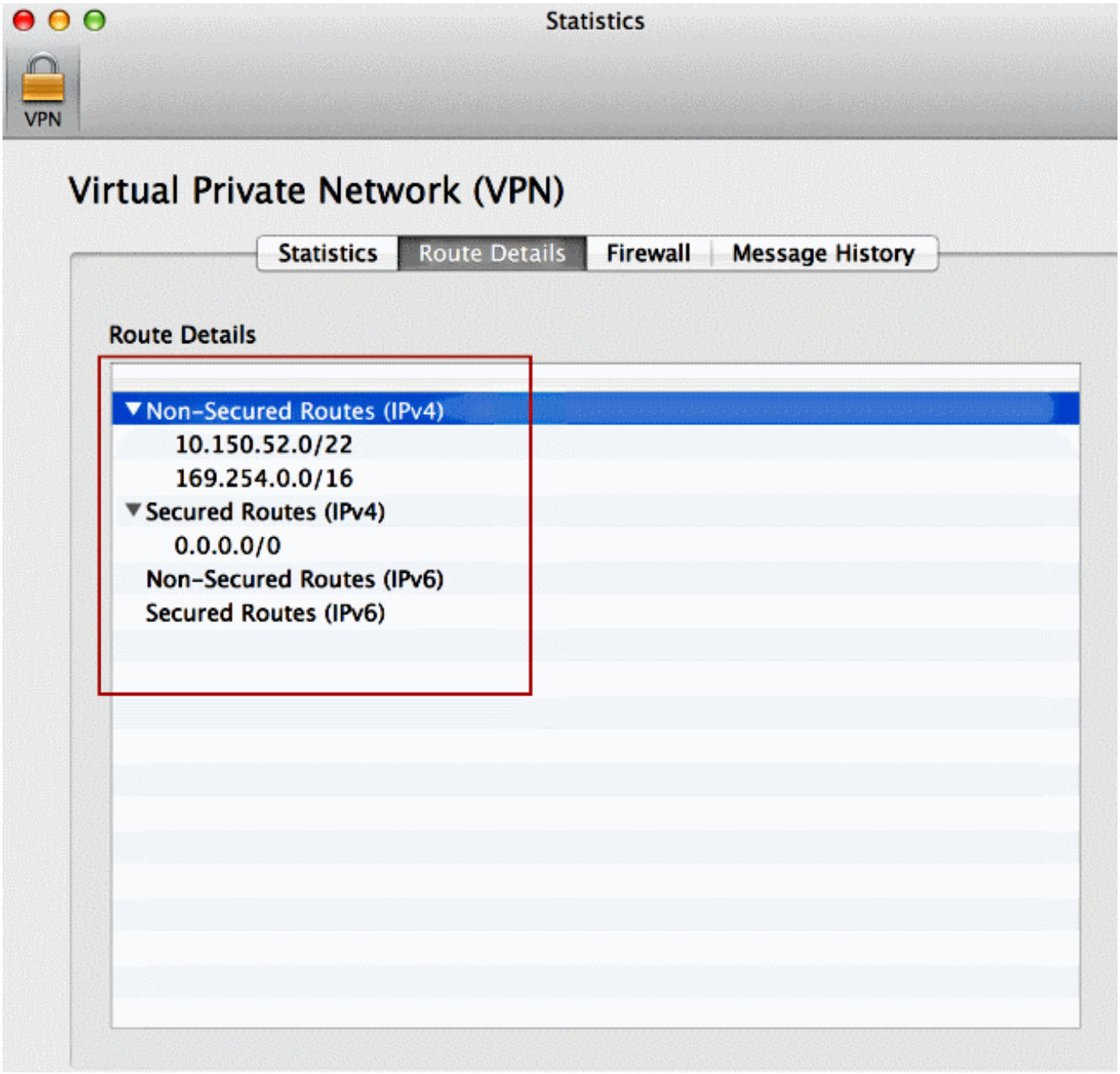


2. Sélectionnez **Fenêtre avancée pour tous les composants > Statistiques...** afin d'afficher le mode Tunnel.



3. Cliquez sur l'onglet **Route Details** afin de voir les routes vers lesquelles le client Cisco AnyConnect Secure Mobility dispose toujours d'un accès local.

   Dans cet exemple, le client est autorisé à accéder au LAN local à 10.150.52.0/22 et 169.254.0.0/16 tandis que tout autre trafic est chiffré et envoyé à travers le tunnel.



Client de mobilité sécurisée Cisco AnyConnect

Lorsque vous examinez les journaux AnyConnect de l'ensemble Diagnostics and Reporting Tool (DART), vous pouvez déterminer si le paramètre qui autorise l'accès LAN local est défini ou non.

```
****************************************

Date : 11/25/2011
Time : 13:01:48
Type : Information
Source : acvpndownloader

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: true
LocalLanAccess: true
```

```
AutoReconnect: true
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
AutoUpdate: true
RSASecurIDIntegration: Automatic
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Native
AllowLocalProxyConnections: true
PPPExclusion: Disable
PPPExclusionServerIP:
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true
```

```
**************************************
```

Tester l'accès local au LAN avec un ping

Une autre façon de vérifier que le client VPN dispose toujours d'un accès LAN local alors qu'il est connecté en tunnel à la tête de réseau VPN est d'utiliser la commande **ping** sur la ligne de commande Microsoft Windows. Voici un exemple où le réseau local du client est 192.168.0.0/24 et un autre hôte est présent sur le réseau avec l'adresse IP 192.168.0.3.

```
C:\>ping 192.168.0.3
Pinging 192.168.0.3 with 32 bytes of data&colon;

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

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

Incapable d'imprimer ou de naviguer par nom

Quand le client VPN est connecté et configuré pour l'accès de réseau local LAN, vous ne pouvez pas imprimer ni naviguer par nom sur le réseau local LAN. Il existe deux options possibles pour contourner cette situation:

- la navigation ou l'impression adresse IP.

  Afin de parcourir, au lieu de la syntaxe **\\sharename**, utilisez la syntaxe **\\x.x.x.x** où *x.x.x.x* est l'adresse IP de l'ordinateur hôte.

  Pour imprimer, modifiez les propriétés de l'imprimante réseau afin d'utiliser une adresse IP au lieu d'un nom. Par exemple, au lieu du la syntaxe \\sharename\printername, utilisez \\x.x.x.x\printername, où x.x.x.x est une adresse IP.
- Créez ou modifiez le fichier LMHOSTS de client VPN. Un fichier LMHOSTS sur un PC Microsoft Windows vous permet de créer des mappages statiques entre les noms d'hôte et les adresses IP. Par exemple, un fichier LMHOSTS pourrait ressembler à ceci:

  ```
  192.168.0.3 SERVER1
  192.168.0.4 SERVER2
  192.168.0.5 SERVER3
  ```

  Dans Microsoft Windows XP Professionnel, le fichier LMHOSTS se trouve dans **%SystemRoot%\System32\Drivers\Etc**. Reportez-vous à votre documentation Microsoft ou à l'article 314108 de la base de connaissances Microsoft pour plus d'informations.

Informations connexes

- Exemple de configuration de PIX/ASA 7.x comme serveur de VPN distant avec l'ASDM
- Exemple de configuration d'un client VPN SSL (SVC) sur IOS avec SDM
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems