Exemple de configuration de transmission tunnel partagée pour clients VPN sur le concentrateur VPN 3000

Contenu

Introduction

Ce document fournit des instructions pas à pas sur la façon d'autoriser les clients VPN à accéder à Internet pendant qu'ils sont connectés par tunnel à un concentrateur de la gamme VPN 3000. 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 partagée peut présenter un risque de sécurité lorsqu'elle est configurée. Puisque les clients VPN ont un accès à Internet non sécurisé, ils peuvent être compromis par un attaquant. Cet attaquant pourrait alors accéder au réseau local de l'entreprise par l'intermédiaire du tunnel IPsec. Une compromission entre une transmission tunnel totale et une transmission tunnel partagée peut être de ne permettre aux clients VPN que l'accès au LAN. Référez-vous à Exemple de configuration de l'accès LAN local pour les clients VPN sur le concentrateur VPN 3000 pour plus d'informations.

Conditions préalables

Conditions requises

Ce document suppose qu'une configuration VPN d'accès à distance fonctionnelle existe déjà sur le concentrateur VPN. Reportez-vous à Exemple de configuration d'IPsec avec un client VPN vers

un concentrateur VPN 3000 si un n'est pas déjà configuré.

Components Used

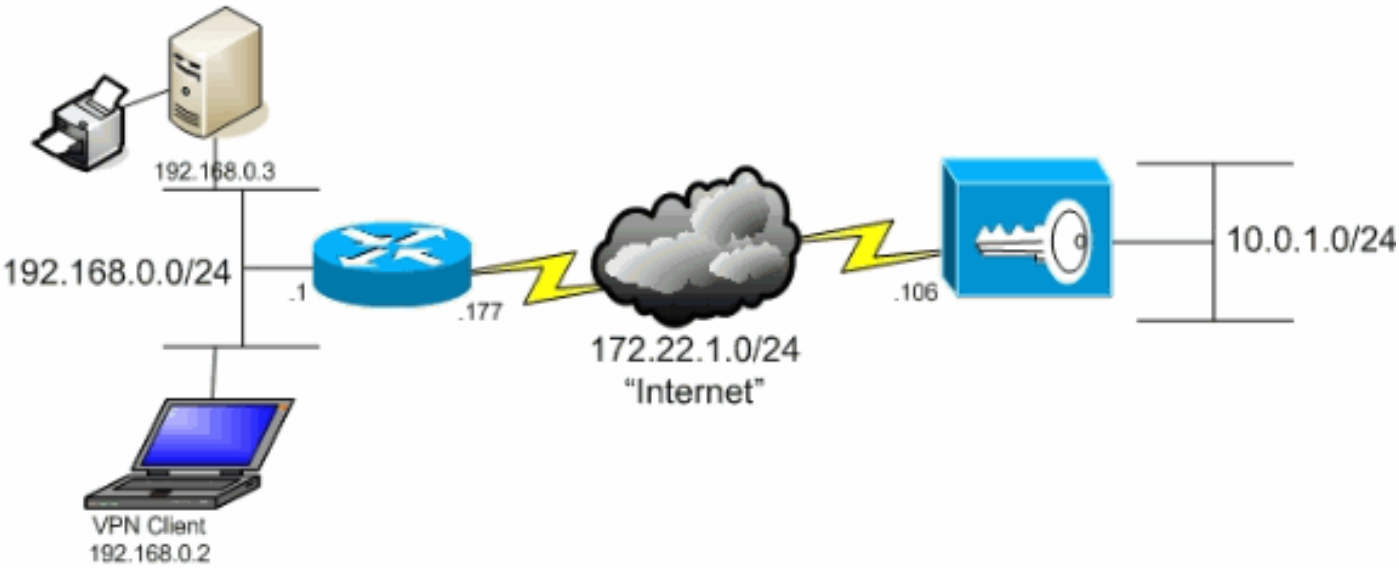
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel de la gamme Cisco VPN 3000 Concentrator version 4.7.2.H
- Client VPN Cisco Version 4.0.5

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. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

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



Conventions

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

Informations générales

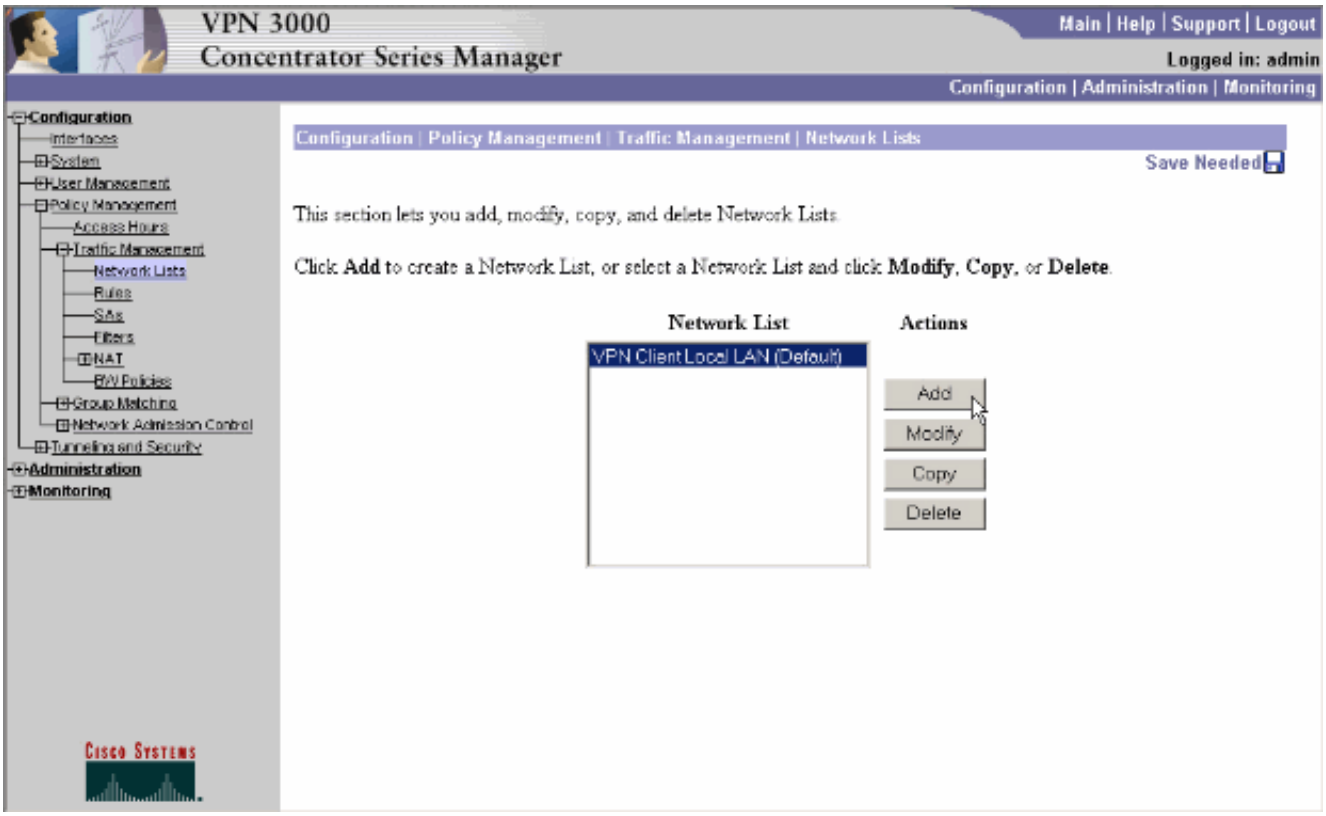
Dans un scénario de client VPN de base vers concentrateur VPN, tout le trafic du client VPN est chiffré et envoyé au concentrateur VPN, quelle que soit la destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande passante. La transmission tunnel partagée peut résoudre ce problème en permettant aux utilisateurs d'envoyer uniquement le trafic destiné au réseau d'entreprise via le tunnel. Tout autre trafic, tel que la messagerie instantanée, la messagerie électronique ou la navigation occasionnelle, est envoyé sur Internet via le réseau local du client VPN.

Configurer la transmission tunnel partagée sur le concentrateur

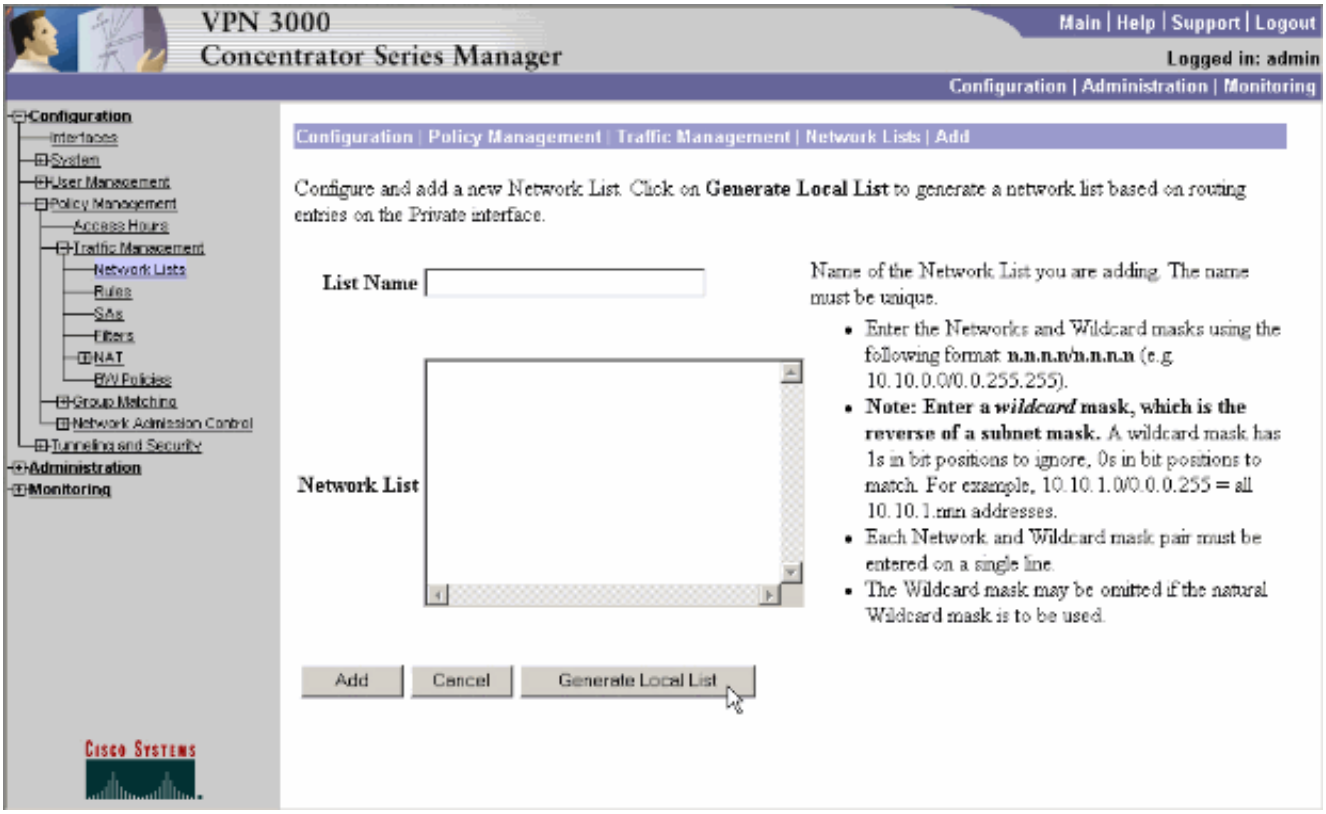
VPN

Complétez ces étapes afin de configurer votre groupe de tunnels pour autoriser la transmission tunnel partagée pour les utilisateurs du groupe. Créez d'abord une liste de réseaux. Cette liste définit les réseaux de destination vers lesquels le client VPN envoie du trafic chiffré. Une fois la liste créée, ajoutez-la à la stratégie de fractionnement en canaux du groupe de tunnels client.

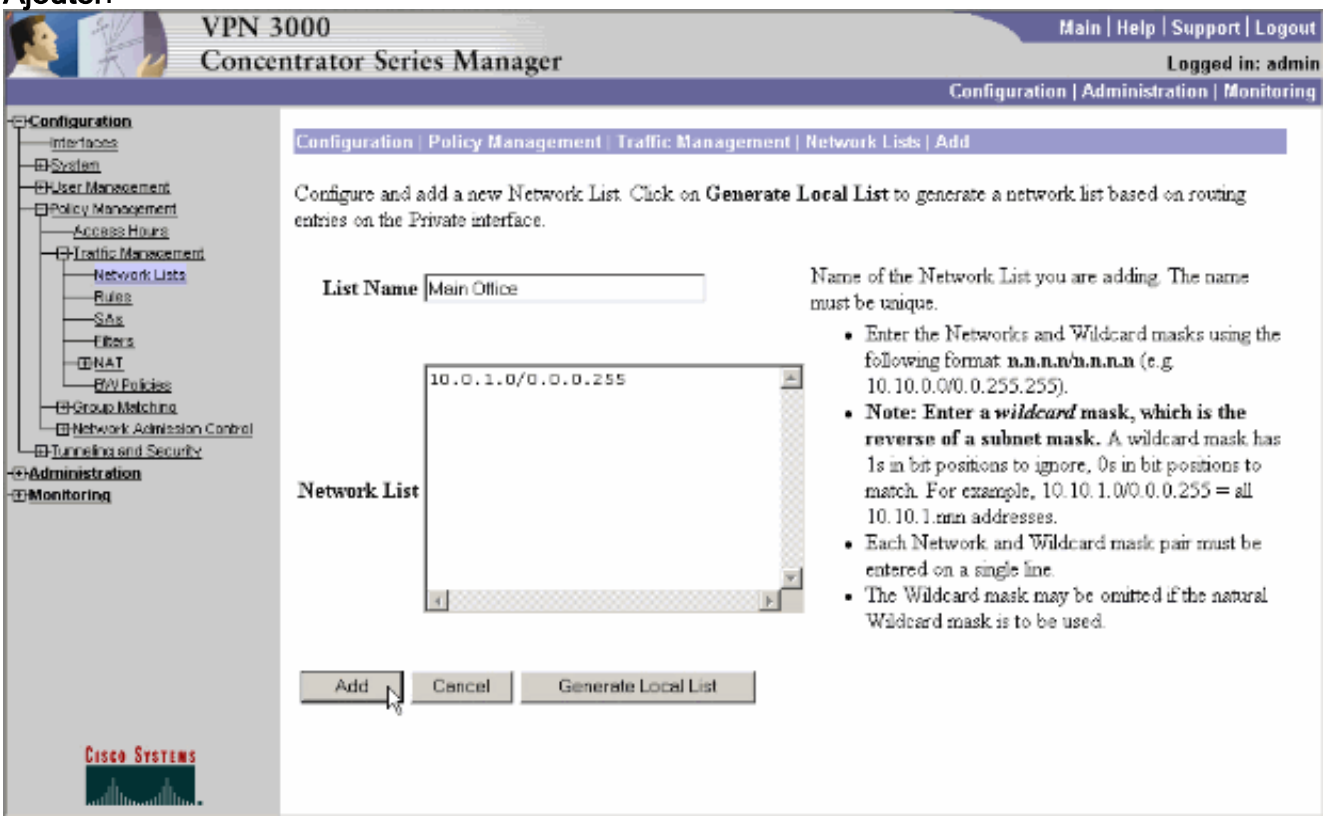
1. Choisissez **Configuration > Policy Management > Traffic Management > Network Lists** et cliquez sur
Add.



2. Cette liste définit les réseaux de destination vers lesquels le client VPN envoie du trafic chiffré. Entrez ces réseaux manuellement ou cliquez sur **Generate Local List** afin de créer une liste basée sur les entrées de routage sur l'interface privée du concentrateur VPN.Dans cet exemple, la liste a été créée
automatiquement.

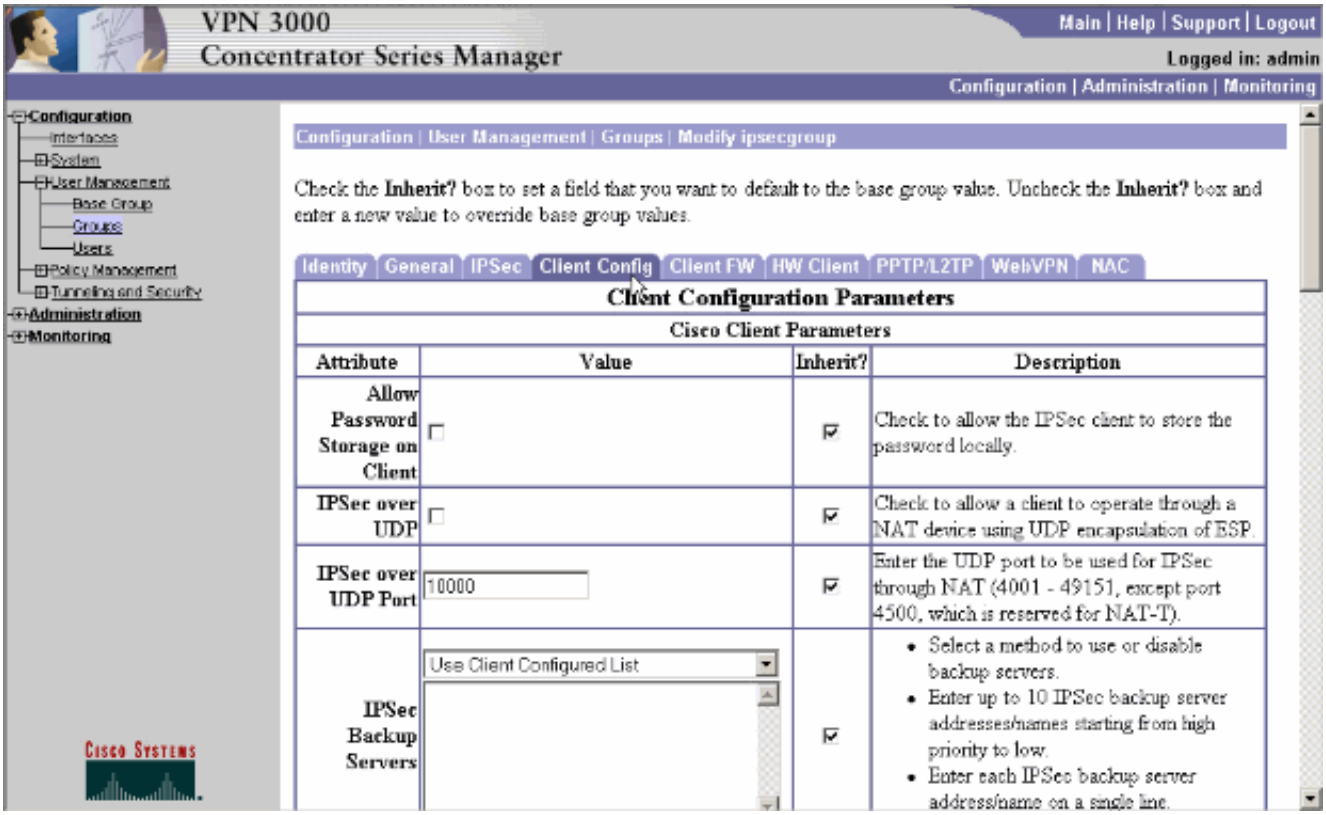


3. Une fois créé ou rempli, indiquez un nom pour la liste et cliquez sur **Ajouter**.

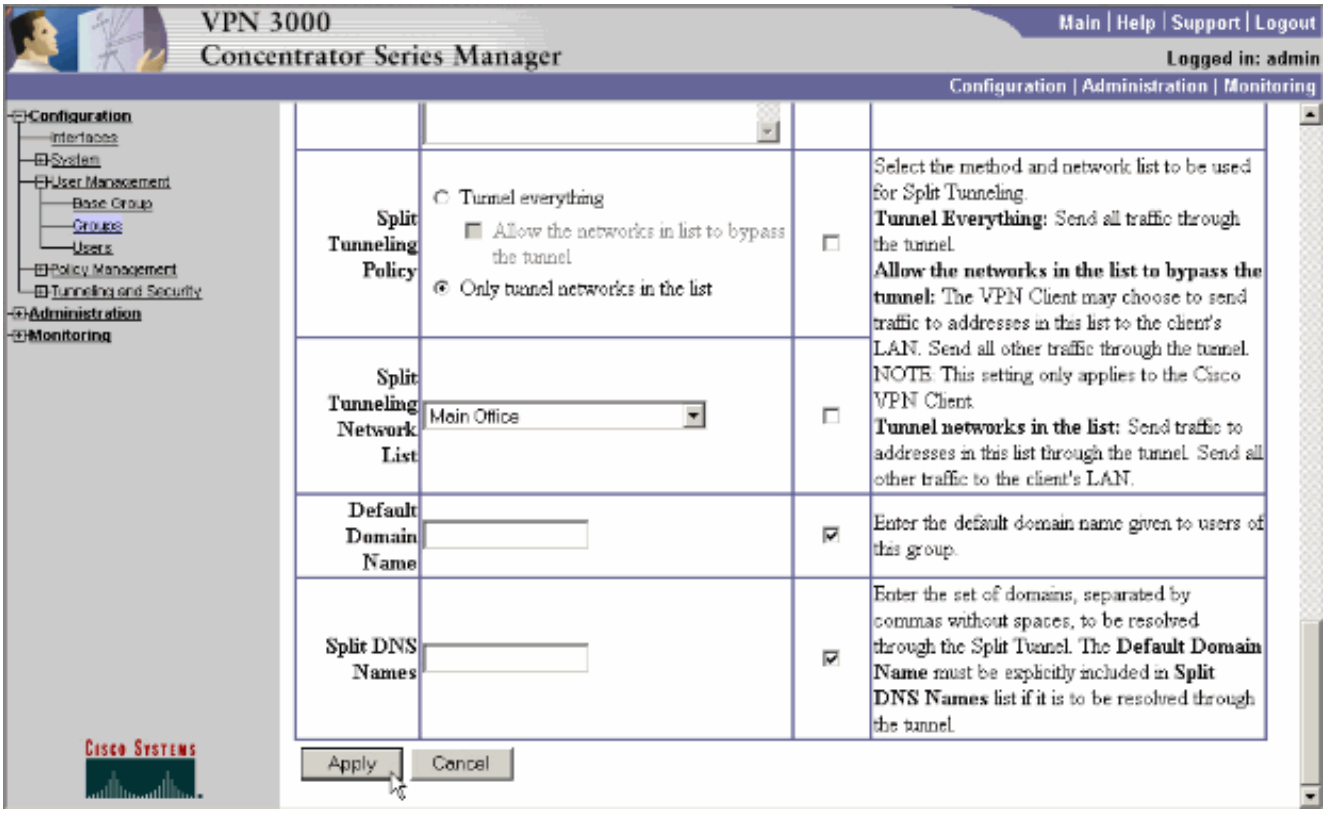


4. Une fois que vous avez créé la liste réseau, affectez-la à un groupe de tunnels. Choisissez **Configuration > User Management > Groups**, sélectionnez le groupe que vous souhaitez modifier, puis cliquez sur **Modify Group**.

5. Accédez à l'onglet Configuration du client du groupe que vous avez choisi de modifier.



6. Faites défiler jusqu'aux sections Politique de fractionnement en canaux et Liste de réseaux de fractionnement en canaux, puis cliquez sur **Réseaux de tunnels uniquement dans la liste**.
7. Sélectionnez la liste créée précédemment dans la liste déroulante. Dans ce cas, il s'agit du **bureau principal**. L'héritage ? sont automatiquement vidées dans les deux cas.



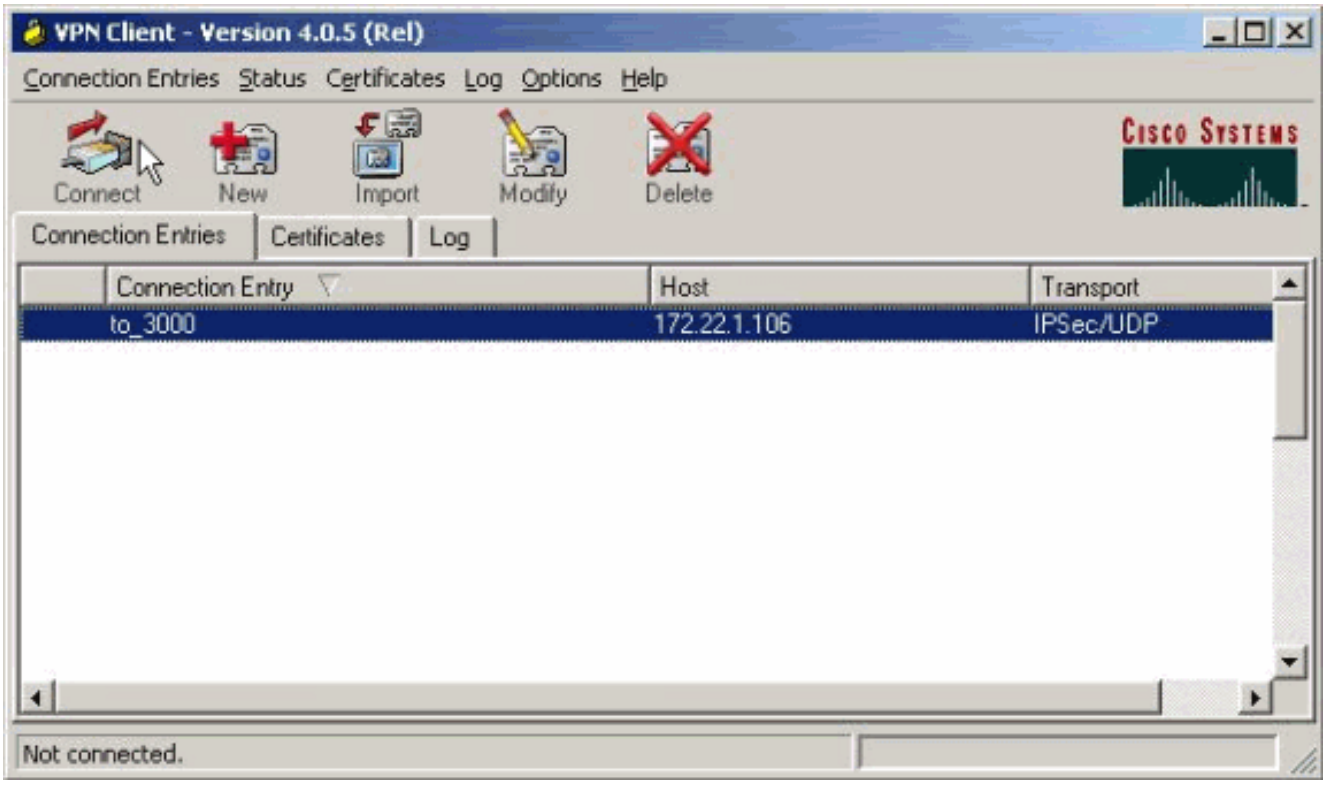
8. Cliquez sur **Apply** lorsque vous avez terminé.

Vérification

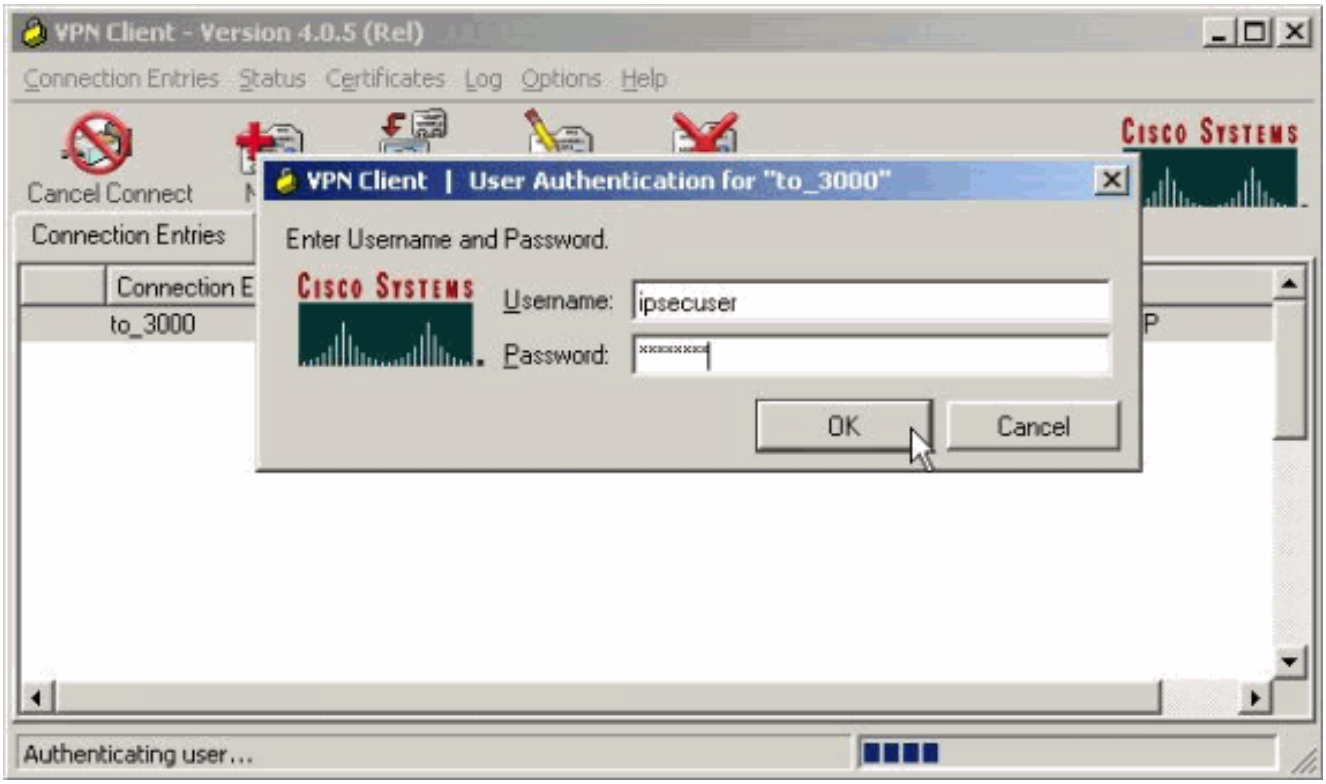
Se connecter avec le client VPN

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

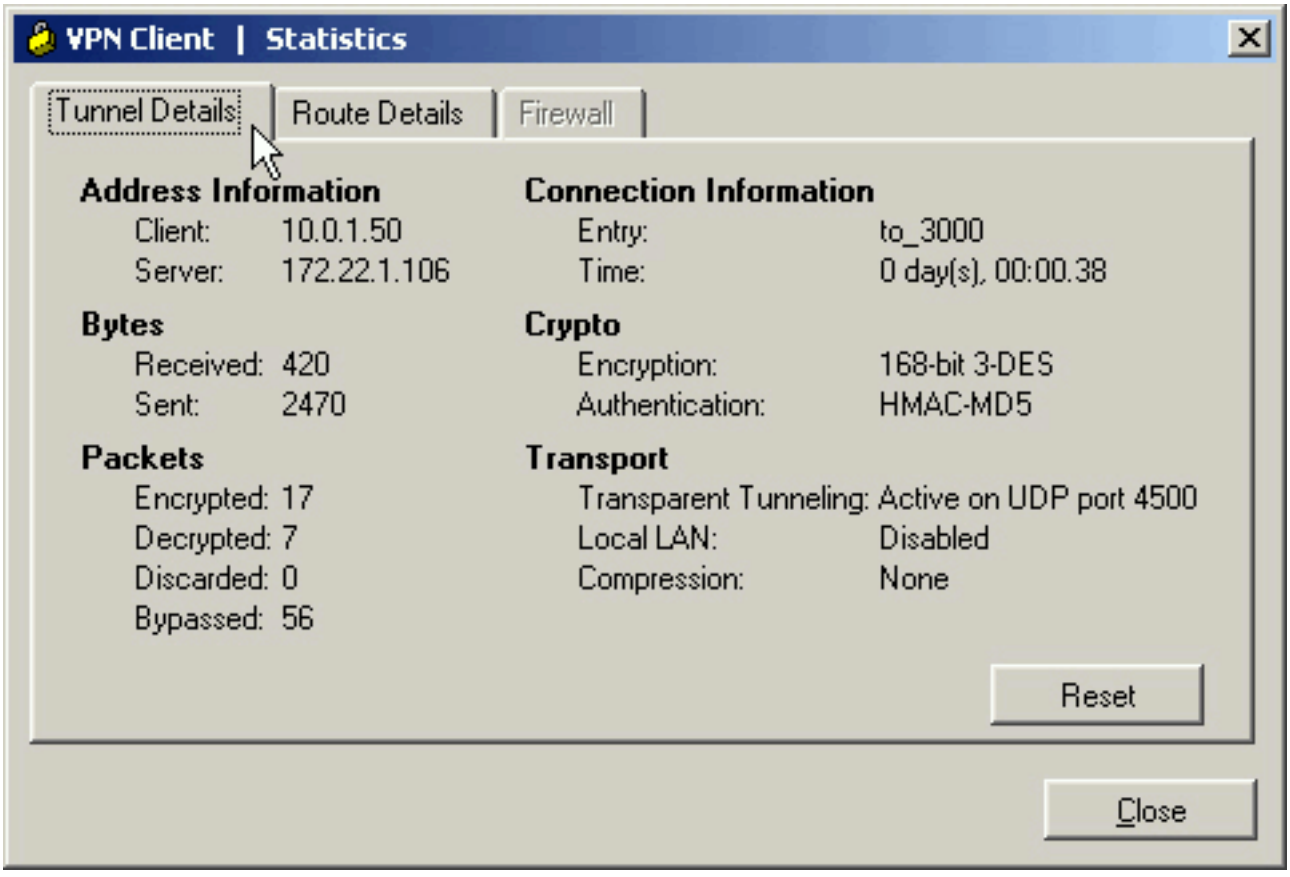
1. Choisissez votre entrée de connexion dans la liste et cliquez sur **Connect**.



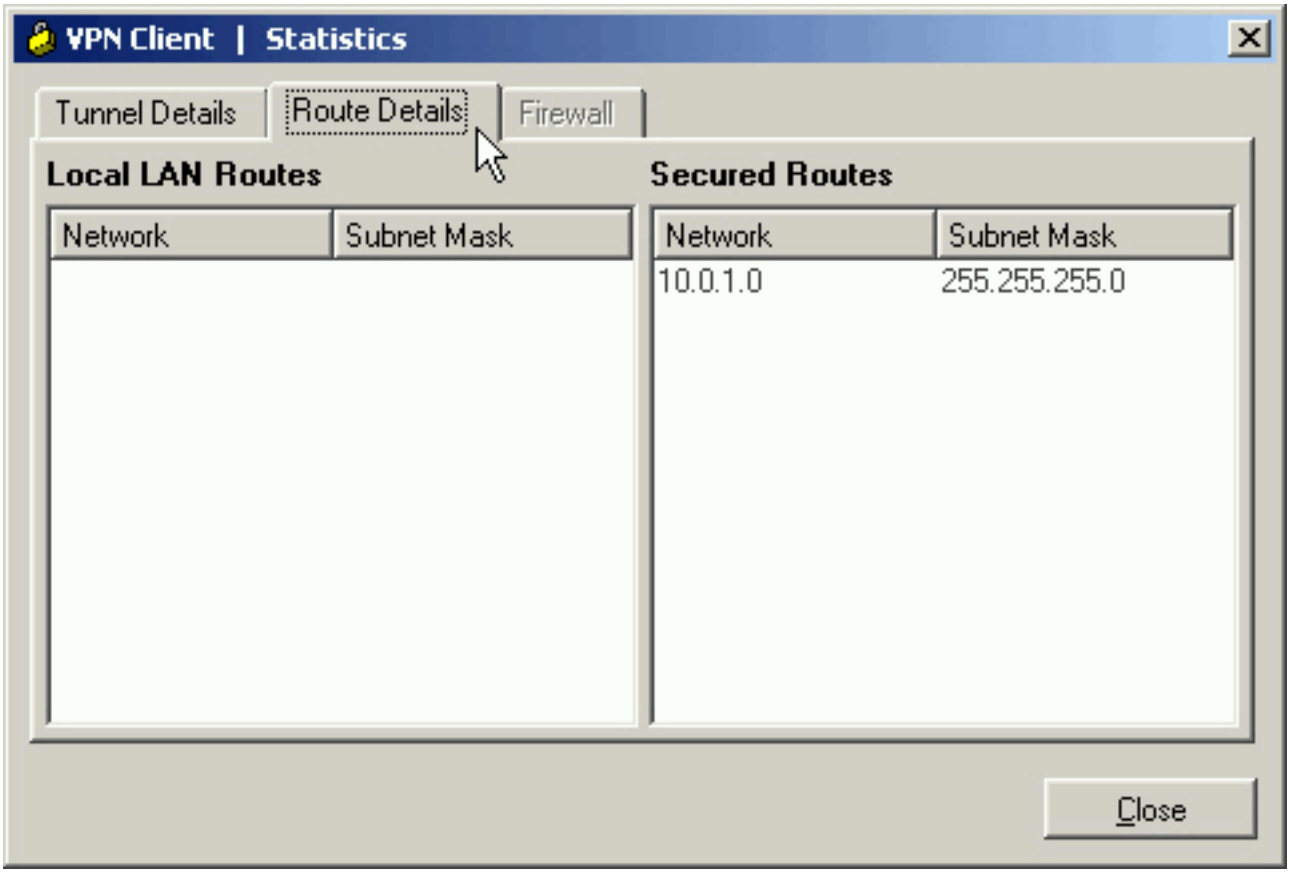
2. Entrez dans vos informations d'identification.



3. Choisissez **Status > Statistics...** afin d'afficher la fenêtre Tunnel Details (Détails du tunnel) dans laquelle vous pouvez inspecter les détails du tunnel et voir le flux du trafic.

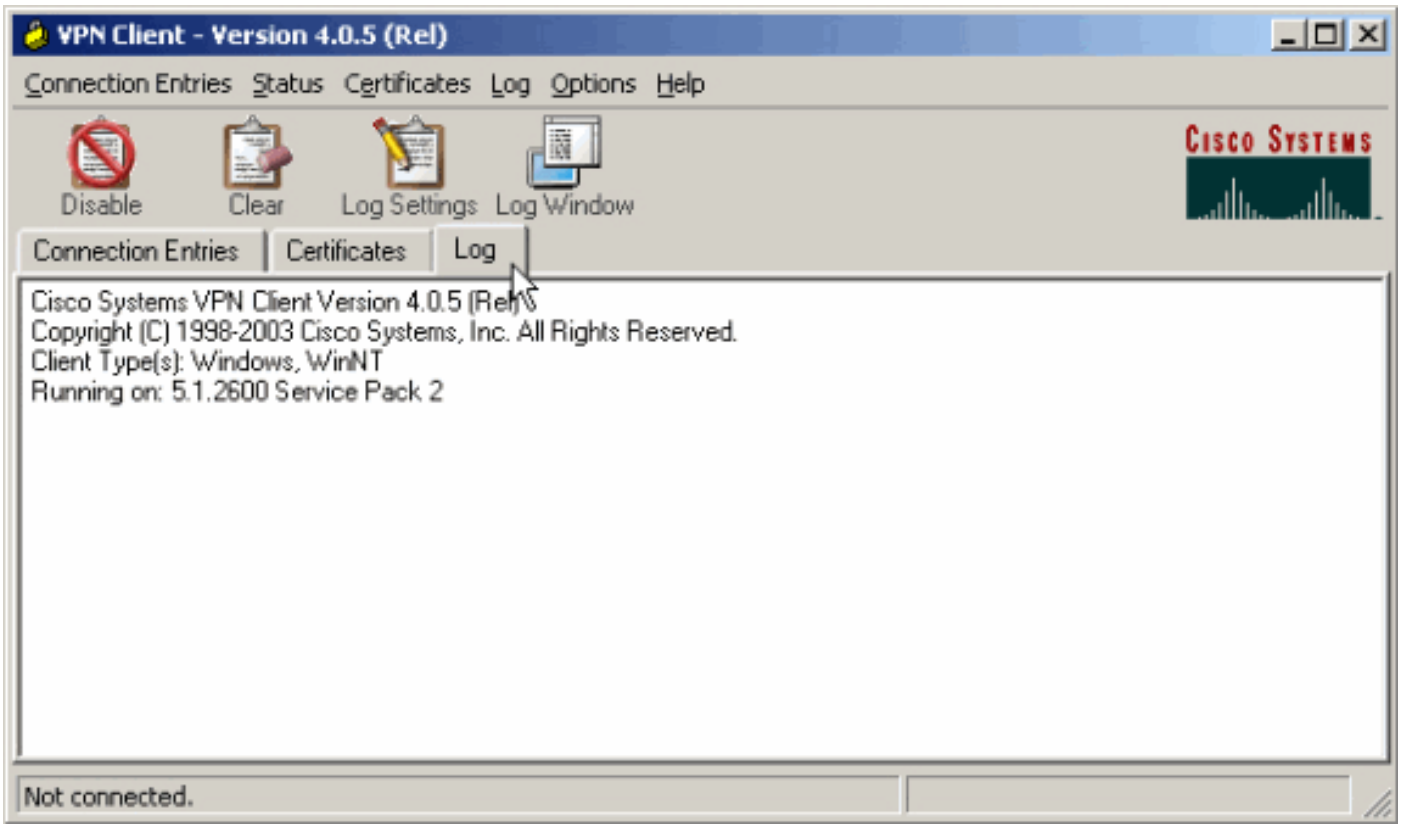


4. Accédez à l'onglet Route Details afin de voir à quels réseaux le client VPN envoie du trafic chiffré. Dans cet exemple, le client VPN communique en toute sécurité avec 10.0.1.0/24 alors que tout autre trafic est envoyé non chiffré à Internet.



Afficher le journal du client VPN

Lorsque vous examinez le journal du client VPN, vous pouvez déterminer si le paramètre qui autorise la transmission tunnel partagée est défini. Accédez à l'onglet Log du client VPN afin d'afficher le journal. Cliquez sur **Paramètres du journal** afin d'ajuster ce qui est consigné. Dans cet exemple, IKE et IPsec sont définis sur **3- Élevé** tandis que tous les autres éléments de journal sont définis sur **1 - Faible**.



```
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      14:21:43.106  07/21/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 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 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.
```

Dépannage

Référez-vous à Exemple de configuration d'IPsec avec client VPN vers concentrateur VPN 3000 - Dépannage pour des informations générales sur le dépannage de cette configuration.

Informations connexes

- Exemple de configuration d'IPsec avec client VPN vers concentrateur VPN 3000
- Concentrateurs VPN de la gamme Cisco 3000
- Client VPN Cisco
- Support et documentation techniques - Cisco Systems