Exemple de configuration d'IPsec entre un concentrateur VPN 3000 et un client VPN 4.x pour Windows à l'aide de RADIUS pour l'authentification et la comptabilisation des utilisateurs

Contenu

Introduction

Ce document décrit comment établir un tunnel d'IPsec entre un concentrateur de Cisco VPN 3000 et un Client VPN Cisco 4.x pour Microsoft Windows qui utilise le RAYON pour l'authentification de l'utilisateur et la comptabilité. Ce document recommande le Cisco Secure Access Control Server (ACS) pour Windows pour que la configuration RADIUS plus facile authentifie les utilisateurs qui se connectent à un concentrateur VPN 3000. Un groupe sur un concentrateur VPN 3000 est une collection d'utilisateurs traités comme entité simple. La configuration des groupes, par opposition aux utilisateurs individuels, peut simplifier des tâches de configuration de gestion du système et de ligne profilée.

Référez-vous à PIX/ASA 7.x et Client VPN Cisco 4.x pour Windows avec l'exemple de configuration d'authentification de RAYON du Microsoft Windows 2003 IAS afin d'installer la connexion VPN d'Accès à distance entre un Client VPN Cisco (4.x pour Windows) et l'appliance 7.x de Sécurité de gamme 500 PIX qui utilise un serveur de RAYON du Service d'authentification Internet de Microsoft Windows 2003 (IAS).

Référez-vous à la configuration d'IPSec entre un routeur Cisco IOS et un Client VPN Cisco 4.x pour Windows utilisant le RAYON pour l'authentification de l'utilisateur afin de configurer une connexion entre un routeur et le Client VPN Cisco 4.x qui utilise le RAYON pour l'authentification de l'utilisateur.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Le Cisco Secure ACS pour le RAYON de Windows est installé et fonctionne correctement avec d'autres périphériques.
- Le concentrateur de Cisco VPN 3000 est configuré et peut être géré avec l'interface HTML.

Composants utilisés

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

- Cisco Secure ACS pour Windows avec la version 4.0
- Concentrateur de la série Cisco VPN 3000 avec le fichier d'image 4.7.2.B
- Client VPN Cisco 4.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.

Conventions

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

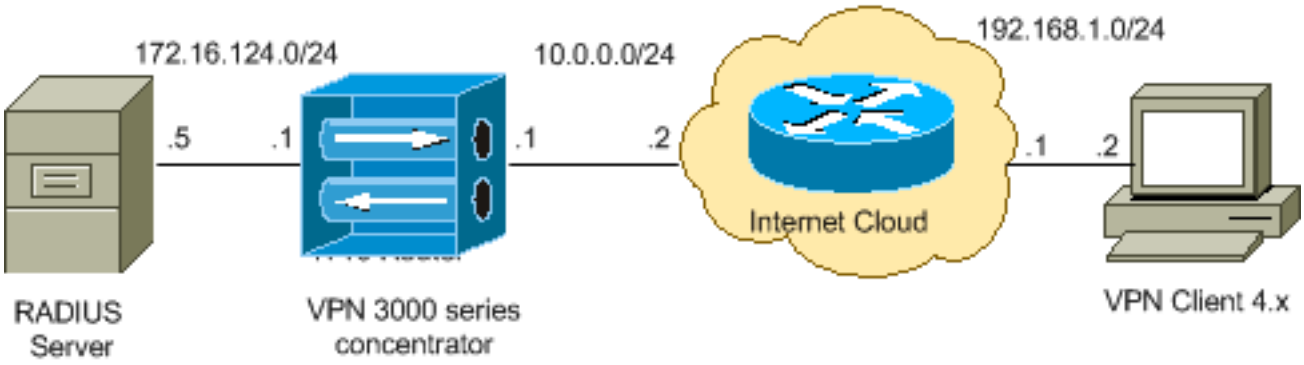
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Remarque: Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

Groupes d'utilisation sur le concentrateur VPN 3000

Des groupes peuvent être définis pour le Cisco Secure ACS pour Windows et le concentrateur VPN 3000, mais ils utilisent des groupes en quelque sorte différemment. Effectuez ces tâches afin de simplifier des choses :

- **Configurez un seul groupe sur le concentrateur VPN 3000** pour quand vous établissez le tunnel initial. Ceci s'appelle souvent le groupe de tunnel et il est utilisé pour établir une session chiffrée d'Échange de clés Internet (IKE) au concentrateur VPN 3000 utilisant une clé pré-partagée (le mot de passe de groupe). C'est le mêmes nom et mot de passe de groupe qui devraient être configurés sur tous les Clients VPN Cisco qui veulent se connecter au concentrateur VPN.
- **Configurez les groupes sur le Cisco Secure ACS pour des Windows Server** qui utilisent des attributs RADIUS standard et particularité de constructeur attribue (les VSAs) pour la Gestion des stratégies. Les VSAs qui devraient être utilisés avec le concentrateur VPN 3000 sont les attributs du RAYON (VPN 3000).
- **Configurez les utilisateurs sur le Cisco Secure ACS pour le serveur de RAYON de Windows et affectez-les à un des groupes** configurés sur le même serveur. Les utilisateurs héritent des attributs définis pour leur groupe et le Cisco Secure ACS pour Windows envoie ces attributs au concentrateur VPN quand l'utilisateur est authentifié.

Comment le concentrateur VPN 3000 utilise des attributs de groupe et d'utilisateur

Après que le concentrateur VPN 3000 authentifie le groupe de tunnel avec le concentrateur VPN et l'utilisateur avec le RAYON, il doit organiser les attributs qu'il a reçus. Le concentrateur VPN utilise les attributs dans cet ordre de préférence, si l'authentification est faite dans le concentrateur VPN ou avec le RAYON :

1. **Attributs d'utilisateur** — Ces attributs ont toujours la priorité au-dessus de tous les autres.
2. **Attributs de groupe de tunnel** — Tous les attributs non retournés quand l'utilisateur a été authentifié sont complétés par les attributs de groupe de tunnel.
3. **Attributs de groupe de base** — En attribue des disparus de l'utilisateur ou des attributs de groupe de tunnel sont complétés par les attributs de groupe de base de concentrateur VPN.

Configuration du concentrateur de la gamme VPN 3000

Remplissez la procédure dans cette section afin de configurer un concentrateur de Cisco VPN 3000 pour les paramètres requis à la connexion d'IPsec aussi bien qu'au client d'AAA pour que l'utilisateur VPN authentifie avec le serveur de RAYON.

En cette configuration de laboratoire, le concentrateur VPN est d'abord accédé à par le port de console et une configuration minimale est ajoutée pendant que cette sortie affiche :

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address ------------------------------------------------------------
-------------- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | --------------------
---------------------------------------------------- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
------------------------------------------------------------------------ Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | ------------------------------------------------------
--------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----------
------------------------------------------------------------------- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ------------------------------------------------
--------------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

Le concentrateur VPN apparaît dans la configuration rapide, et ces éléments sont configurés.

- Heure/date
- Interfaces/masques dans le **Configuration > Interfaces** (public=10.0.0.1/24, private=172.16.124.1/24)
- Passerelle par défaut dans la **configuration > le système > le Routage IP > le Default_Gateway** (10.0.0.2)

En ce moment, le concentrateur VPN est accessible par le HTML du réseau intérieur.

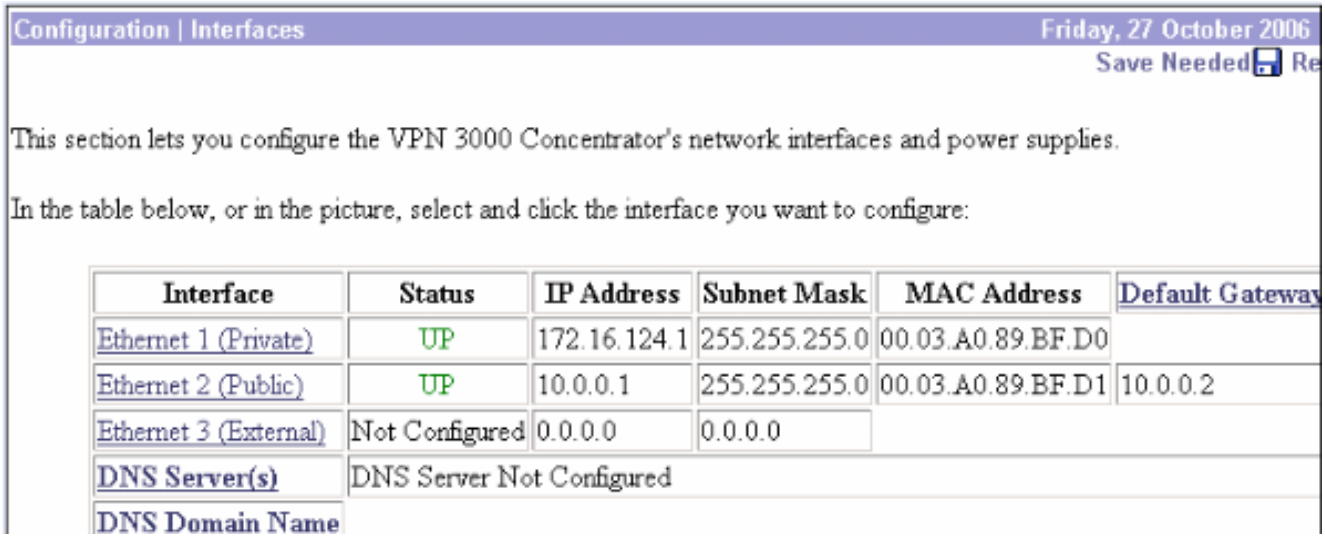
Remarque: Si le concentrateur VPN est géré de l'extérieur, vous exécutez également ces étapes :

1. Choisissez la **configuration > le filtre IP 1-Interfaces > 2-Public > 4-Select > 1. privé (par défaut)**.
2. Choisissez la **gestion > le 7-Access redresse > liste de contrôle 2-Access > poste de travail du gestionnaire 1-Add** afin d'ajouter l'adresse IP du gestionnaire externe.

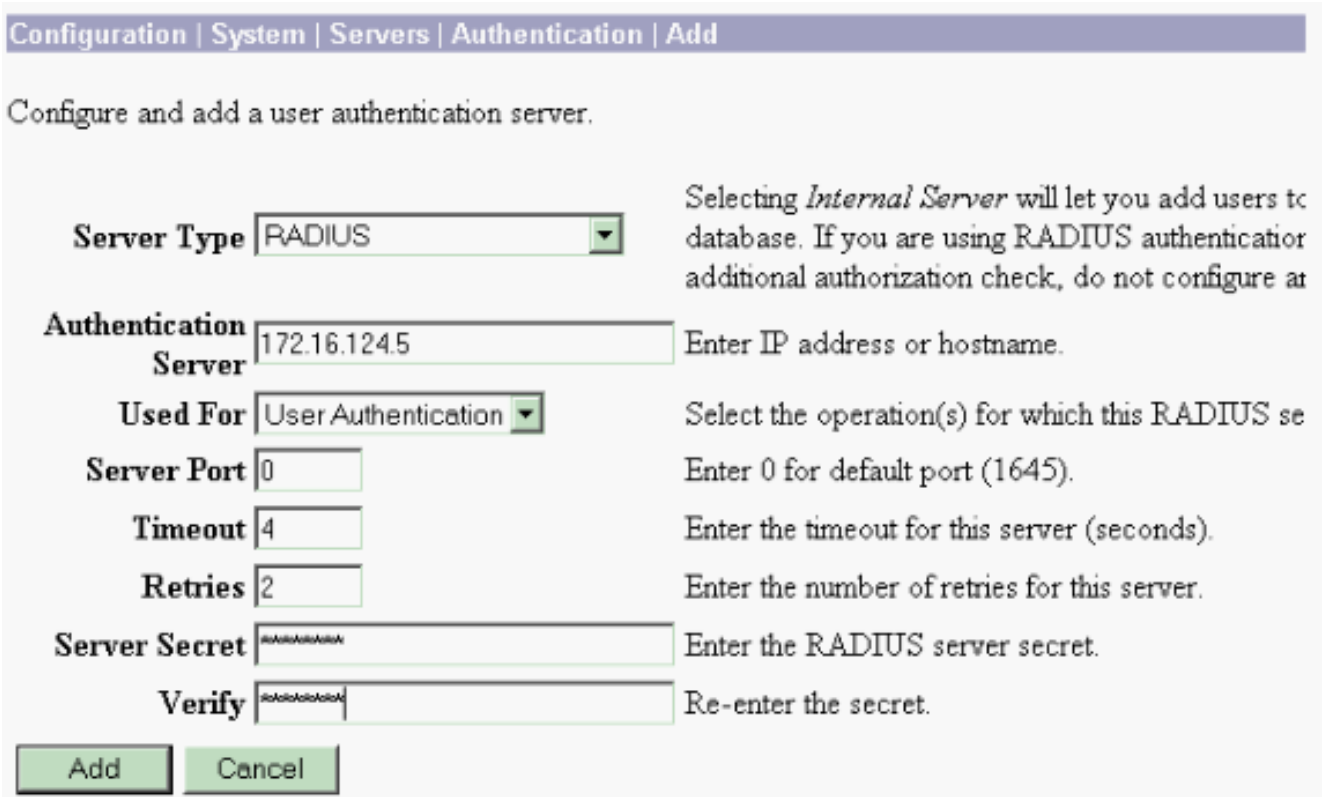
Ces étapes sont seulement exigées si vous gérez le concentrateur VPN de l'extérieur.

Une fois que vous vous êtes terminé ces deux étapes, le reste de la configuration peut être fait le GUI à l'aide d'un navigateur Web et en se connectant à l'IP de l'interface que vous avez juste configurée. Dans cet exemple et en ce moment, le concentrateur VPN est accessible par le HTML du réseau intérieur :

1. Choisissez le **Configuration > Interfaces** afin de revérifier les interfaces après que vous apportiez le
   GUI.

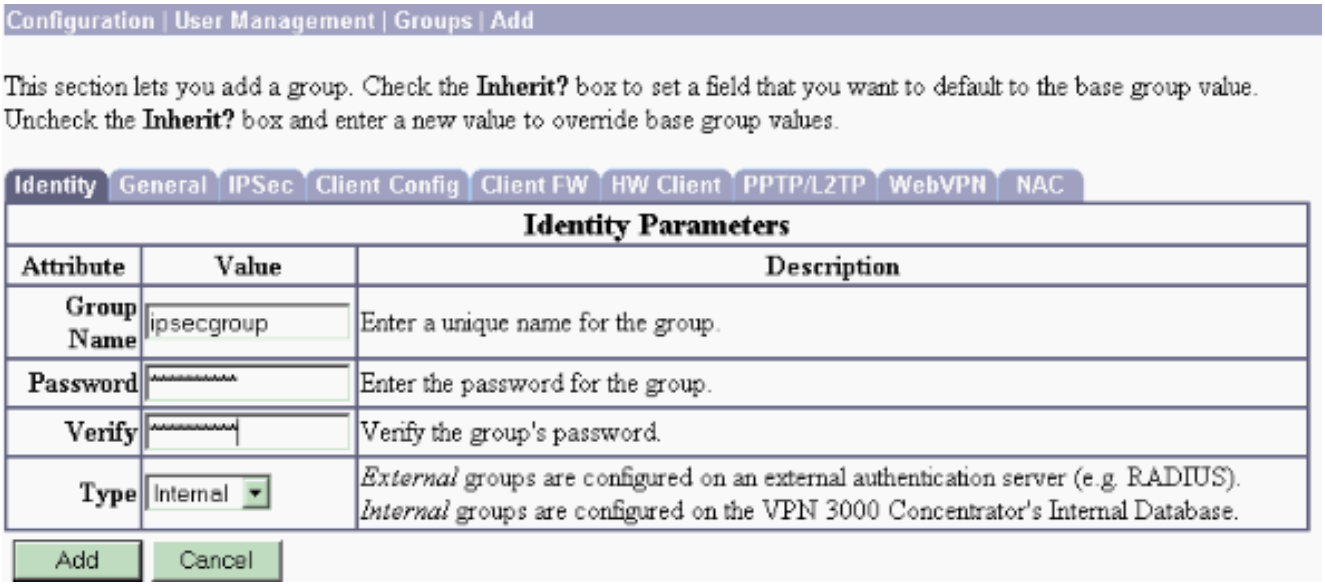


2. Terminez-vous ces étapes afin d'ajouter le Cisco Secure ACS pour le serveur de RAYON de Windows à la configuration de concentrateur VPN 3000.Choisissez la **configuration > le système > les serveurs > l'authentification**, et cliquez sur Add du menu de
   gauche.

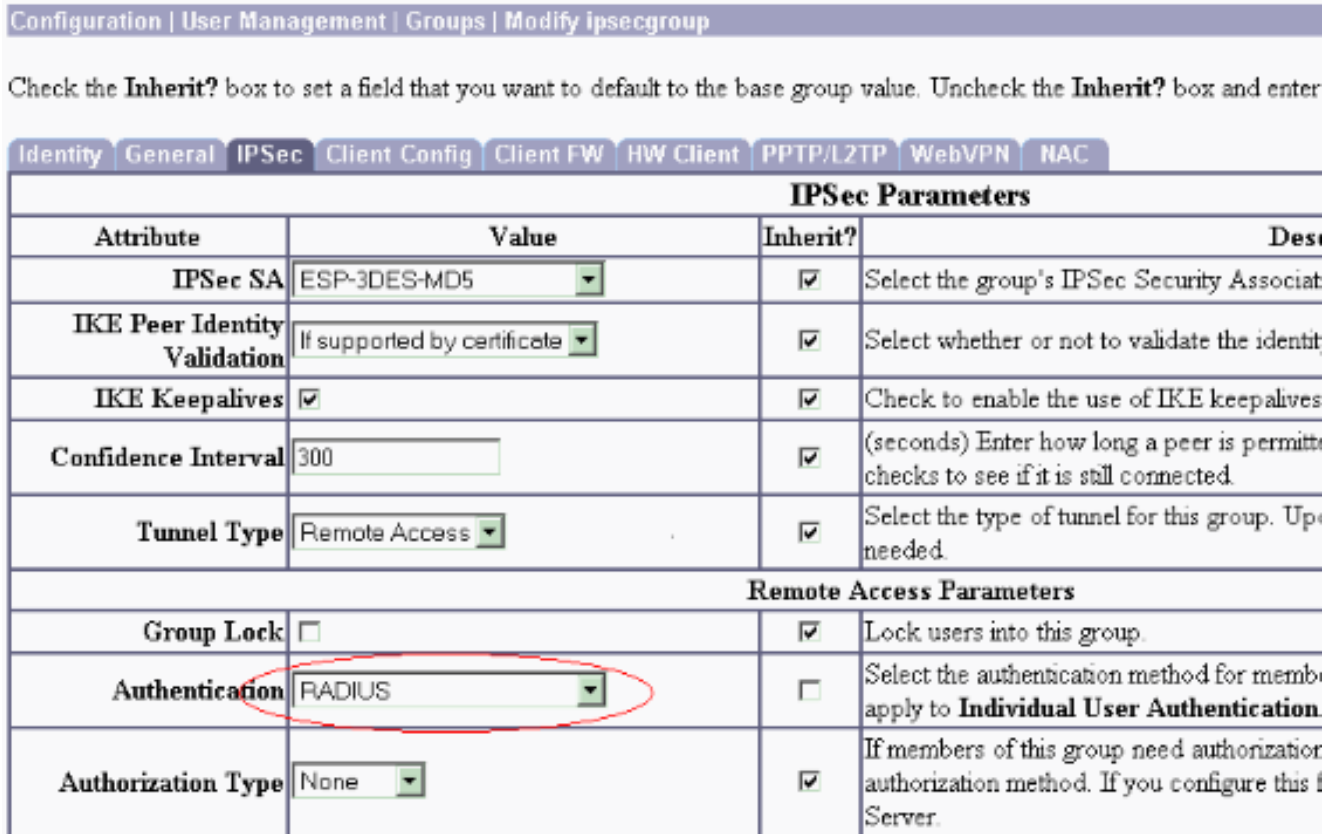


Choisissez le **RAYON de** type de serveur et ajoutez ces paramètres pour votre Cisco Secure ACS pour le serveur de RAYON de Windows. Laissez tous autres paramètres dans leur état par défaut.**Serveur d'authentification** — Écrivez l'adresse IP de votre Cisco Secure ACS pour le serveur de RAYON de Windows.**Secret de serveur** — Écrivez le secret de serveur de RAYON. Ceci doit être le même secret que vous utilisez quand vous configurez le concentrateur VPN 3000 dans le Cisco Secure ACS pour la configuration de Windows.**Vérifiez** — Ressaisissez le mot de passe pour la vérification.Ceci ajoute le serveur d'authentification en configuration globale du concentrateur VPN 3000. Ce serveur est utilisé par tous les groupes excepté quand un serveur d'authentification a été spécifiquement défini. Si un serveur d'authentification n'est pas configuré pour un groupe, il retourne au serveur global d'authentification.

3. Terminez-vous ces étapes afin de configurer le groupe de tunnel sur le concentrateur VPN 3000.Choisissez le **Configuration > User Management > Groups du** menu de gauche et cliquez sur Add.Changez ou ajoutez ces paramètres dans les onglets de configuration. Ne cliquez sur Apply pas jusqu'à ce que vous changiez tous ces paramètres :**Remarque:** Ces paramètres sont le minimum requis pour des connexions VPN d'Accès à distance. Ces paramètres supposent également que les valeurs par défaut dans le groupe de base sur le concentrateur VPN 3000 n'ont pas été changées.**Identité**

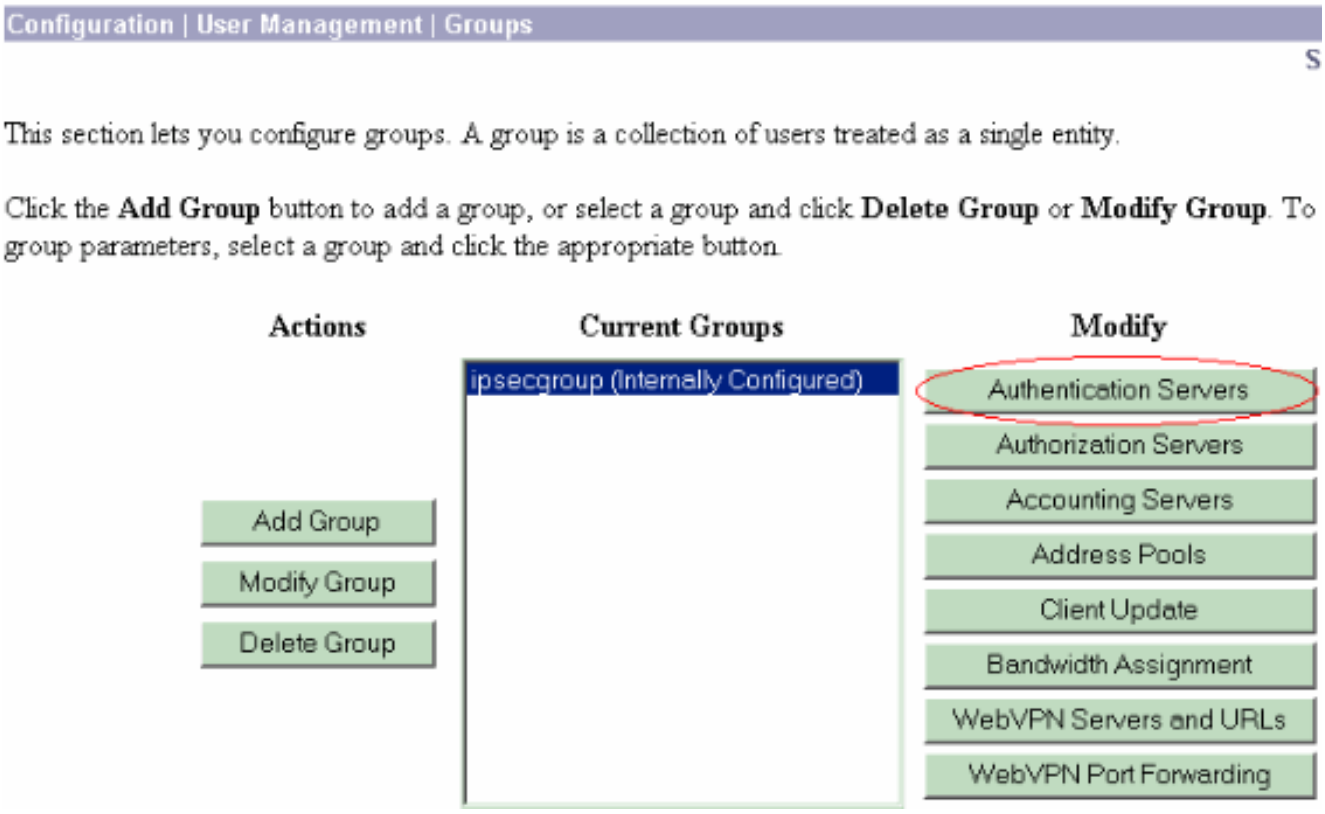


Nom de groupe — Introduisez un nom de groupe. Par exemple, IPsecUsers.**Mot de passe** — Entrez un mot de passe pour le groupe. C'est la clé pré-partagée pour la session d'IKE.**Vérifiez** — Ressaisissez le mot de passe pour la vérification.**Type** — Laissez ceci comme par défaut :
Interne.**IPsec**



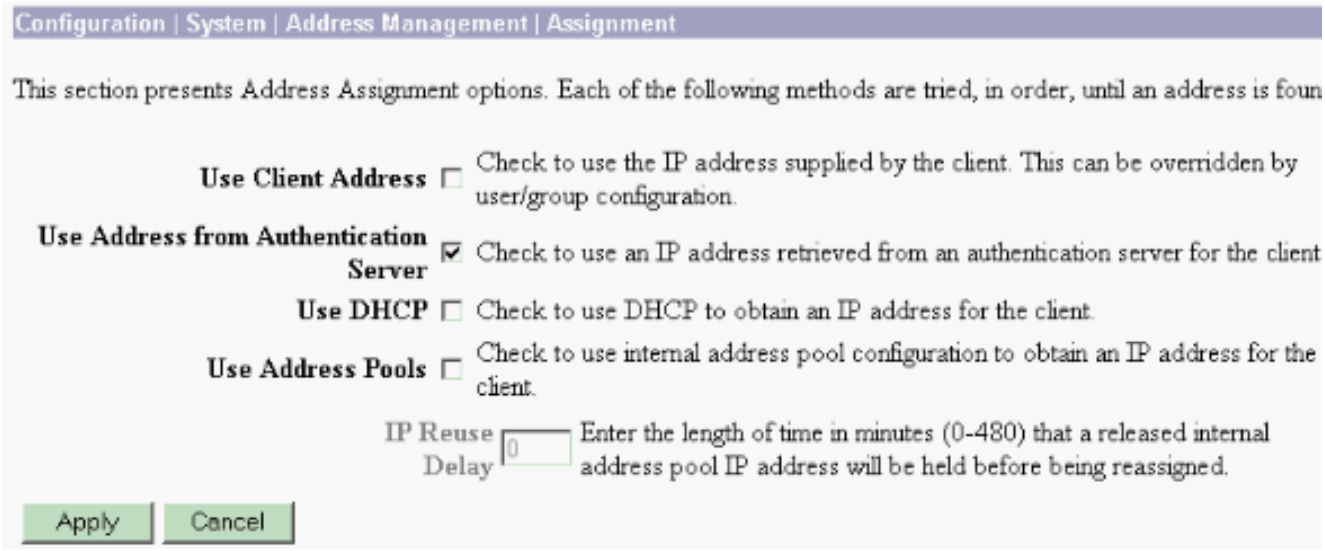
Type de tunnel — Choisissez la **remote-access**.**Authentification** — RAYON. Ceci indique au concentrateur VPN quelle méthode à l'utiliser pour authentifier des utilisateurs.**Mode Config** — **Mode Config de** contrôle.Cliquez sur **Apply**.

4. Terminez-vous ces étapes afin de configurer de plusieurs serveurs d'authentification sur le concentrateur VPN 3000.Une fois que le groupe est défini, mettez en valeur ce groupe, et cliquez sur les **serveurs d'authentification** sous la colonne de modifier. Différents serveurs d'authentification peuvent être définis pour chaque groupe même si ces serveurs n'existent pas dans les serveurs
globaux.



Choisissez le **RAYON de** type de serveur, et ajoutez ces paramètres pour votre Cisco Secure ACS pour le serveur de RAYON de Windows. Laissez tous autres paramètres dans leur état par défaut.**Serveur d'authentification** — Écrivez l'adresse IP de votre Cisco Secure ACS pour le serveur de RAYON de Windows.**Secret de serveur** — Écrivez le secret de serveur de RAYON. Ceci doit être le même secret que vous utilisez quand vous configurez le concentrateur VPN 3000 dans le Cisco Secure ACS pour la configuration de Windows.**Vérifiez** — Ressaisissez le mot de passe pour la vérification.

5. Choisissez la **configuration > le système > l'adresse d'utilisation de gestion d'adresses > d'affectation** et de contrôle du **serveur d'authentification** afin d'assigner l'adresse IP aux clients vpn du pool d'IP créé dans le serveur de RAYON une fois que le client obtient authentifié.



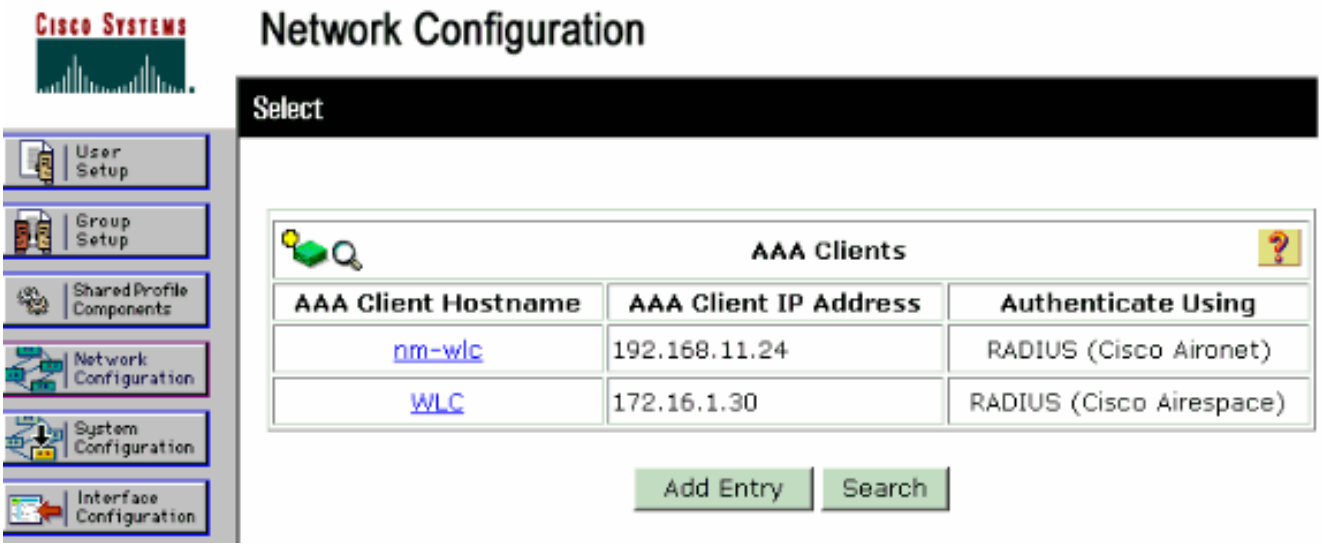
Configuration du serveur RADIUS

Cette section du document décrit la procédure exigée pour configurer le Cisco Secure ACS en tant que serveur de RAYON pour l'authentification d'utilisateur de client VPN expédié par le

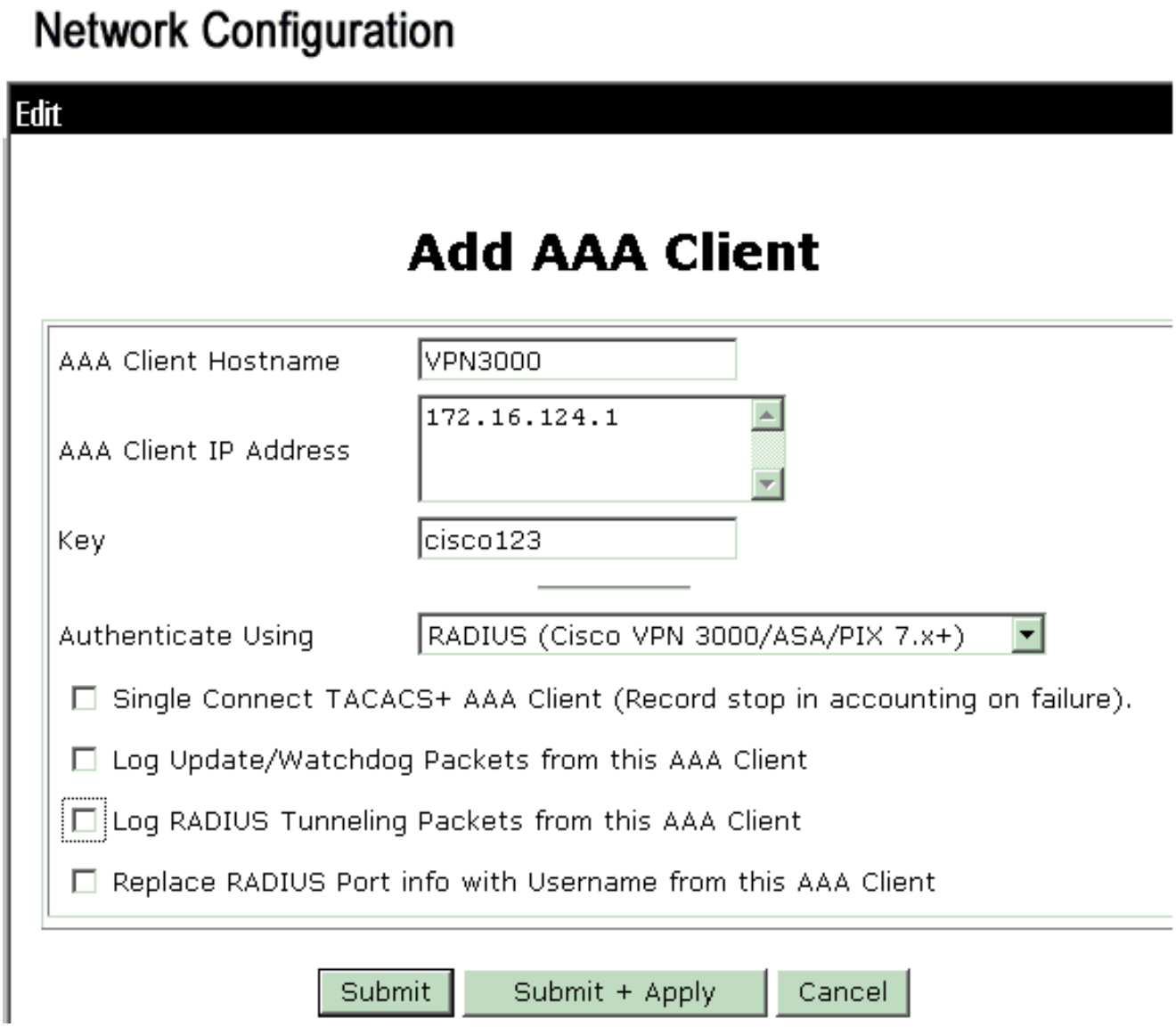
Concentrateur de la série Cisco VPN 3000 - client d'AAA.

Double-cliquer l'icône d'**admin ACS** afin de commencer la session d'admin sur le PC qui exécute le Cisco Secure ACS pour le serveur de RAYON de Windows. Procédure de connexion avec le nom d'utilisateur et mot de passe approprié, s'il y a lieu.

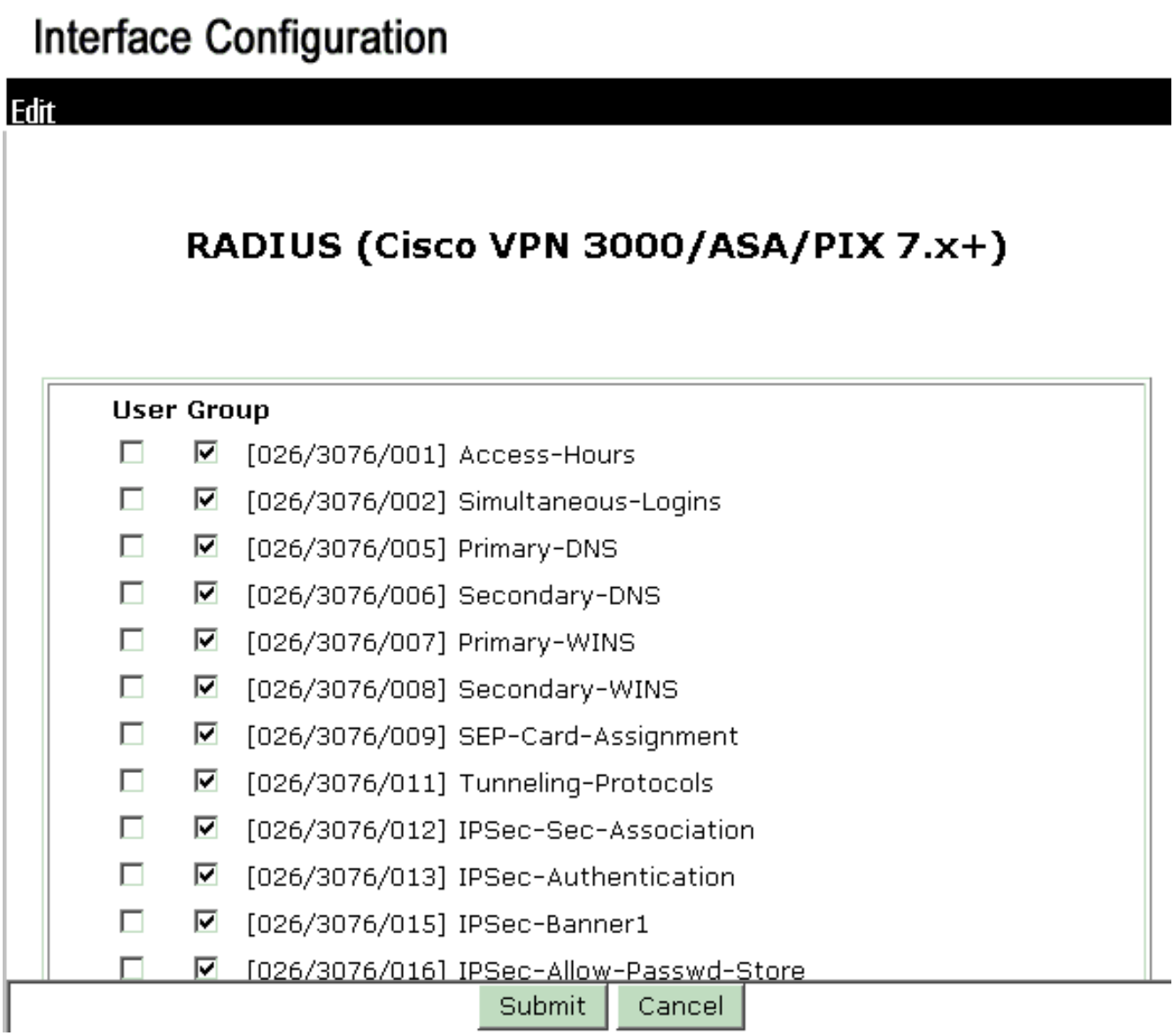
1. Terminez-vous ces étapes afin d'ajouter le concentrateur VPN 3000 au Cisco Secure ACS pour la configuration de Windows Server.Choisissez la **configuration réseau** et cliquez sur Add l'**entrée** afin d'ajouter un client d'AAA au serveur de RAYON.



Ajoutez ces paramètres pour votre concentrateur VPN 3000 :

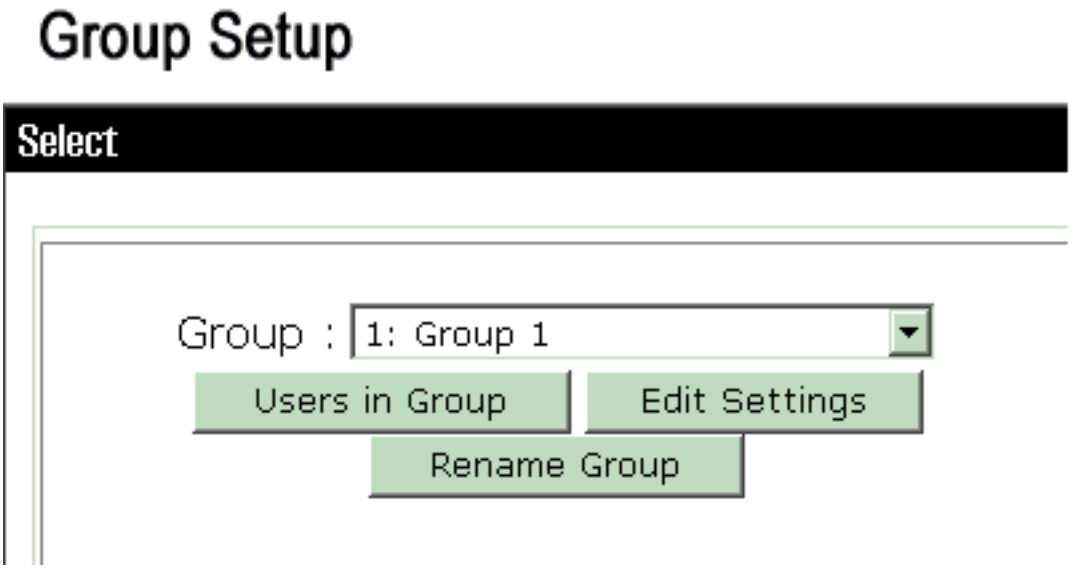


Adresse Internet de client d'AAA — Entrez dans l'adresse Internet de votre concentrateur VPN 3000 (pour la résolution de DN).**Adresse IP de client d'AAA** — Écrivez l'adresse IP de votre concentrateur VPN 3000.**Clé** — Écrivez le secret de serveur de RAYON. Ceci doit être le même secret que vous avez configuré quand vous avez ajouté le serveur d'authentification sur le concentrateur VPN.**Authentifiez utilisant** — Choisissez le **RAYON (Cisco VPN 3000/ASA/PIX 7.x+)**. Ceci permet aux VSAs VPN 3000 pour afficher dans la fenêtre de configuration de groupe.Cliquez sur **Submit**.Choisissez la **configuration d'interface**, cliquez sur le **RAYON (Cisco VPN 3000/ASA/PIX 7.x+)**, et vérifiez la Constructeur-**particularité du groupe**
[26].

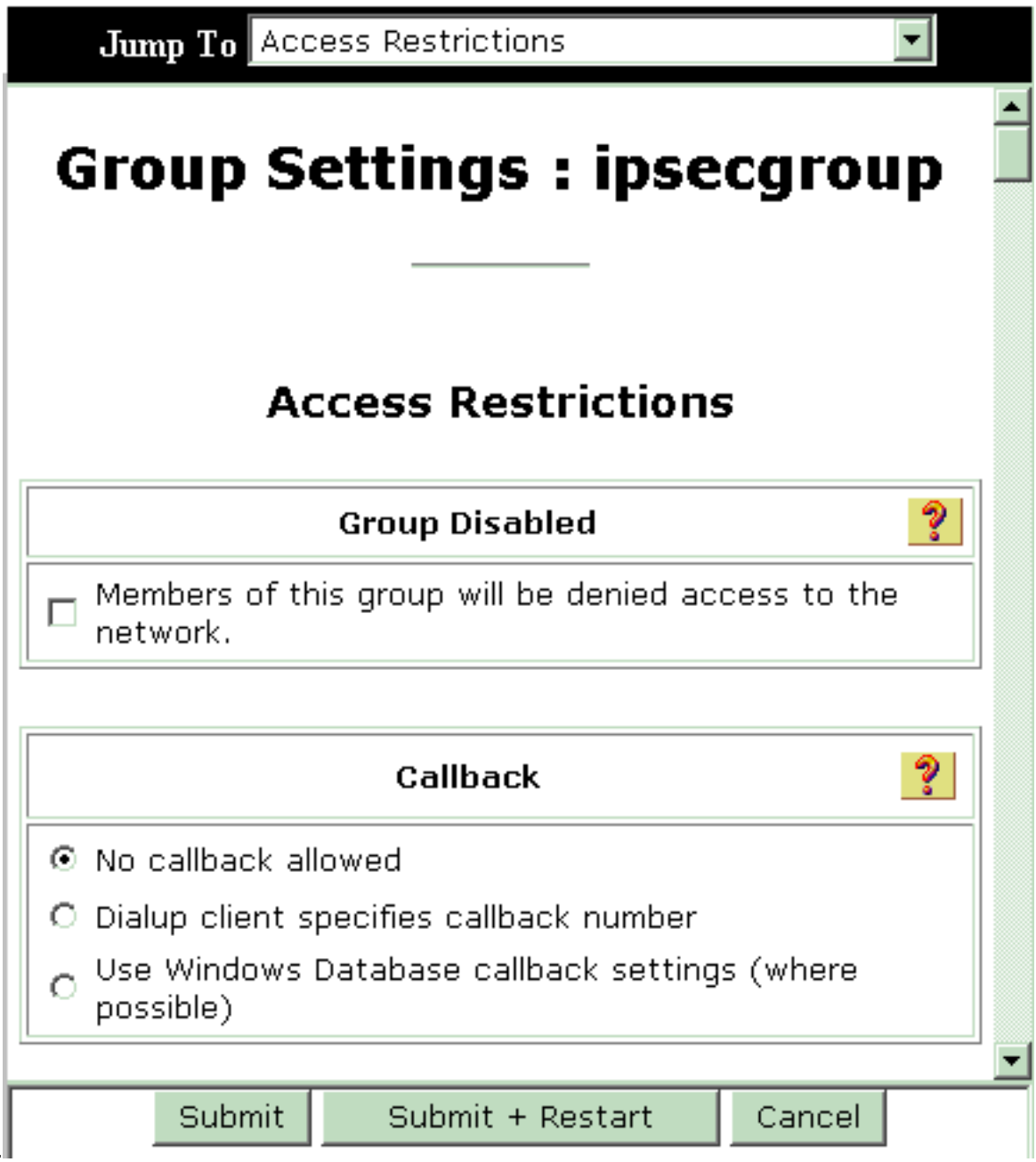


Remarque: Le 'attribut RADIUS 26' se rapporte à tous les attributs spécifiques de constructeur. Par exemple, choisissez la **configuration d'interface > le RAYON (Cisco VPN 3000)** et voyez que tout les début disponible d'attributs avec 026. Ceci prouve que tous ces attributs spécifiques de constructeur tombent sous la norme du RAYON 26 IETF. Ces attributs n'apparaissent pas dans l'installation d'utilisateur ou de groupe par défaut. Afin de révéler dans l'installation de groupe, créez un client d'AAA (dans ce cas concentrateur VPN 3000) qui authentifie avec le RAYON en configuration réseau. Vérifiez alors les attributs qui doivent apparaître dans l'installation utilisateur, le Group Setup, ou chacun des deux de la configuration d'interface.Référez-vous aux attributs RADIUS pour plus d'informations sur les attributs disponibles et leur utilisation.Cliquez sur **Submit**.

2. Terminez-vous ces étapes afin d'ajouter des groupes au Cisco Secure ACS pour la configuration de Windows.Choisissez le **Group Setup**, puis sélectionnez un des groupes de modèle, par exemple, le groupe 1, et le clic **renomment le**

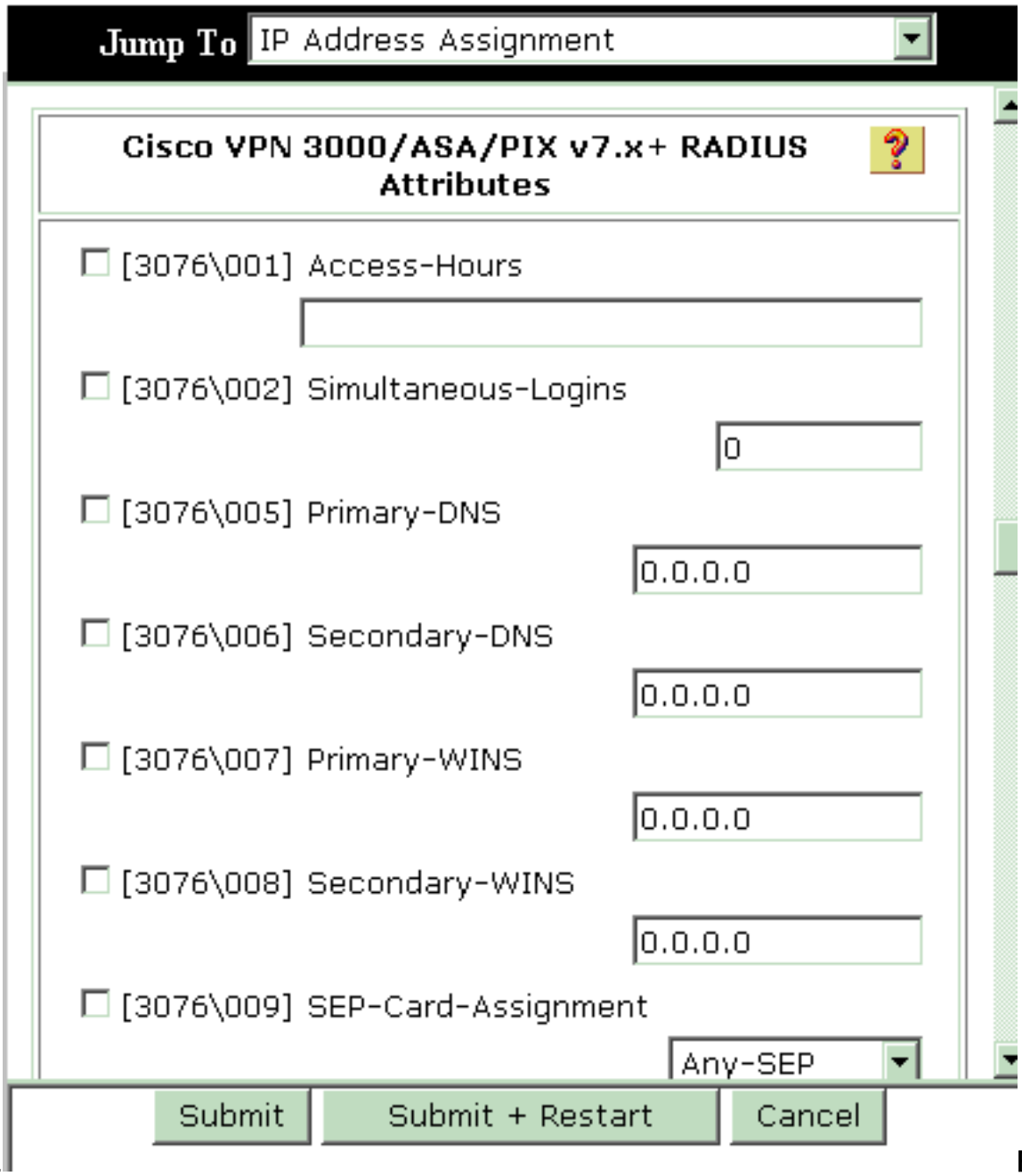


groupe. Changez le nom à quelque chose appropriée pour votre organisation., par exemple, ipsecgroup. Puisque des utilisateurs sont ajoutés à ces groupes, faites le nom de groupe refléter le but réel de ce groupe. Si tous les utilisateurs sont mis dans le même groupe, vous pouvez l'appeler des users group VPN.Cliquez sur Edit les **configurations** afin d'éditer les paramètres dans votre groupe nouvellement



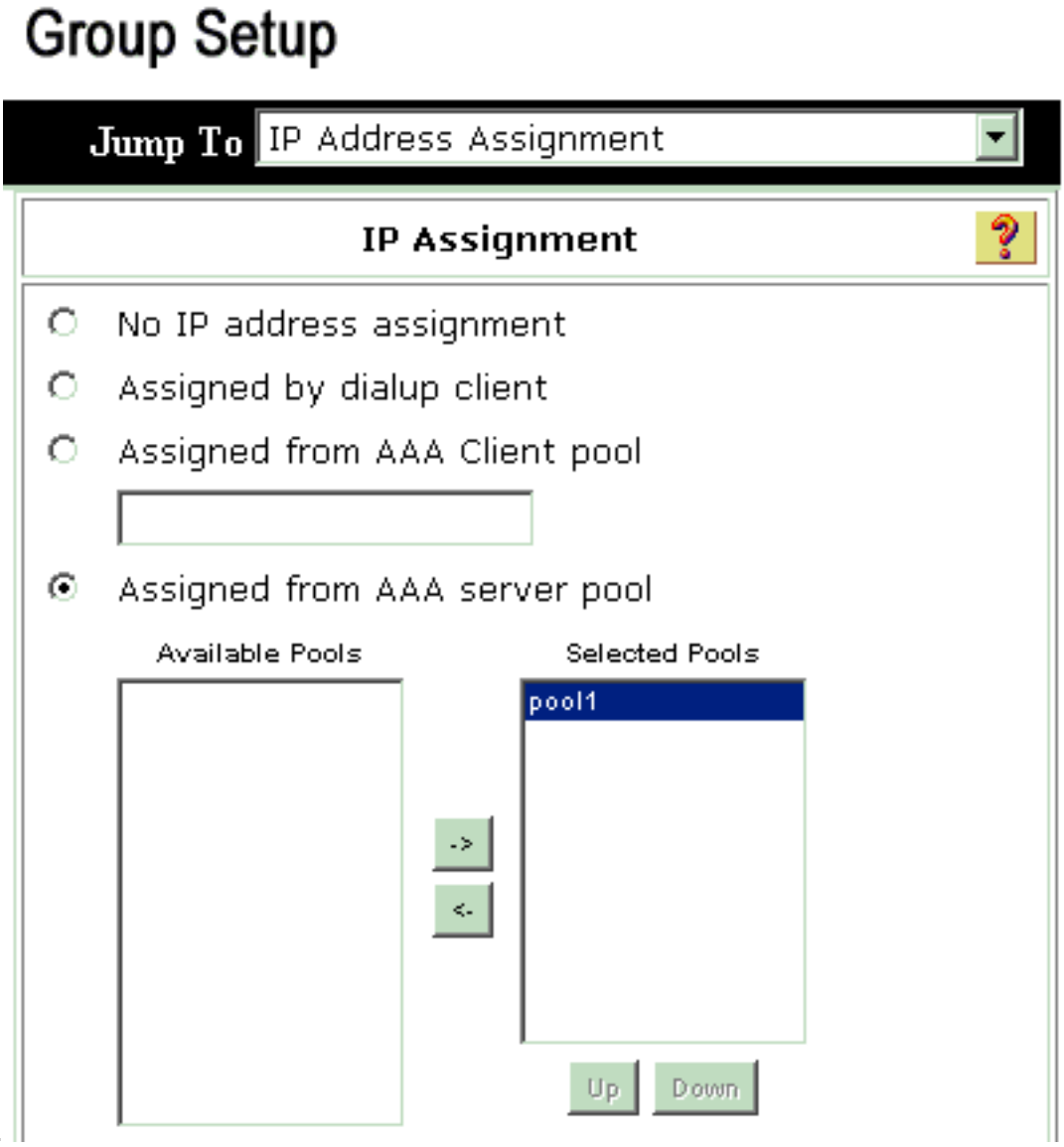
renommé.

Cliquez sur le **RAYON de Cisco VPN 3000** et configurez ces attributs recommandés. Ceci permet des utilisateurs assignés à ce groupe pour hériter des attributs RADIUS de Cisco VPN 3000, qui te permet pour centraliser des stratégies pour tous les utilisateurs dans le Cisco Secure ACS pour



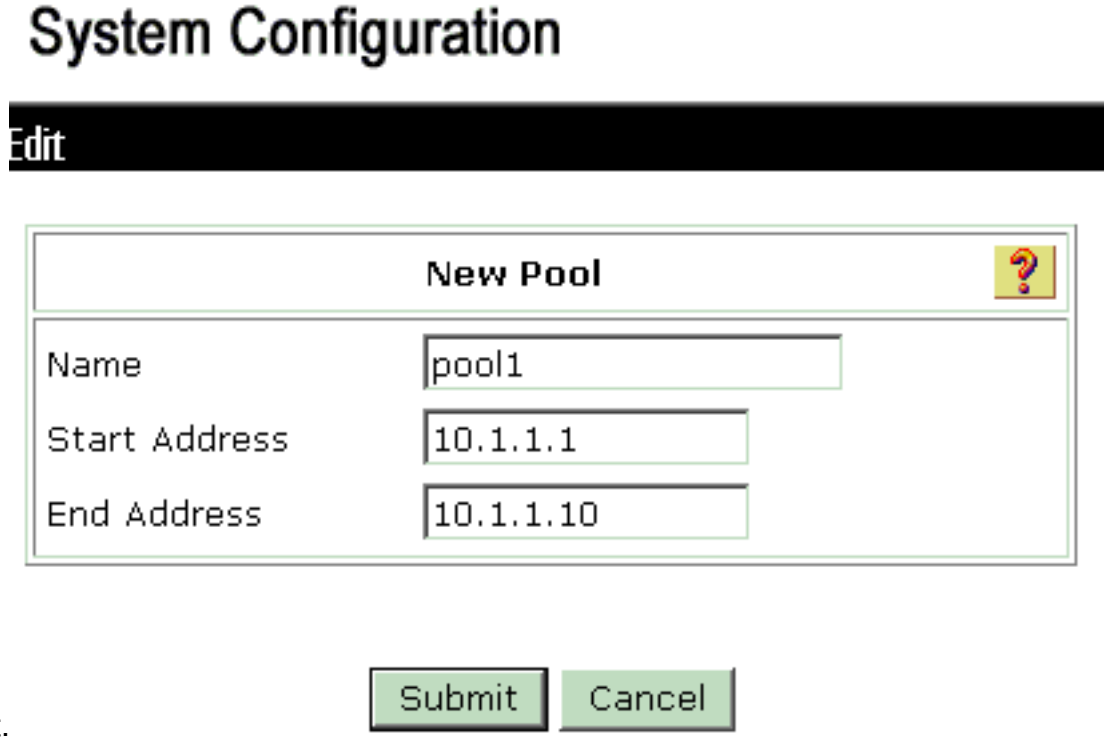
Windows. **Re marque:** Techniquement, les attributs RADIUS VPN 3000 ne sont pas exigés pour être configurés tant que le groupe de tunnel est installé dans l'étape 3 de la configuration du concentrateur de la gamme VPN 3000 et le groupe de base dans le concentrateur VPN ne change pas des valeurs par défaut d'origine.**Attributs VPN 3000 recommandés :DNS principal** — Écrivez l'adresse IP de votre serveur de DNS principal.**DNS secondaire** — Écrivez l'adresse IP de votre serveur de DNS secondaire.**PRIMAIRE-WINS** — Écrivez l'adresse IP de votre serveur WINS primaire.**SECONDAIRE-WINS** — Écrivez l'adresse IP de votre serveur WINS secondaire.**Tunnellisation-protocoles** — Choisissez **IPsec**. Ceci permet *seulement des* connexions client d'IPsec. On ne permet pas PPTP ou L2TP.**IPsec-Sec-association** — Écrivez **ESP-3DES-MD5**. Ceci s'assure que tous vos clients d'IPsec se connectent au cryptage le plus élevé disponible.**IPsec-Autoriser-Mot de passe-mémoire** — Choisissez **rejettent** ainsi des utilisateurs ne sont pas permis pour sauvegarder leur mot de passe dans le client vpn.**IPsec-bannière** — Entrez dans une bannière de message d'accueil à présenter à l'utilisateur sur la connexion. Par exemple, « accueil à l'accès VPN des employés de MyCompany ! »**Domaine d'IPsec-par défaut** — Écrivez le nom de domaine de

votre société. Par exemple, « mycompany.com ».Cet ensemble d'attributs n'est pas nécessaire. Mais si vous êtes incertain si les attributs de groupe de base du concentrateur VPN 3000 ont changé, alors Cisco recommande que vous configuriez ces attributs :**Simultané-procédures de connexion** — Écrivez le nombre de fois où vous permettez à un utilisateur pour ouvrir une session simultanément avec le même nom d'utilisateur. La recommandation est 1 ou 2.**Sept-Carte-affectation** — Choisissez Tout-**SEPT**.**IPsec-Mode-config** — Choisissez **EN FONCTION**.**IPsec au-dessus d'UDP** — Choisissez **HORS FONCTION**, à moins que vous vouliez que les utilisateurs dans ce groupe se connectent utilisant IPsec au-dessus du protocole UDP. Si vous sélectionnez EN FONCTION, le client vpn a toujours la capacité localement de désactiver IPsec au-dessus d'UDP et de se connecter normalement.**IPsec au-dessus de port UDP** — Sélectionnez un numéro de port UDP de l'ordre de 4001 à 49151. Ceci est utilisé seulement si IPsec au-dessus d'UDP est allumé.Le prochain ensemble d'attributs exige que vous placez quelque chose sur le concentrateur VPN d'abord avant que vous puissiez les utiliser. Ceci est seulement recommandé pour des utilisateurs avancés.**Access-heures** — Ceci exige de vous d'installer une chaîne des heures d'Access sur le concentrateur VPN 3000 sous la **configuration >** la **Gestion des stratégies**. Au lieu de cela, heures d'Access d'utilisation disponibles dans le Cisco Secure ACS pour que Windows gère cet attribut.**IPsec-Fractionnement-Tunnel-liste** — Ceci exige de vous d'installer une liste des réseaux sur le concentrateur VPN sous la **configuration >** la **Gestion des stratégies >** la **gestion de trafic**. C'est une liste de réseaux envoyée vers le bas au client qui indiquent le client chiffrer des données seulement à ces réseaux dans la liste.Choisissez l'**affectation IP dans l'installation de groupe** et le contrôle **assigné du groupe de serveur d'AAA** afin d'assigner les adresses IP aux utilisateurs de client vpn une fois qu'elles sont obtiennent

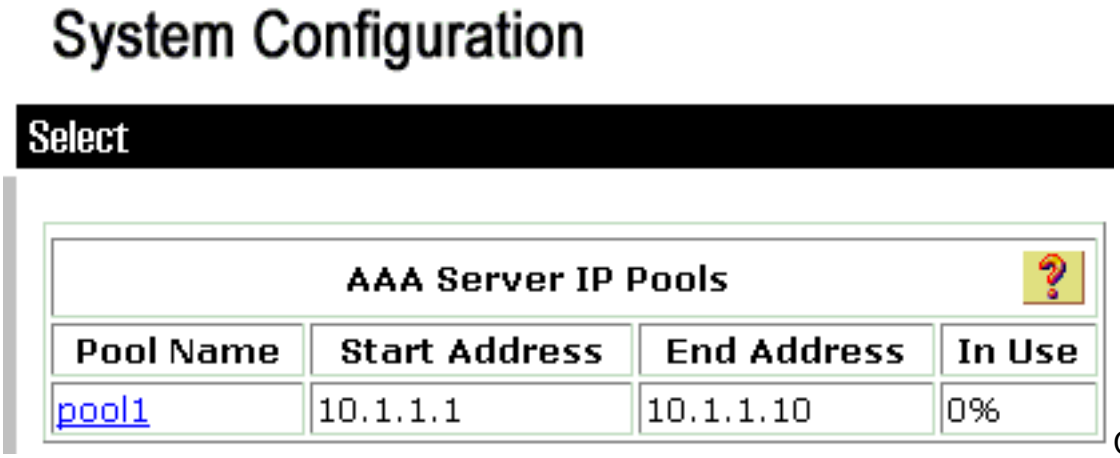


authentifié. Ch

oisissez la **configuration système > les groupes IP** afin de créer un pool d'IP pour des utilisateurs de client vpn et cliquer sur

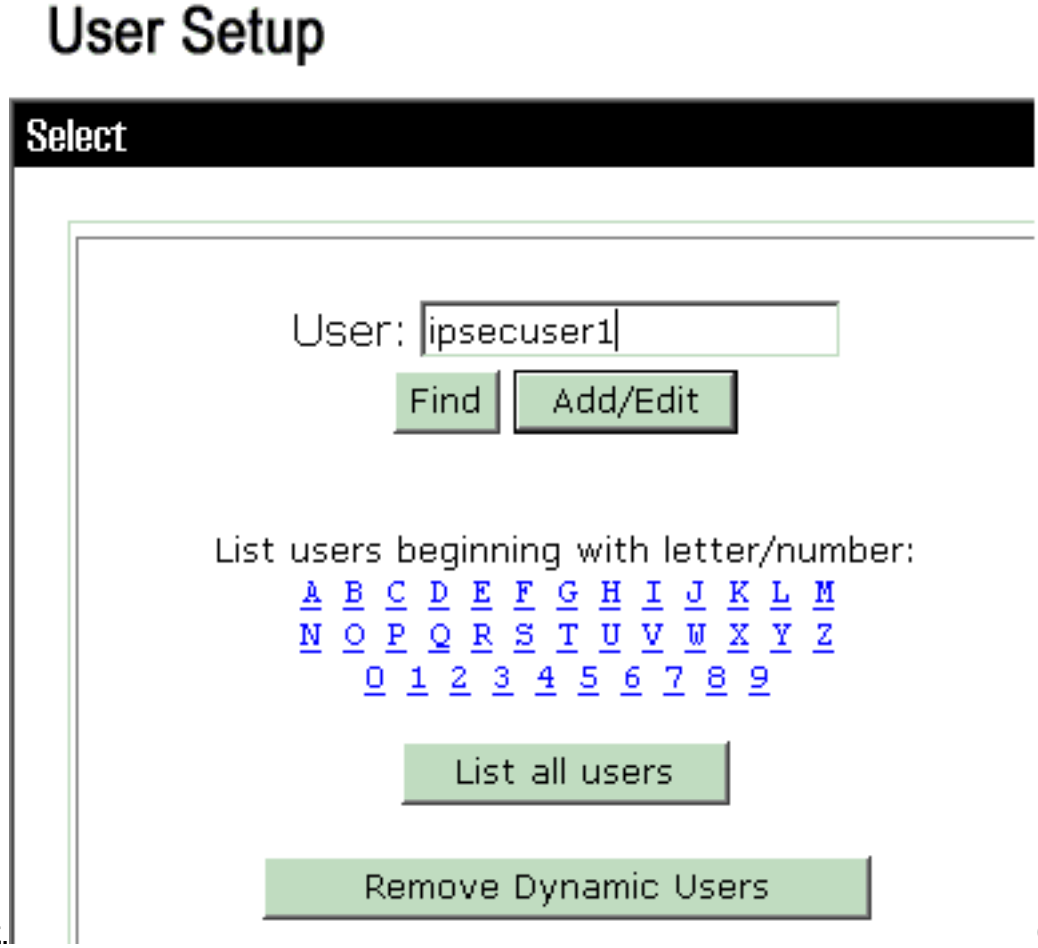


Submit.

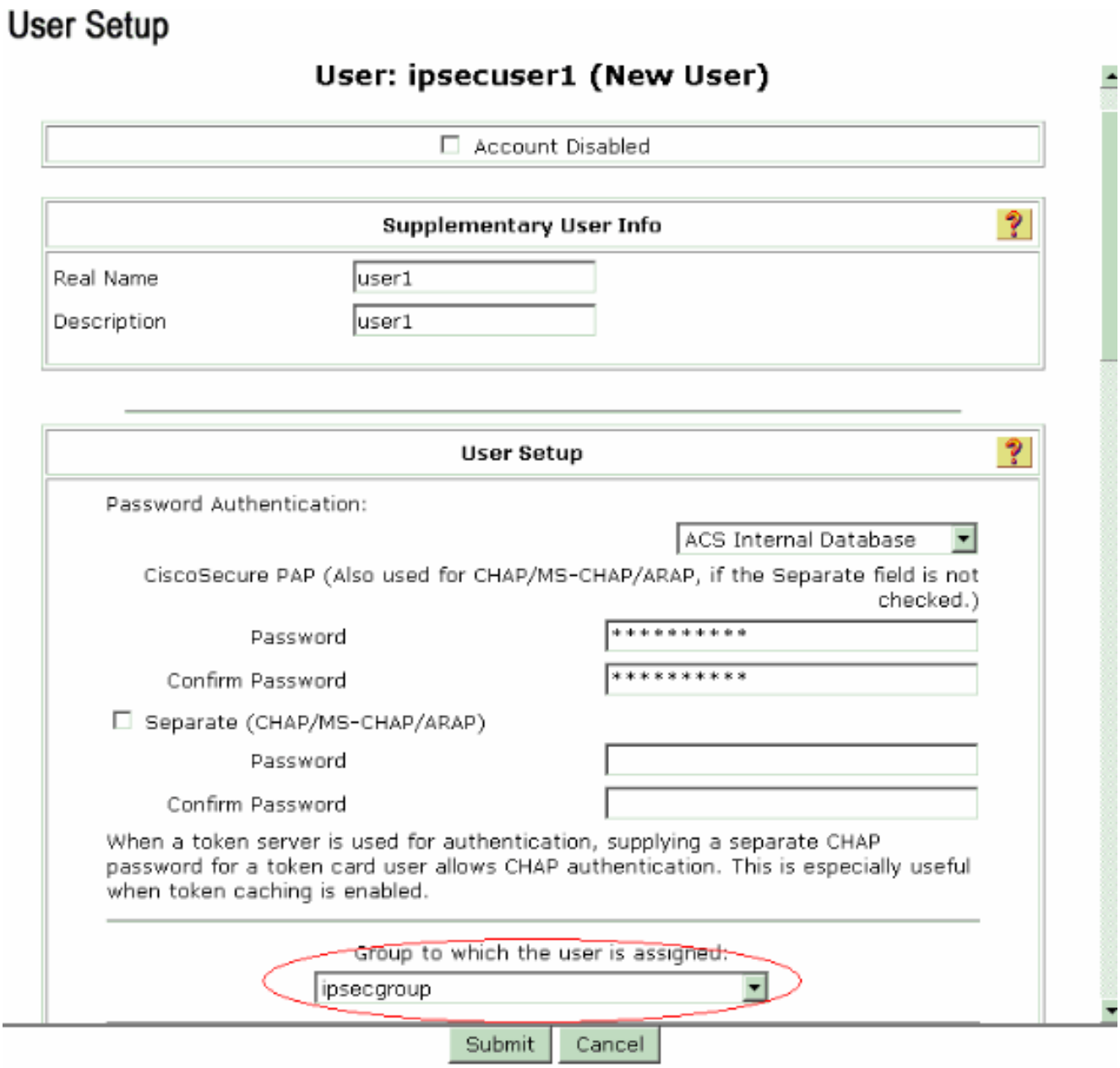


Choisissez **soumettent > reprise** afin de sauvegarder la configuration et lancer le nouveau groupe.Répétez ces étapes afin d'ajouter plus de groupes.

3. **Configurez les utilisateurs sur le Cisco Secure ACS pour Windows.**Choisissez User Setup, écrivez un nom d'utilisateur, et cliquez sur



Add**/l'éditez.** Configu rez ces paramètres sous la section User Setup :

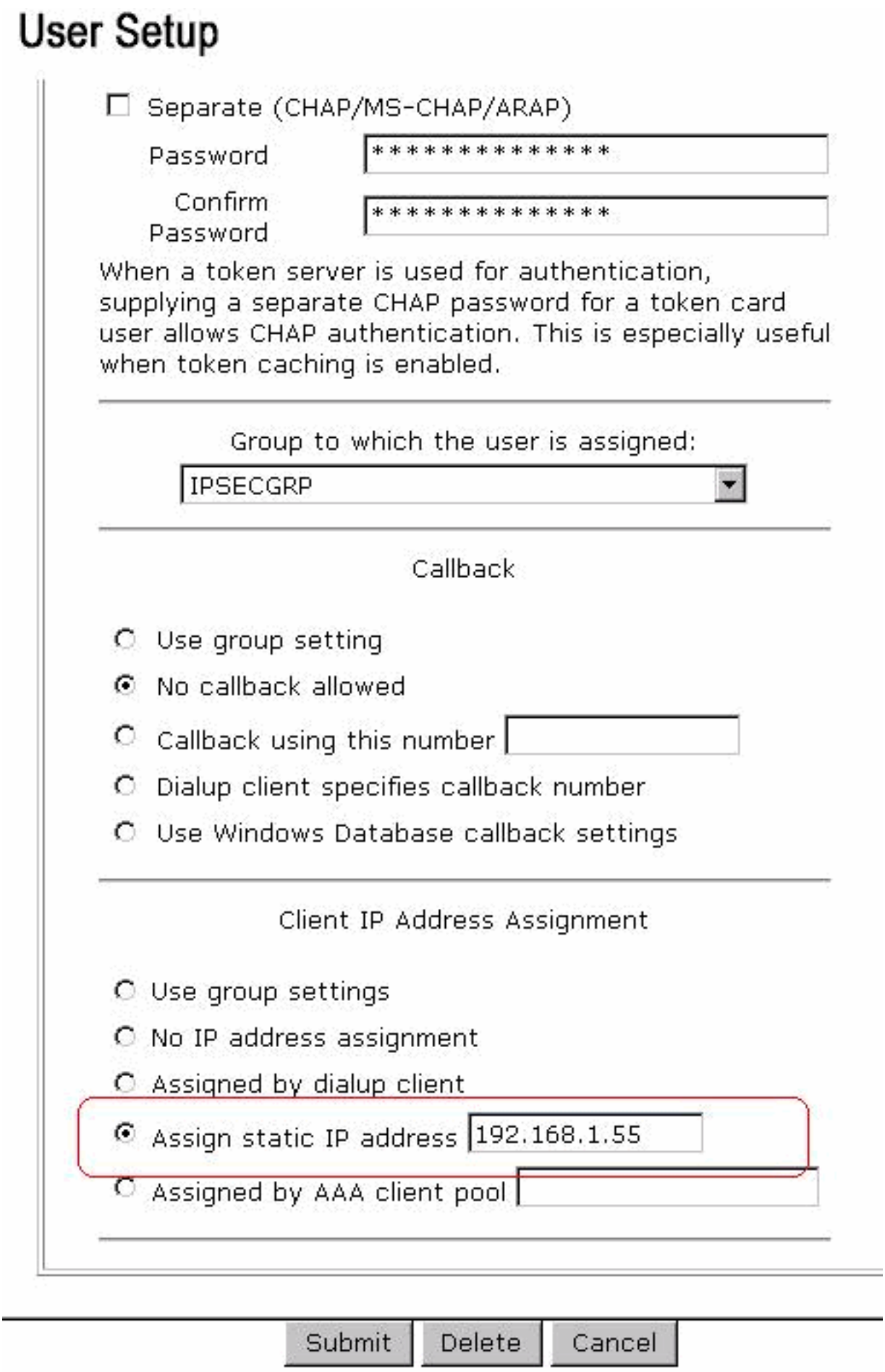


Authentification de mot de passe — Choisissez les **ACS Internal Database**.**PAP Cisco Secure - Mot de passe** — Entrez un mot de passe pour l'utilisateur.**PAP Cisco Secure - Confirmation du mot de passe** — Ressaisissez le mot de passe pour le nouvel utilisateur.**Le groupe auquel l'utilisateur est assigné** — sélectionnez le nom du groupe que vous avez créé dans l'étape précédente.Cliquez sur Submit afin de sauvegarder et lancer les paramètres utilisateurs.Répétez ces étapes afin d'ajouter des utilisateurs supplémentaires.

Assignez une adresse IP statique à l'utilisateur de client vpn

Procédez comme suit :

1. Créez un nouveau groupe VPN IPSECGRP.
2. Créez un utilisateur qui veut recevoir l'IP statique et choisir **IPSECGRP**. Choisissez **assignent l'adresse IP statique** avec l'adresse IP statique qui est assignée sous l'affectation d'adresse IP de

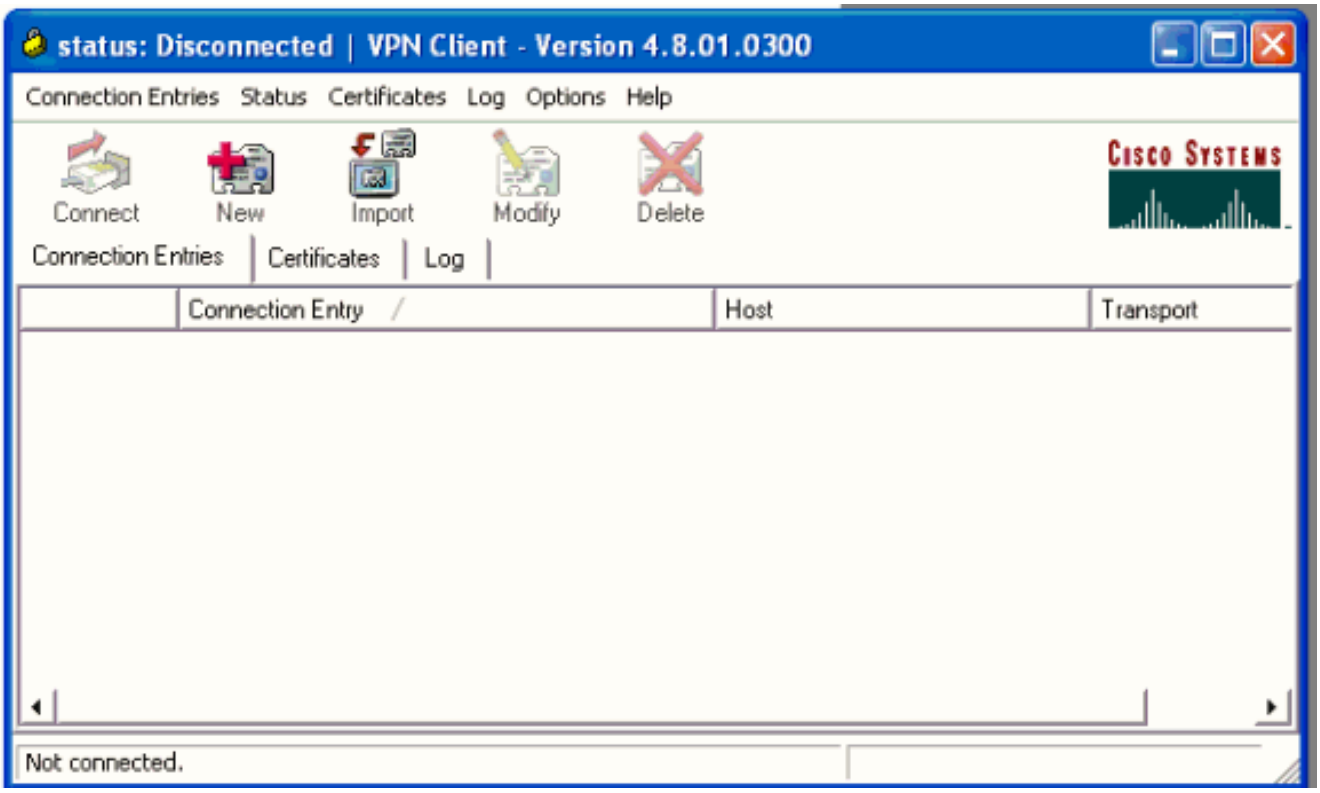


client.

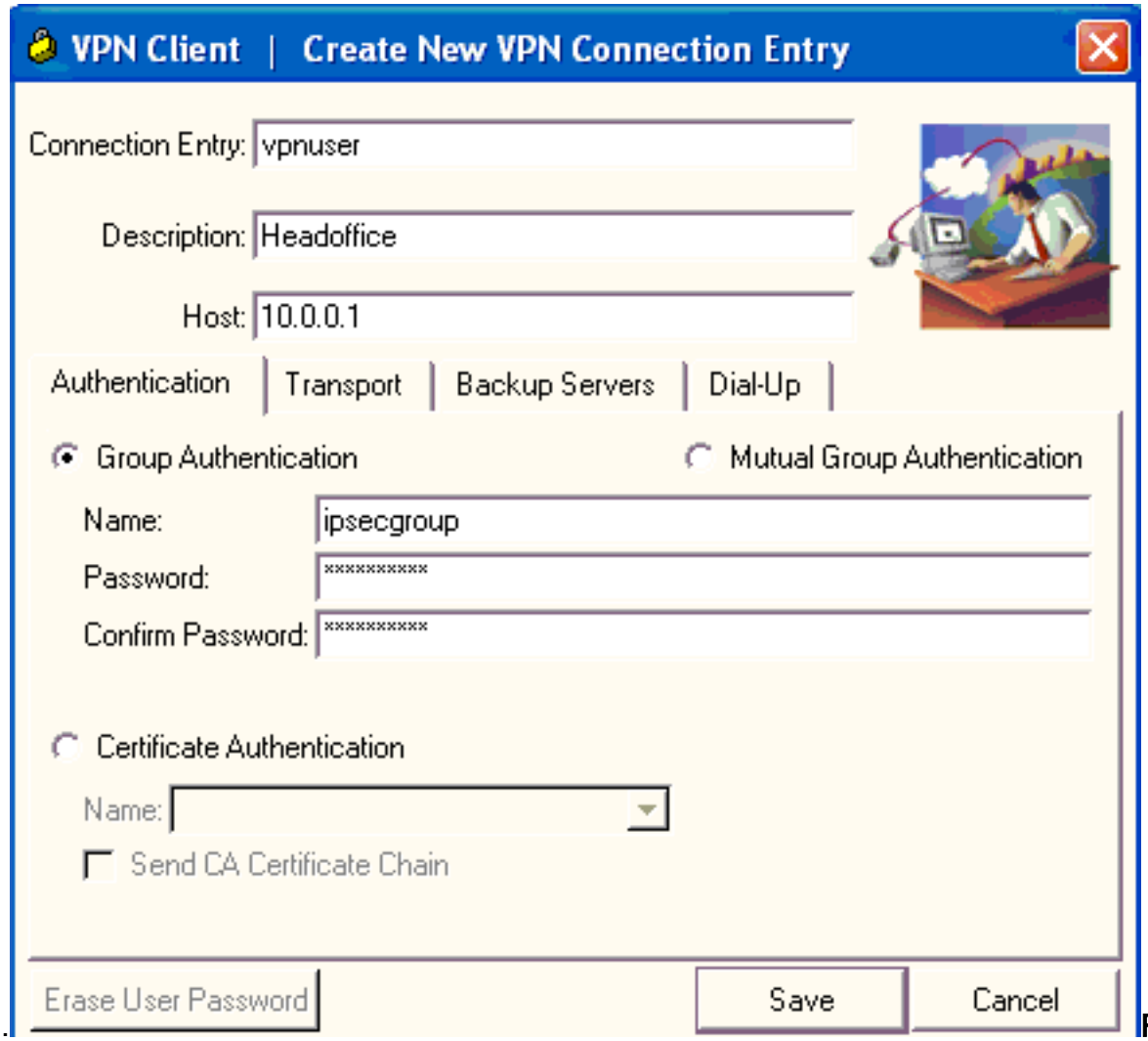
[Configuration de client vpn]

Cette section décrit la configuration de côté de client vpn.

1. Choisissez le **début > les programmes > le client vpn de Cisco Systems > le client vpn**.
2. Cliquez sur New afin de lancer la nouvelle fenêtre d'entrée de connexion VPN de création.



3. Une fois incité, assignez un nom à votre entrée. Vous pouvez également écrire une description si vous souhaitez. Spécifiez l'adresse IP d'interface publique de concentrateur VPN 3000 dans la colonne d'hôte et choisissez l'**authentification de groupe**. Fournissez alors le nom et le mot de passe de groupe. **Sauvegarde de** clic afin de se terminer la nouvelle entrée de connexion

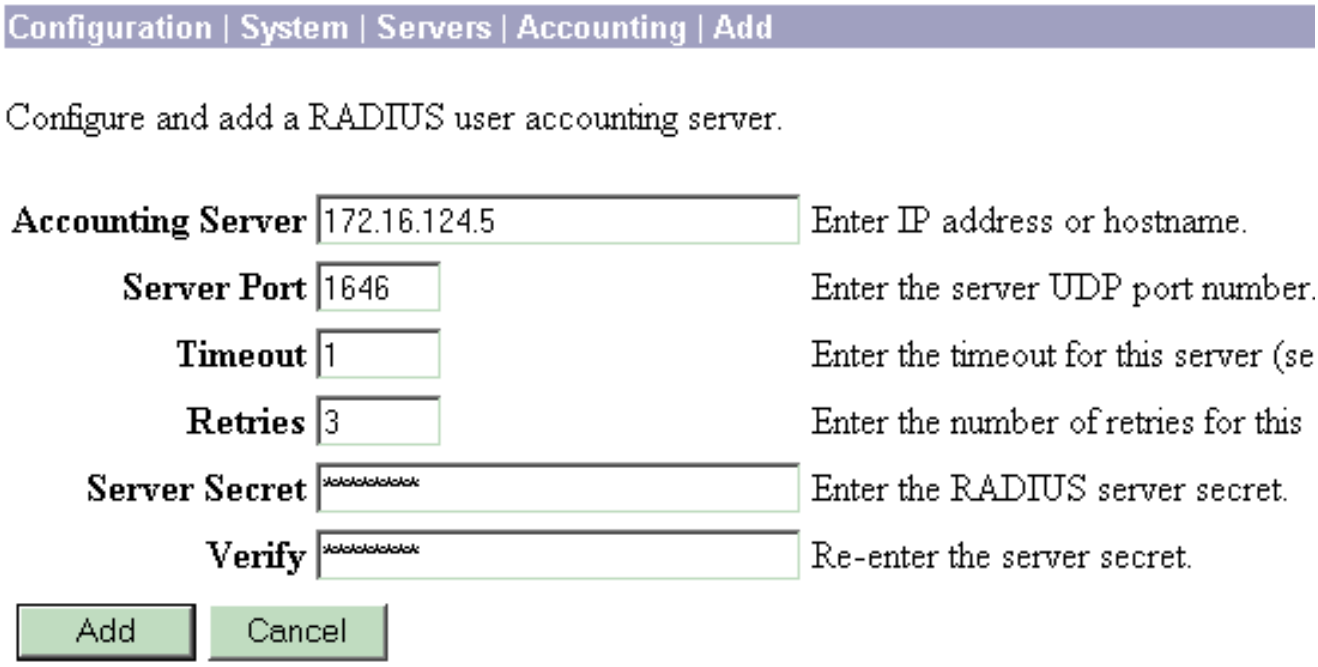


VPN. **Remarque:** Soyez sûr que le client VPN est configuré utiliser le mêmes nom et mot de passe configuré de groupe dans le Concentrateur de la série Cisco VPN 3000.

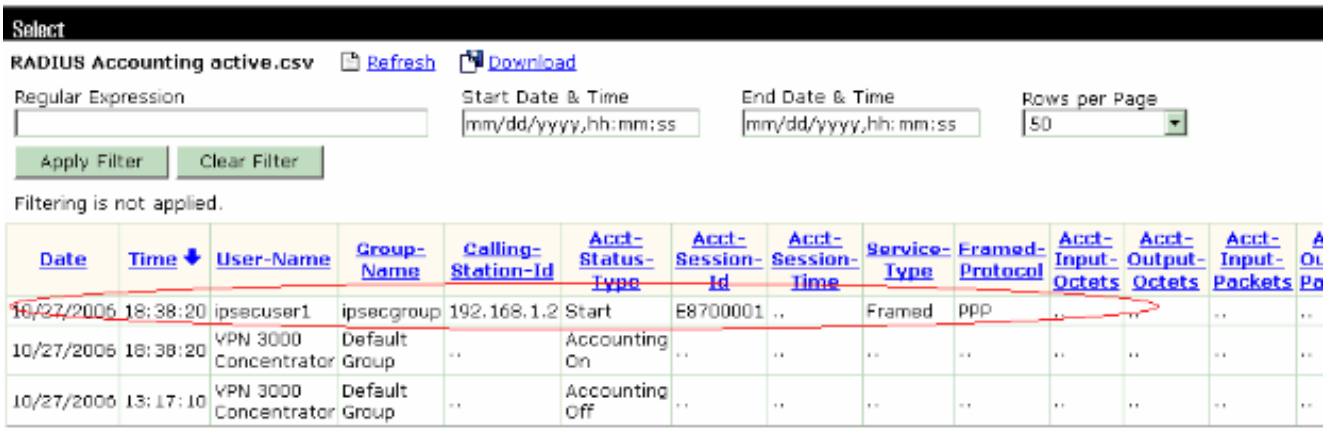
Ajoutez la gestion des comptes

Après l'authentification fonctionne, vous pouvez ajouter la comptabilité.

1. Sur le VPN 3000, choisissez la **configuration > le système > les serveurs > les serveurs de comptabilité**, et ajoutez le **Cisco Secure ACS pour des Windows Server**.
2. Vous pouvez ajouter des serveurs de comptabilité individuelle à chaque groupe quand vous choisissez le **Configuration > User Management > Groups**, mettez en valeur un groupe et le clic **modifient Acct. Serveurs**. Écrivez alors l'adresse IP du serveur de comptabilité avec le secret de
serveur.



Dans le Cisco Secure ACS pour Windows, les enregistrements des comptes apparaissent pendant que cette sortie affiche
:



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Vérifiez le concentrateur VPN

Du côté de concentrateur VPN 3000, choisissez la **gestion > gèrent des sessions** afin de vérifier l'établissement distant de tunnel VPN.

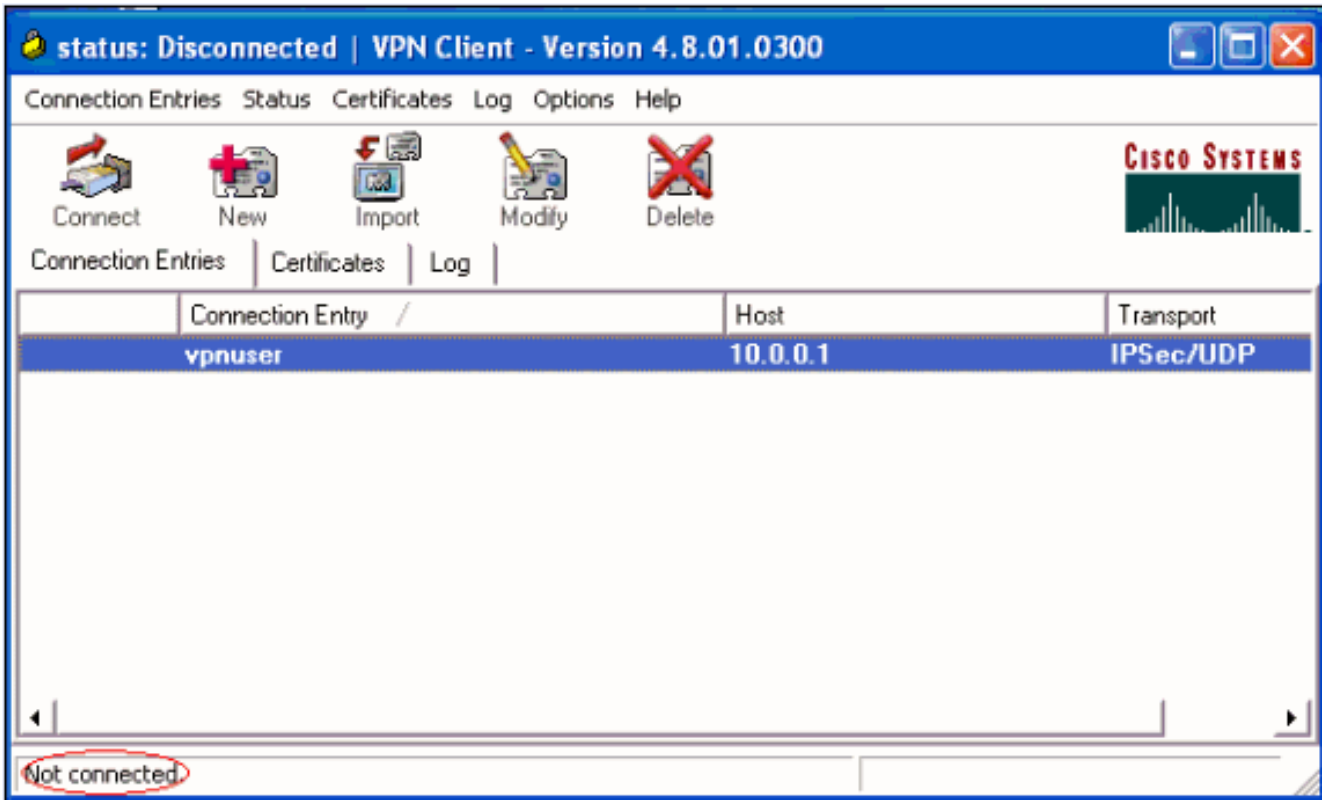
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout | Ping]

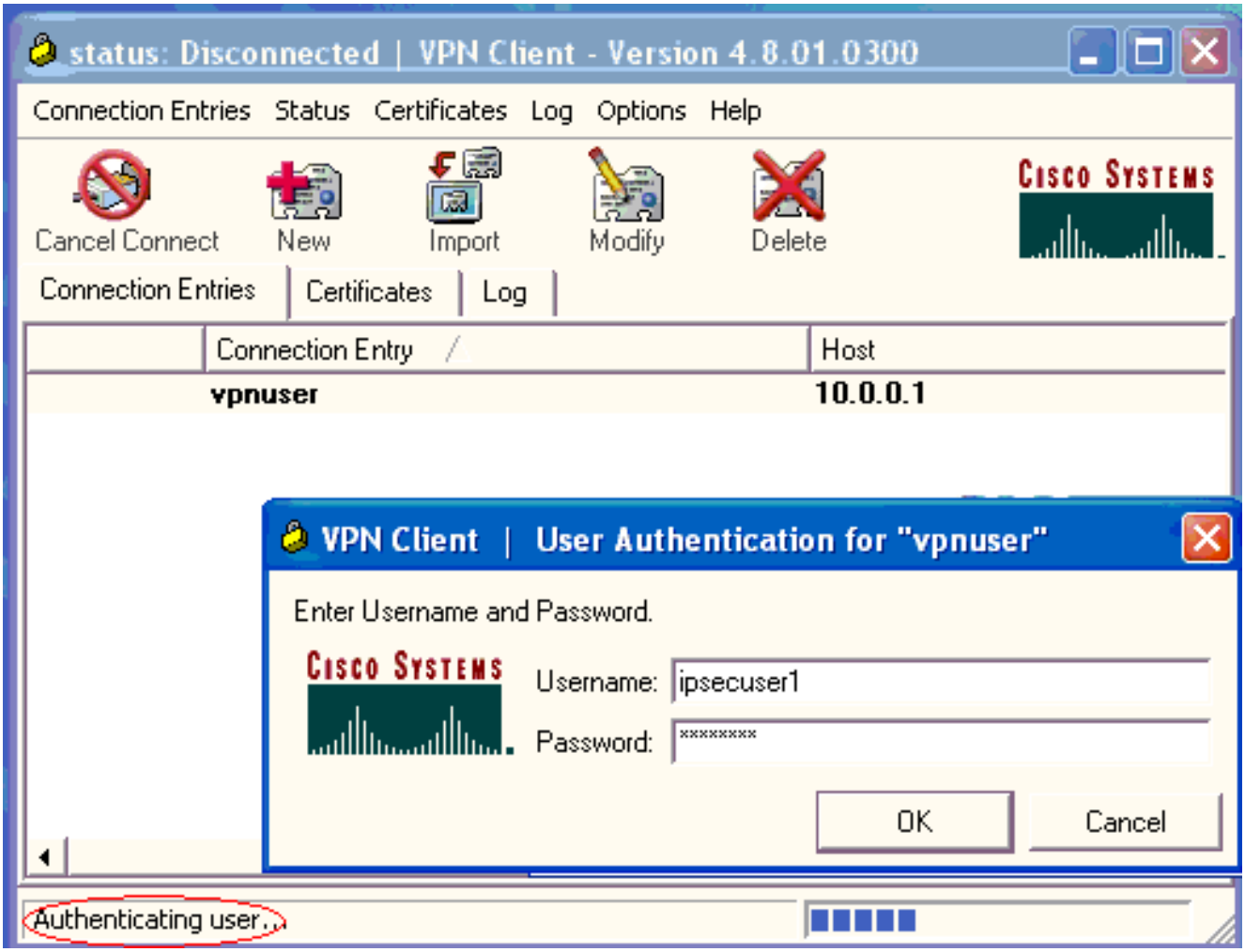
Vérifiez le client vpn

Terminez-vous ces étapes afin de vérifier le client vpn.

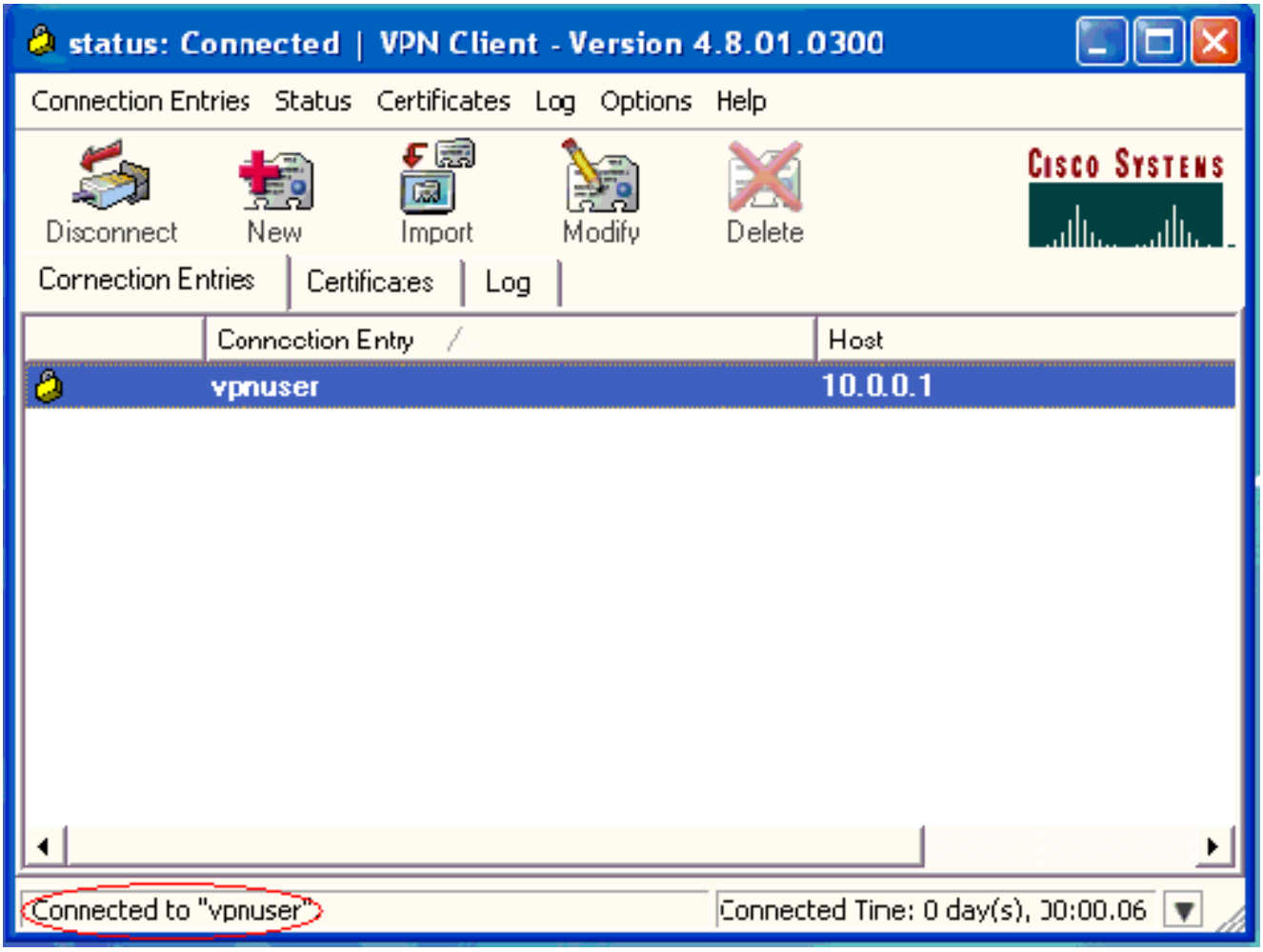
1. Le clic **se connectent** afin d'initier une connexion VPN.



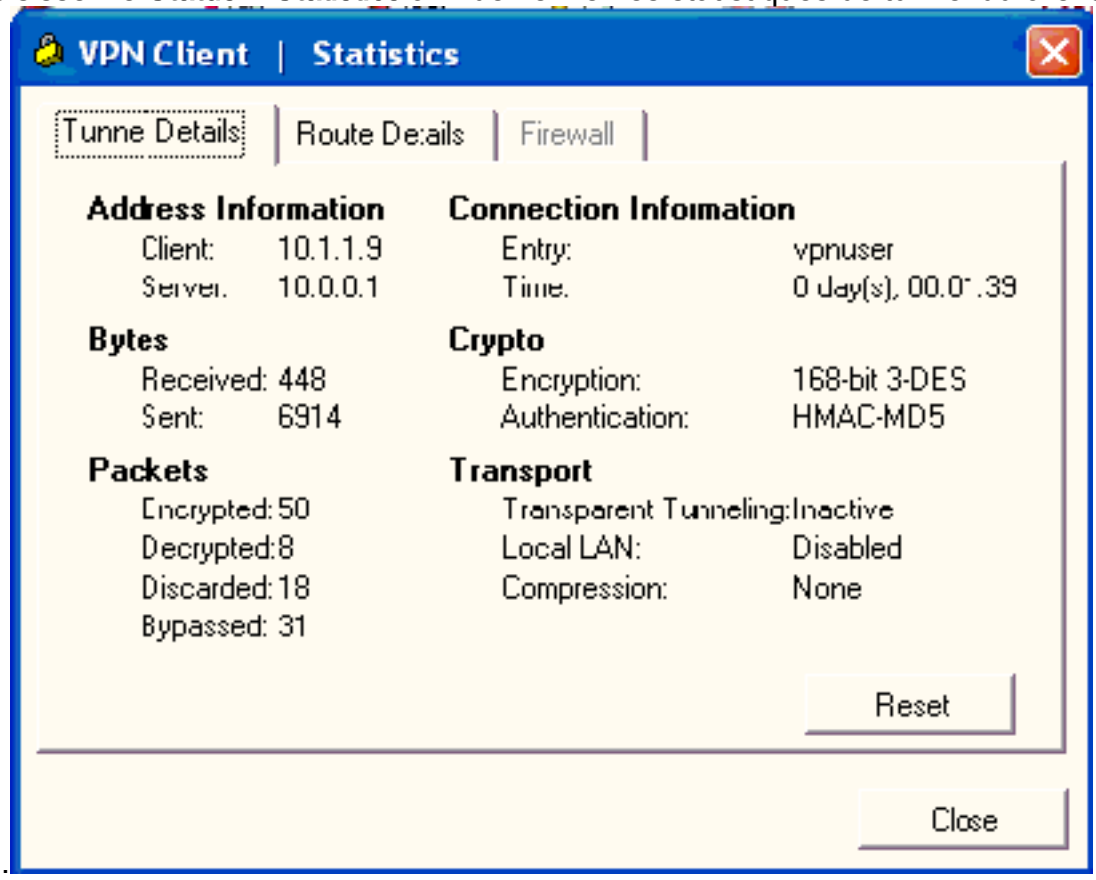
2. Cette fenêtre apparaît pour l'authentification de l'utilisateur. Entrez un nom d'utilisateur valide et un mot de passe afin d'établir la connexion VPN.



3. Le client vpn obtient lié au concentrateur VPN 3000 au lieu d'exploitation principal.



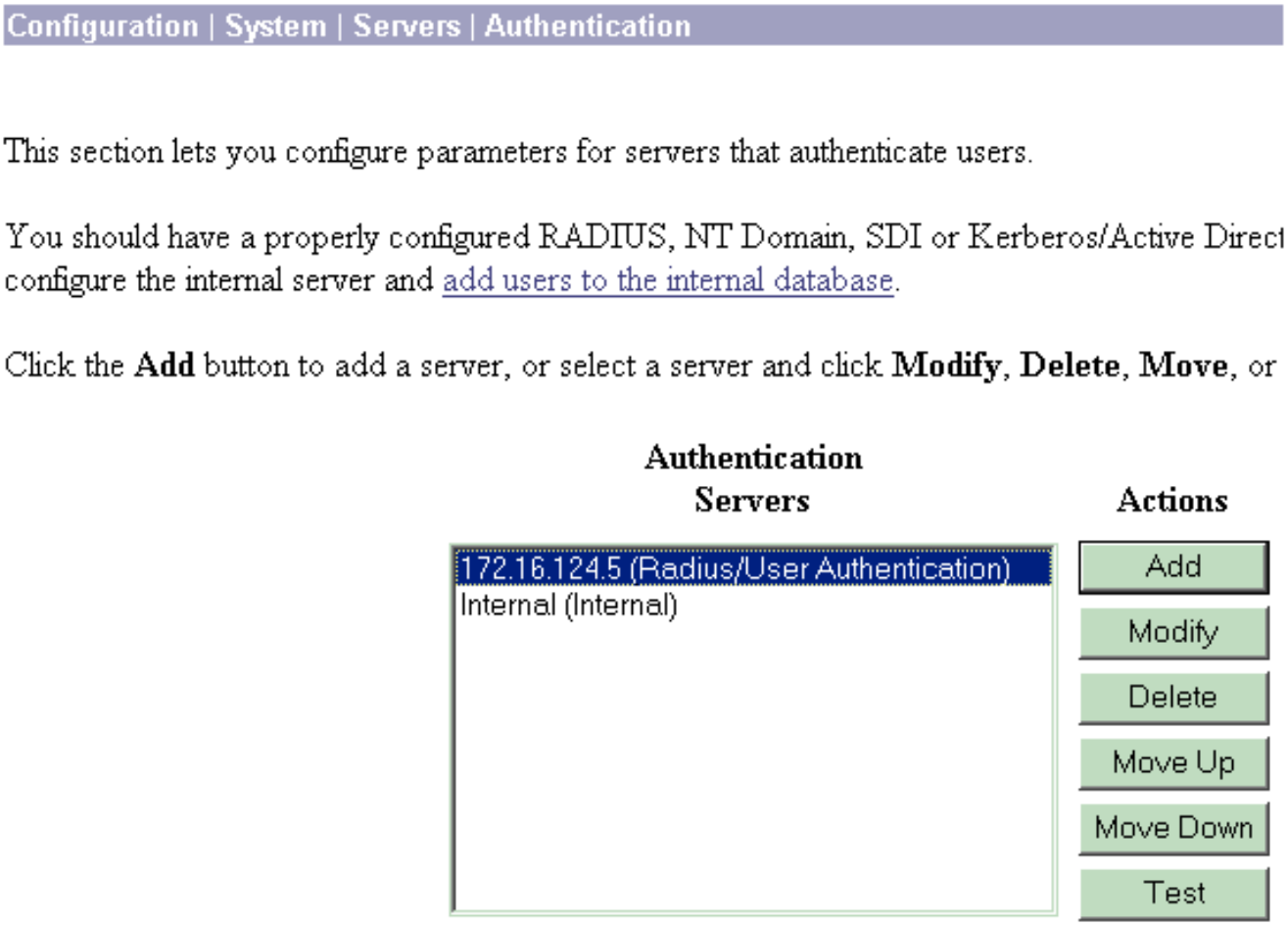
4. Choisissez le **Status > Statistics** afin de vérifier les statistiques de tunnel du client vpn.



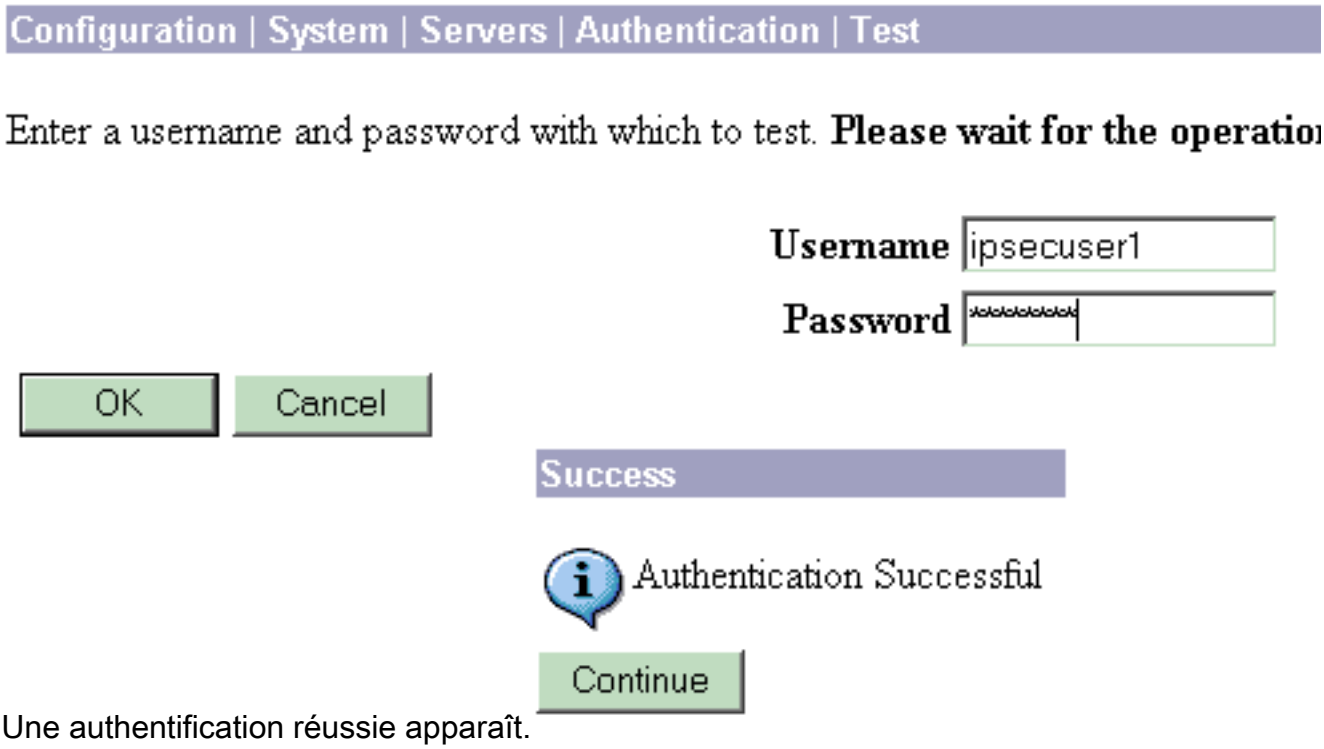
Dépannez

Complétez ces étapes afin de dépanner votre configuration.

1. Choisissez la **configuration > le système > les serveurs > l'authentification** et terminez-vous ces étapes afin de tester la Connectivité entre le serveur de RAYON et le concentrateur VPN 3000.Sélectionnez votre serveur, et puis cliquez sur le **test**.

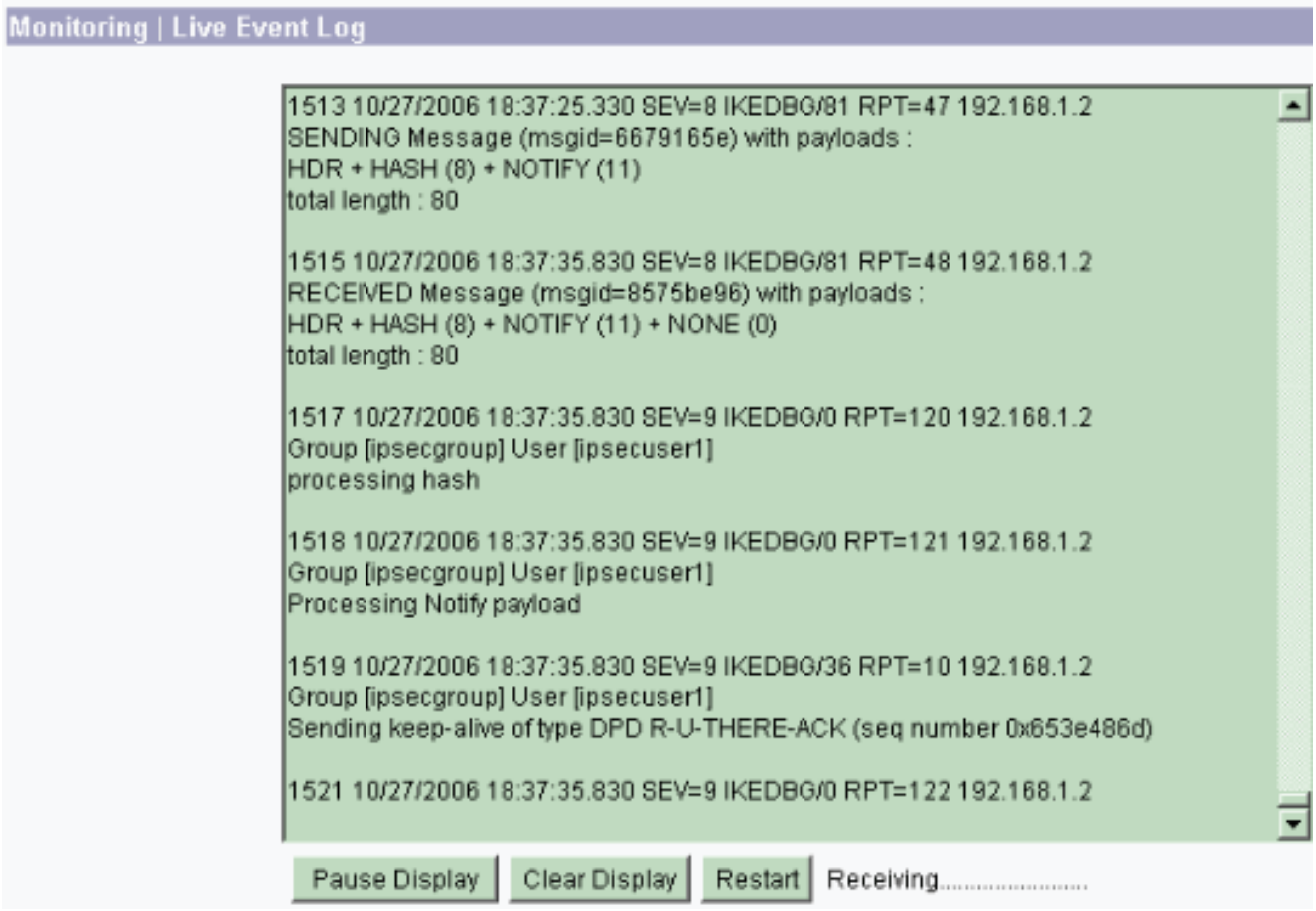


Entrez le nom d'utilisateur RADIUS et le mot de passe et cliquez sur OK.



Une authentification réussie apparaît.

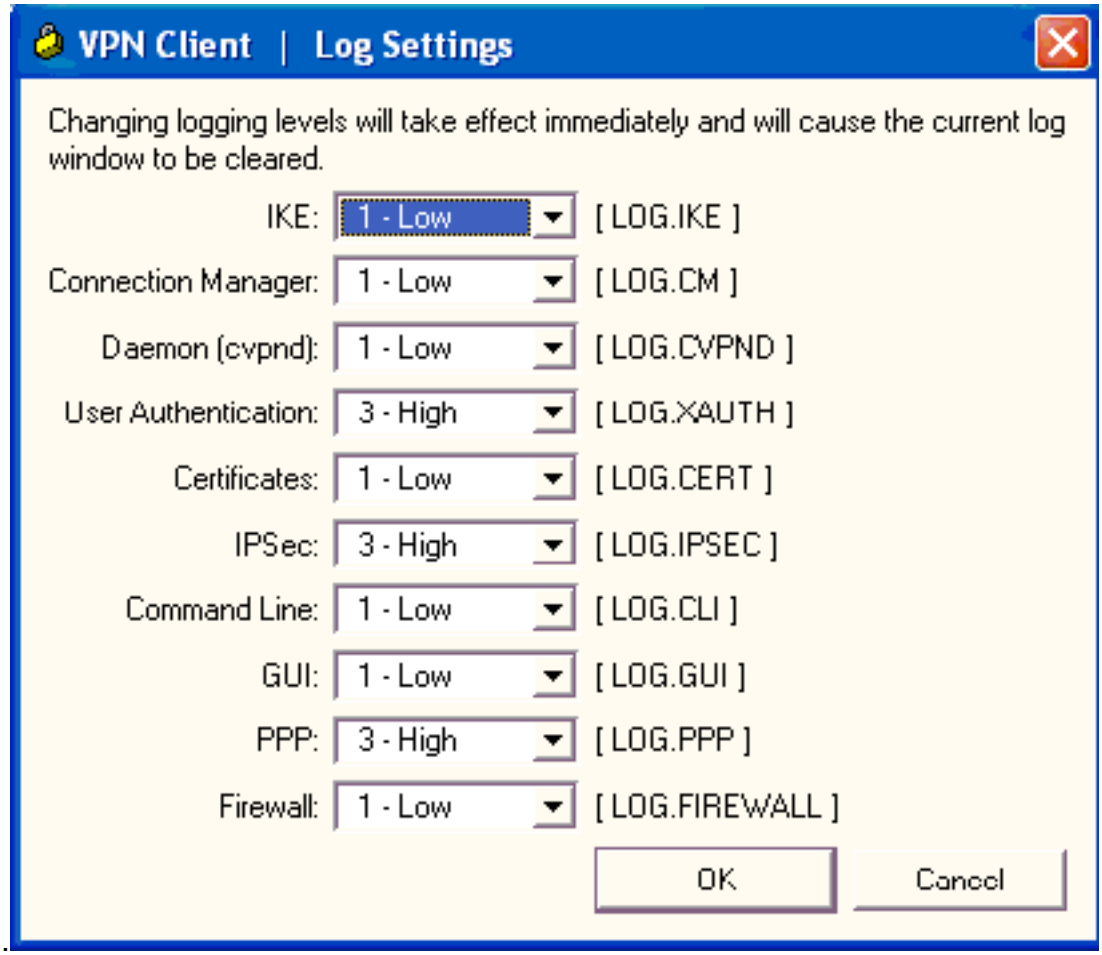
2. S'il échoue, il y a un problème de configuration ou un problème de connectivité IP. Vérifiez le login d'essais ratés le serveur ACS pour des messages liés à la panne.Si message n'apparaît pas dans ce log puis il y a probablement un problème de connectivité IP. La demande RADIUS n'atteint pas le serveur de RAYON. Vérifiez les filtres appliqués à l'interface appropriée de concentrateur VPN 3000 permet 1645) paquets de RAYON (dedans et.Si le test d'authentification est réussi, mais les procédures de connexion au concentrateur VPN 3000 continuent à échouer, vérifiez le journal d'événements filtrables par l'intermédiaire du port de console.Si les connexions ne fonctionnent pas, vous pouvez ajouter AUTHENTIQUE, IKE, et les classes d'événement d'IPsec au concentrateur VPN quand vous sélectionnez la **configuration > le système > les événements > les classes > modifient (sévérité à Log=1-9, sévérité à Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG, et IPSECDECODE sont également disponibles, mais peut fournir trop d'informations. Si les informations détaillées sont nécessaires sur les attributs qui sont passés vers le bas du serveur de RAYON, AUTHDECODE, IKEDECODE, et IPSECDECODE fournissent ceci à la sévérité au niveau Log=1-13.
3. Récupérez le journal d'événements de la **surveillance > du journal d'événements**.



Dépannez le client vpn 4.8 pour Windows

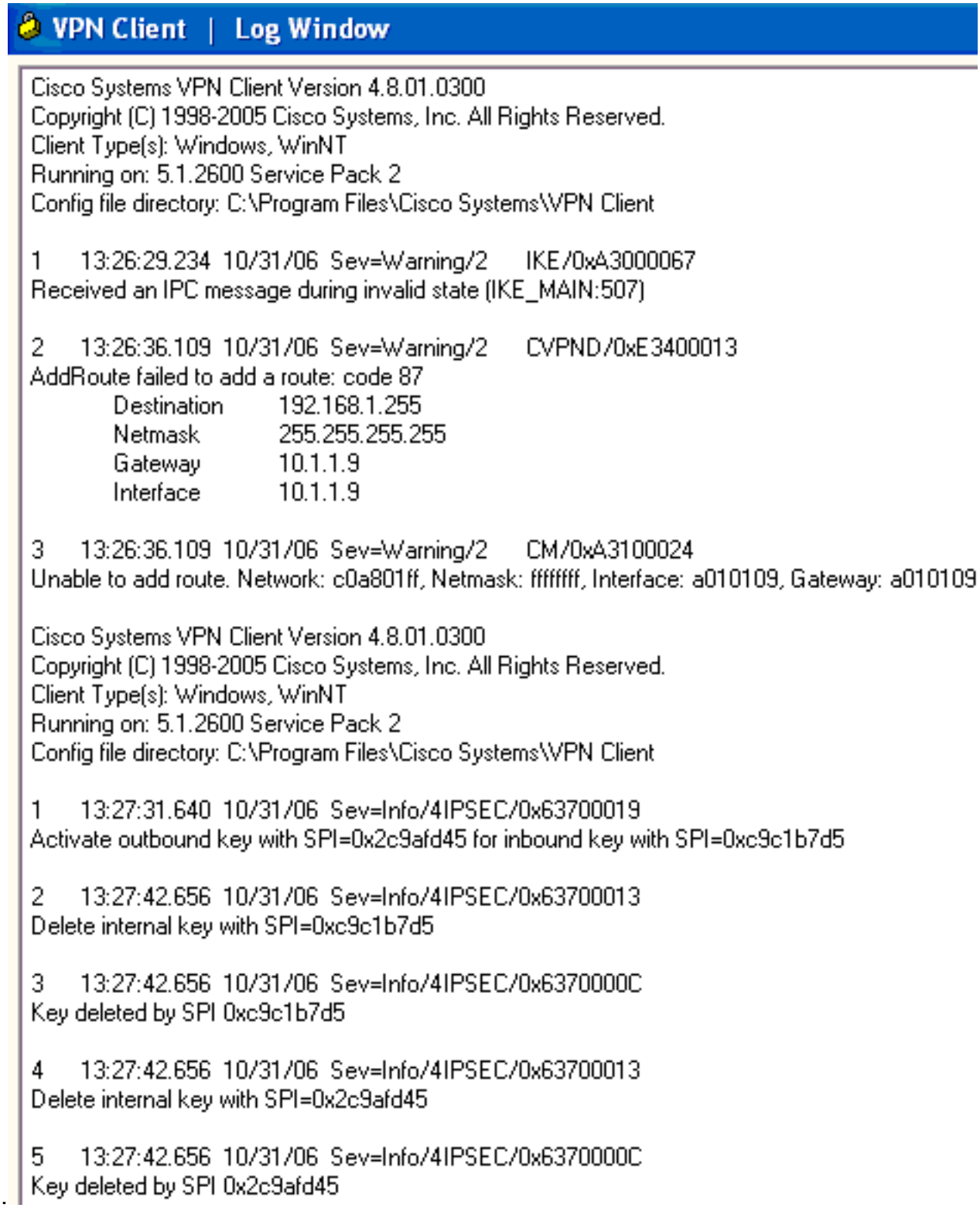
Terminez-vous ces étapes afin de dépanner le client vpn 4.8 pour Windows.

1. Choisissez le **Log > Log settings** afin d'activer les niveaux de log dans le client



vpn.

2. Choisissez le **Log > Log Window** afin de visualiser les entrées de journal dans le client



vpn.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Cisco VPN Client Support Page
- Négociation IPSec/Protocoles IKE
- Cisco Secure ACS pour la page d'assistance de Windows
- Configurer les filtres dynamiques sur un serveur de RAYON
- Support et documentation techniques - Cisco Systems