

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

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

[Informations générales](#)

[Configurer la transmission tunnel partagée sur le concentrateur VPN](#)

[Vérification](#)

[Se connecter avec le client VPN](#)

[Afficher le journal du client VPN](#)

[Dépannage](#)

[Informations connexes](#)

## 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

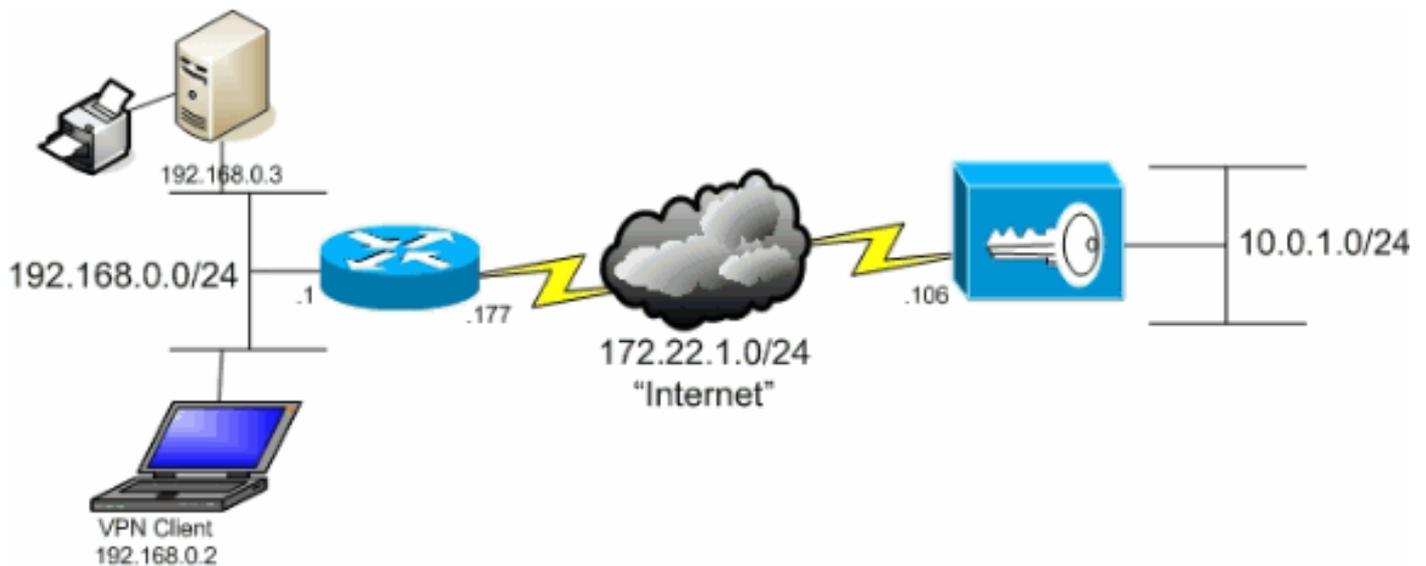
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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

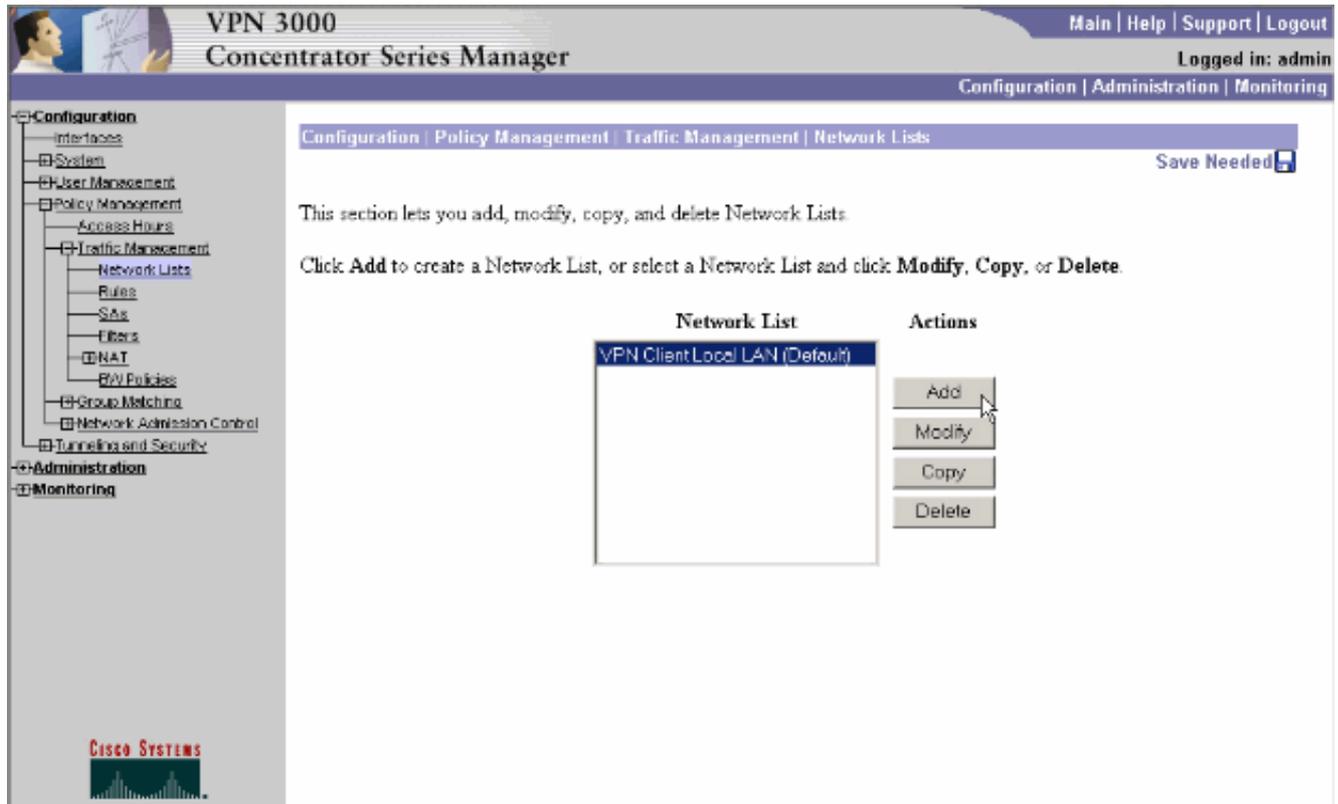
Dans un scénario de client VPN de base vers concentrateur VPN, tout le trafic du client VPN est chiffré et envoyé au concentrateur VPN, quelle que soit la destination. En fonction de votre configuration et du nombre d'utilisateurs pris en charge, une telle configuration peut devenir gourmande en bande 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.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Network List

Add Cancel Generate Local List

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format **n.n.n.n/w.w.w.w** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.mmm addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

CISCO SYSTEMS

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

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name

Network List

Add Cancel Generate Local List

Name of the Network List you are adding. The name must be unique.

- Enter the Networks and Wildcard masks using the following format **n.n.n.n/w.w.w.w** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a wildcard mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.255 = all 10.10.1.mmm addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

CISCO SYSTEMS

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**.

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups

Save Needed

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

Actions

Current Groups

Modify

ipsecgroup (Inmemory Configured)

Authentication Servers

Authorization Servers

Accounting Servers

Address Pools

Client Update

Bandwidth Assignment

WebVPN Servers and URLs

WebVPN Port Forwarding

Add Group

Modify Group

Delete Group

CISCO SYSTEMS

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

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | User Management | Groups | Modify ipsecgroup

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP | WebVPN | NAC

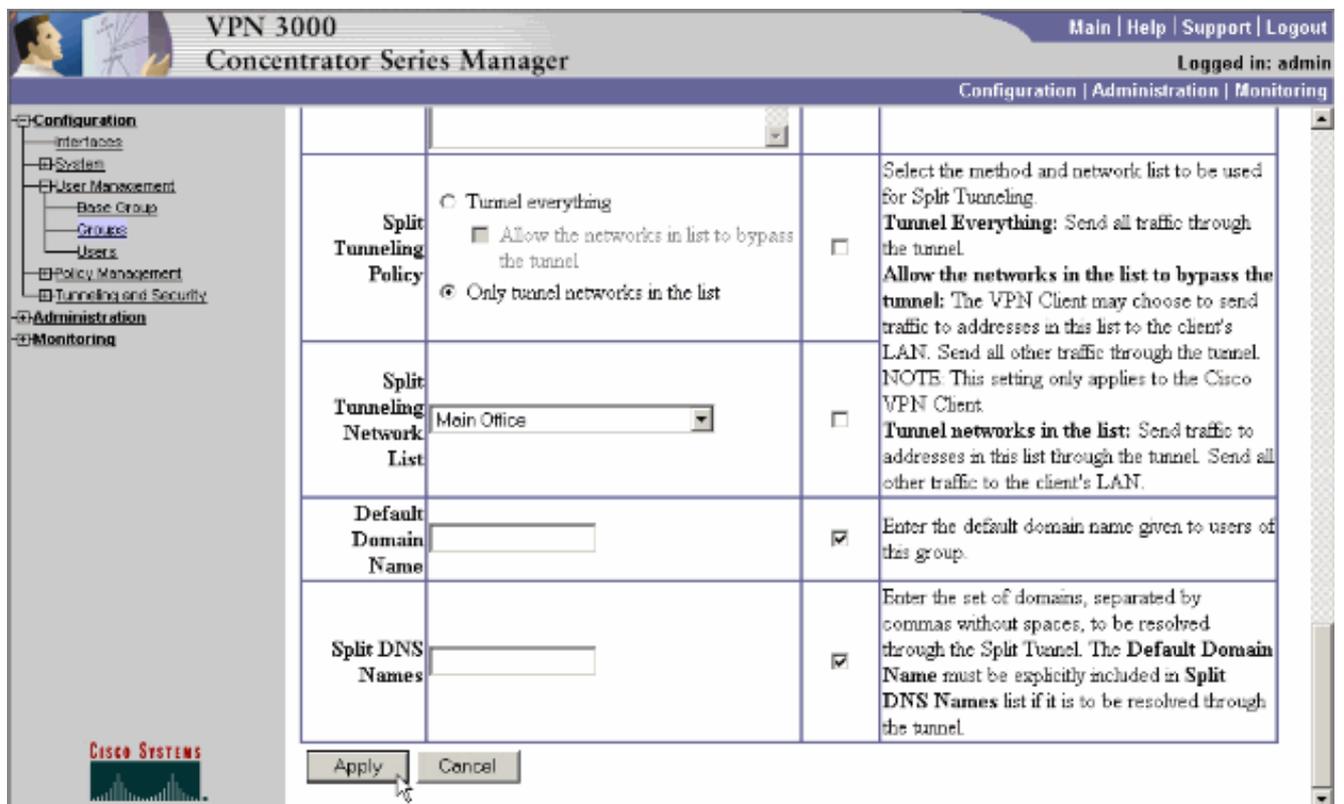
**Client Configuration Parameters**

Cisco Client Parameters

Attribute	Value	Inherit?	Description
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPSec client to store the password locally.
IPSec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPSec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> <li>Select a method to use or disable backup servers.</li> <li>Enter up to 10 IPSec backup server addresses/names starting from high priority to low.</li> <li>Enter each IPSec backup server address/name on a single line.</li> </ul>

CISCO SYSTEMS

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.



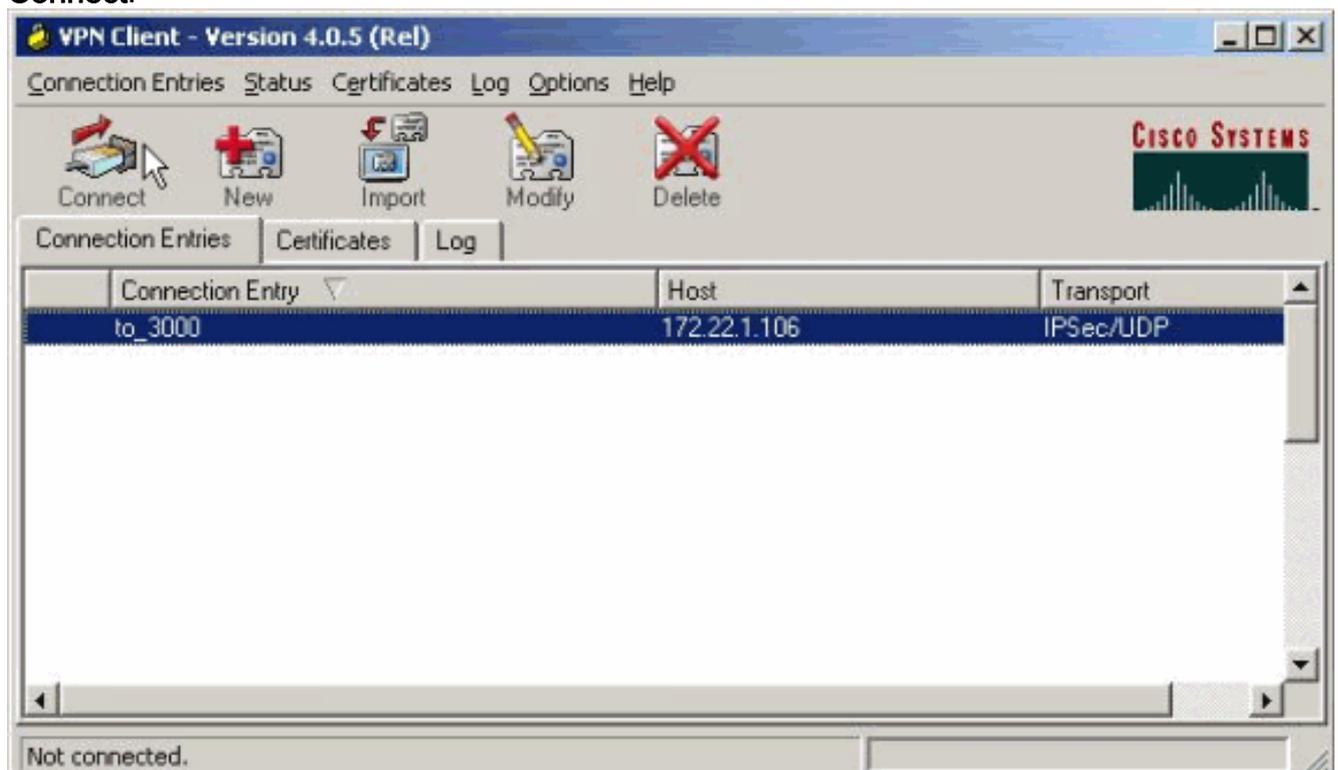
8. Cliquez sur **Apply** lorsque vous avez terminé.

## Vérification

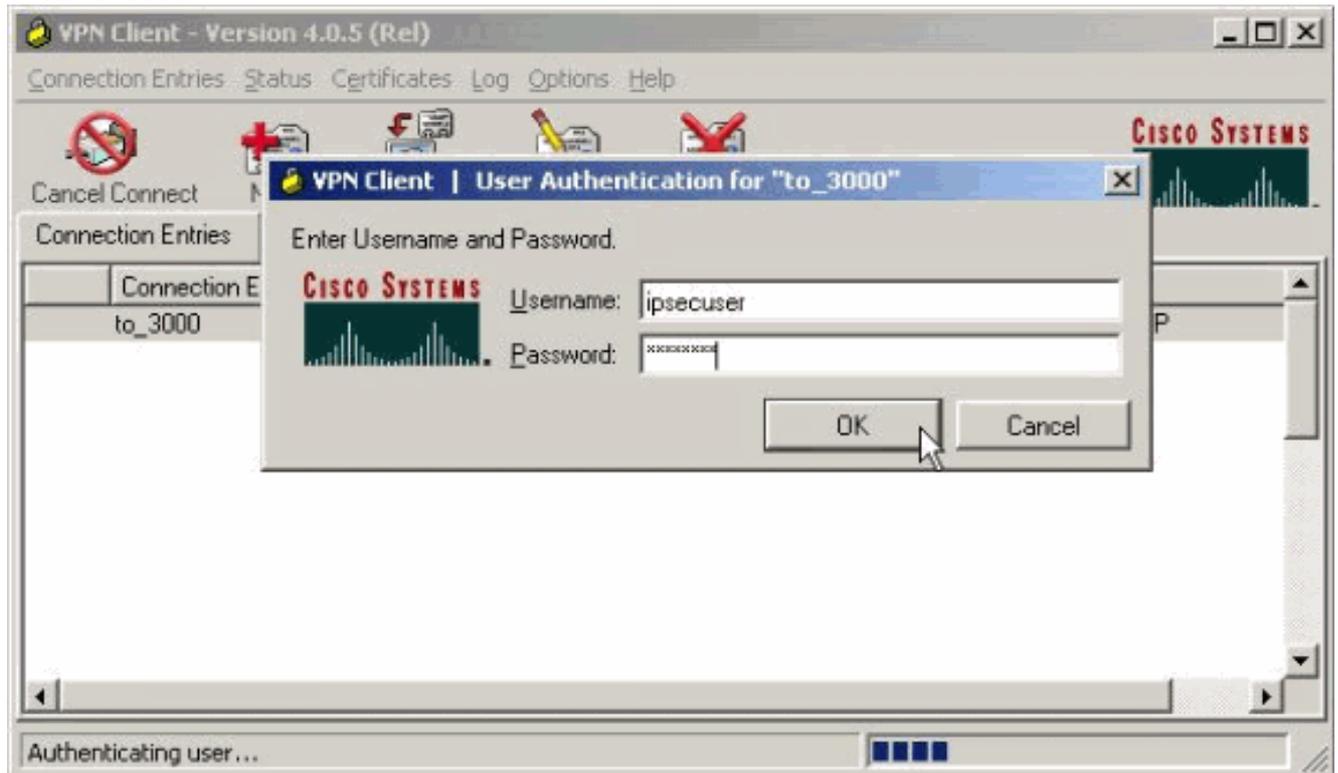
### Se connecter avec le client VPN

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

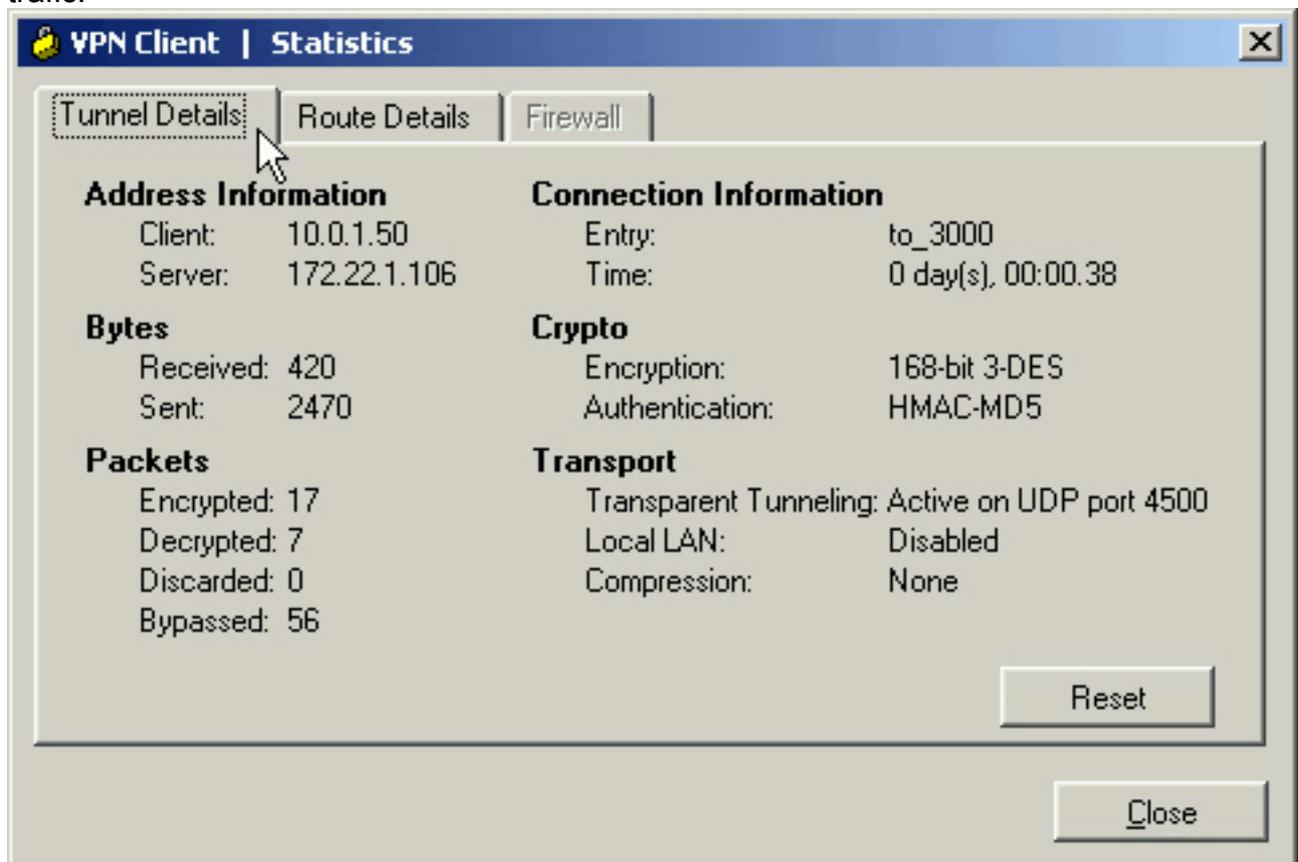
1. Choisissez votre entrée de connexion dans la liste et cliquez sur **Connect**.



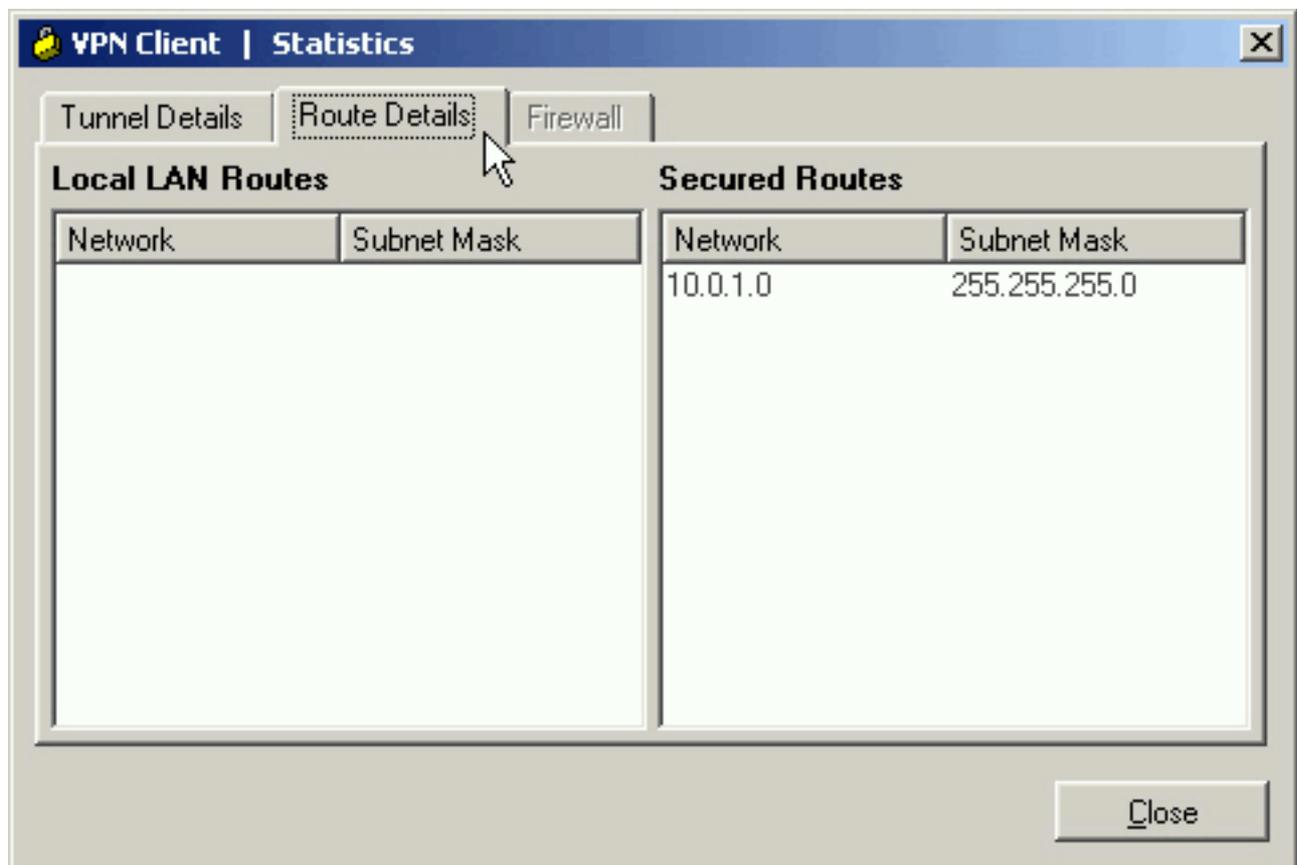
- Entrez dans vos informations d'identification.



- 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.

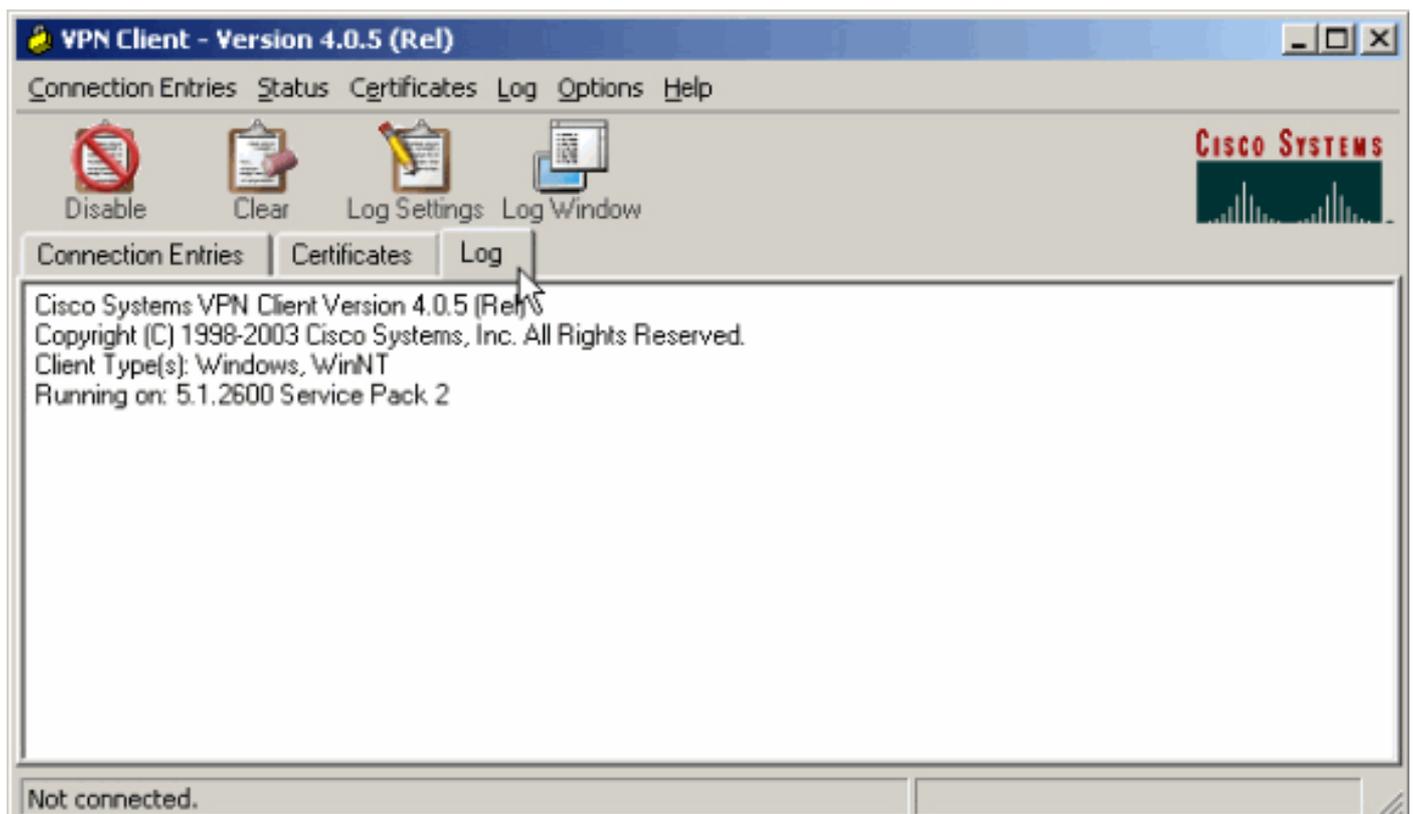


- Accédez à l'onglet **Route Details** afin de voir à quels réseaux le client VPN envoie du trafic chiffré. Dans cet exemple, le client VPN communique en toute sécurité avec 10.0.1.0/24 alors que tout autre trafic est envoyé non chiffré à Internet.



### [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 suppressed.* 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 suppressed.*

## 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](#)