

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](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Utiliser des groupes sur le concentrateur VPN 3000](#)

[Utilisation des attributs de groupe et d'utilisateur par le concentrateur VPN 3000](#)

[Configuration du concentrateur de la gamme VPN 3000](#)

[Configuration du serveur RADIUS](#)

[Attribuer une adresse IP statique à l'utilisateur du client VPN](#)

[Configuration du client VPN](#)

[Ajoutez la gestion des comptes](#)

[Vérification](#)

[Vérifier le concentrateur VPN](#)

[Vérifier le client VPN](#)

[Dépannage](#)

[Dépannage du client VPN 4.8 pour Windows](#)

[Informations connexes](#)

[Introduction](#)

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

Référez-vous à [Exemple de configuration d'authentification RADIUS PIX/ASA 7.x et Cisco VPN Client 4.x pour Windows avec Microsoft Windows 2003 IAS](#) afin de configurer la connexion VPN d'accès à distance entre un client VPN Cisco (4.x pour Windows) et le dispositif de sécurité de la gamme PIX 500 7.x qui utilise un serveur RADIUS Microsoft Windows 2003.

Référez-vous à [Configuration d'IPsec entre un routeur Cisco IOS et un client VPN Cisco 4.x pour Windows utilisant RADIUS pour l'authentification utilisateur](#) afin de configurer une connexion entre un routeur et le client VPN Cisco 4.x qui utilise RADIUS pour l'authentification utilisateur.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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 gamme Cisco VPN 3000 avec fichier image 4.7.2.B
- Client VPN Cisco 4.x

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.

Conventions

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

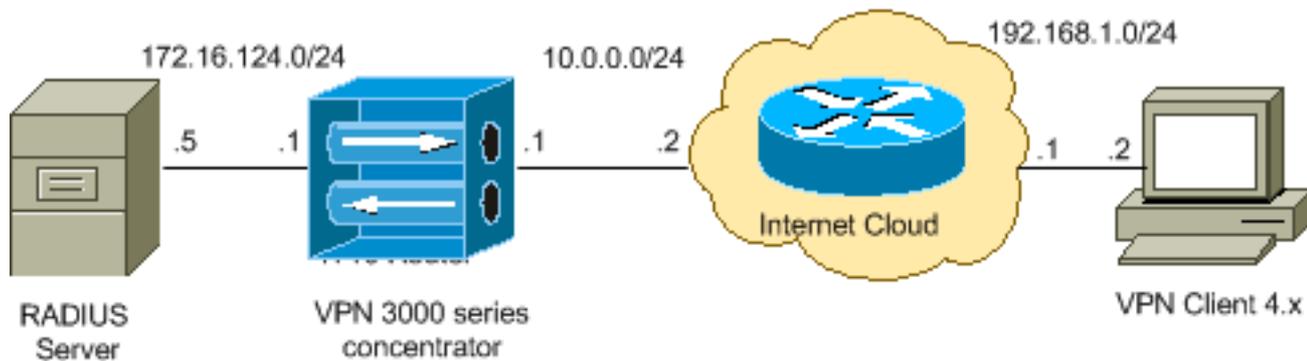
Configuration

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

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) 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 IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses [RFC 1918 qui ont été utilisés dans un environnement de laboratoire.](#)

Utiliser des groupes sur le concentrateur VPN 3000

Les groupes peuvent être définis à la fois pour Cisco Secure ACS pour Windows et le concentrateur VPN 3000, mais ils utilisent des groupes légèrement différents. Effectuez ces tâches afin de simplifier les choses :

- **Configurez un groupe unique sur le concentrateur VPN 3000** pour lorsque vous établissez le tunnel initial. Il s'agit souvent du groupe de tunnels et il est utilisé pour établir une session Internet Key Exchange (IKE) cryptée vers le concentrateur VPN 3000 à l'aide d'une clé pré-partagée (le mot de passe du groupe). Il s'agit du même nom de groupe et du même mot de passe qui doivent être configurés sur tous les clients VPN Cisco qui veulent se connecter au concentrateur VPN.
- **Configurez des groupes sur le serveur Cisco Secure ACS pour Windows** qui utilisent des attributs RADIUS standard et des attributs spécifiques au fournisseur (VSA) pour la gestion des stratégies. Les VSA qui doivent être utilisées avec le concentrateur VPN 3000 sont les attributs RADIUS (VPN 3000).
- **Configurez les utilisateurs sur le serveur Cisco Secure ACS pour Windows RADIUS et attribuez-les à l'un des groupes** configurés sur le même serveur. Les utilisateurs héritent des attributs définis pour leur groupe et Cisco Secure ACS pour Windows envoie ces attributs au concentrateur VPN lorsque l'utilisateur est authentifié.

Utilisation des attributs de groupe et d'utilisateur par le concentrateur VPN 3000

Une fois que le concentrateur VPN 3000 a authentifié le groupe de tunnels avec le concentrateur VPN et l'utilisateur avec RADIUS, il doit organiser les attributs qu'il a reçus. Le concentrateur VPN utilise les attributs dans cet ordre de préférence, que l'authentification soit effectuée dans le concentrateur VPN ou avec RADIUS :

1. **Attributs utilisateur** : ces attributs ont toujours la priorité sur les autres.
2. **Attributs du groupe de tunnels** - Tous les attributs non retournés lorsque l'utilisateur a été authentifié sont remplis par les attributs du groupe de tunnels.
3. **Attributs du groupe de base** - Tous les attributs manquants des attributs utilisateur ou groupe de tunnels sont remplis par les attributs du groupe de base du concentrateur VPN.

Configuration du concentrateur de la gamme VPN 3000

Suivez la procédure décrite dans cette section afin de configurer un concentrateur VPN Cisco 3000 pour les paramètres requis pour la connexion IPsec ainsi que le client AAA pour que l'utilisateur VPN s'authentifie auprès du serveur RADIUS.

Dans ce paramètre de travaux pratiques, le concentrateur VPN est d'abord accessible via le port de console et une configuration minimale est ajoutée comme le montre le résultat suivant :

```
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 Configuration rapide et ces éléments sont configurés.

- Heure/Date
- Interfaces/masques dans **Configuration > Interfaces** (public=10.0.0.1/24, private=172.16.124.1/24)
- Passerelle par défaut dans **Configuration > System > IP routing > Default_Gateway** (10.0.0.2)

À ce stade, le concentrateur VPN est accessible via HTML depuis le réseau interne.

Remarque : si le concentrateur VPN est géré de l'extérieur, vous devez également effectuer les étapes suivantes :

1. Choisissez **Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Privé** (par défaut).

2. Choisissez **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation** afin d'ajouter l'adresse IP du gestionnaire externe.

Ces étapes ne sont requises que si vous gérez le concentrateur VPN depuis l'extérieur.

Une fois ces deux étapes terminées, le reste de la configuration peut être effectué via l'interface utilisateur graphique en utilisant un navigateur Web et en se connectant à l'adresse IP de l'interface que vous venez de configurer. Dans cet exemple et à ce stade, le concentrateur VPN est accessible via HTML à partir du réseau interne :

1. Choisissez **Configuration > Interfaces** afin de vérifier les interfaces après avoir activé l'interface utilisateur graphique.

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	172.16.124.1	255.255.255.0	00.03.A0.89.BF.D0	
Ethernet 2 (Public)	UP	10.0.0.1	255.255.255.0	00.03.A0.89.BF.D1	10.0.0.2
Ethernet 3 (External)	Not Configured	0.0.0.0	0.0.0.0		
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

2. Complétez ces étapes afin d'ajouter le serveur Cisco Secure ACS pour Windows RADIUS à la configuration du concentrateur VPN 3000. Choisissez **Configuration > System > Servers > Authentication**, puis cliquez sur **Add** dans le menu de gauche.

Configure and add a user authentication server.

Server Type:

Authentication Server: Enter IP address or hostname.

Used For: Select the operation(s) for which this RADIUS se

Server Port: Enter 0 for default port (1645).

Timeout: Enter the timeout for this server (seconds).

Retries: Enter the number of retries for this server.

Server Secret: Enter the RADIUS server secret.

Verify: Re-enter the secret.

Choisissez le type de serveur **RADIUS** et ajoutez ces paramètres pour votre serveur Cisco

Secure ACS pour Windows RADIUS. Laissez tous les autres paramètres dans leur état par défaut. **Authentication Server** : saisissez l'adresse IP de votre serveur Cisco Secure ACS pour Windows RADIUS. **Server Secret** : saisissez le secret du serveur RADIUS. Ce doit être le même secret que celui que vous utilisez lorsque vous configurez le concentrateur VPN 3000 dans la configuration de Cisco Secure ACS pour Windows. **Verify** : saisissez à nouveau le mot de passe pour vérification. Ceci ajoute le serveur d'authentification dans la configuration globale du concentrateur VPN 3000. Ce serveur est utilisé par tous les groupes sauf lorsqu'un serveur d'authentification a été spécifiquement défini. Si un serveur d'authentification n'est pas configuré pour un groupe, il revient au serveur d'authentification global.

3. Complétez ces étapes afin de configurer le groupe de tunnels sur le concentrateur VPN 3000. Choisissez **Configuration > User Management > Groups** dans le menu de gauche et cliquez sur **Add**. Modifiez ou ajoutez ces paramètres dans les onglets Configuration. Ne cliquez pas sur Appliquer tant que vous n'avez pas modifié tous ces paramètres : **Remarque** : ces paramètres sont le minimum requis pour les connexions VPN d'accès à distance. Ces paramètres supposent également que les paramètres par défaut du groupe de base sur le concentrateur VPN 3000 n'ont pas été modifiés. **Identité**

Configuration | User Management | Groups | Add

This section lets you add a group. 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

Identity Parameters

Attribute	Value	Description
Group Name	<input type="text" value="ipsecgroup"/>	Enter a unique name for the group.
Password	<input type="password" value=""/>	Enter the password for the group.
Verify	<input type="password" value=""/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.</i>

Group Name : saisissez un nom de groupe. Par exemple, IPsecUsers. **Password** : saisissez un mot de passe pour le groupe. Il s'agit de la clé pré-partagée pour la session IKE. **Verify** : saisissez à nouveau le mot de passe pour vérification. **Type** : laissez ceci comme valeur par défaut : Interne. **IPsec**

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

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Associat
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identit
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives
Confidence Interval	300	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitte checks to see if it is still connected.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Up needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	RADIUS	<input type="checkbox"/>	Select the authentication method for membe apply to Individual User Authentication .
Authorization Type	None	<input checked="" type="checkbox"/>	If members of this group need authorizatio authorization method. If you configure this f Server.

Tunnel Type : choisissez **Remote-Access**. **Authentication** : RADIUS. Cela indique au concentrateur VPN quelle méthode utiliser pour authentifier les utilisateurs. **Mode Config** : cochez **Mode Config**. Cliquez sur Apply.

- Complétez ces étapes afin de configurer plusieurs serveurs d'authentification sur le concentrateur VPN 3000. Une fois le groupe défini, mettez-le en surbrillance, puis cliquez sur **Serveurs d'authentification** sous la colonne Modifier. Des serveurs d'authentification individuels peuvent être définis pour chaque groupe même si ces serveurs n'existent pas dans les serveurs globaux.

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 group parameters, select a group and click the appropriate button.

Actions	Current Groups	Modify
<p>Add Group</p> <p>Modify Group</p> <p>Delete Group</p>	<p>ipsecgroup (Internally Configured)</p>	<p>Authentication Servers</p> <p>Authorization Servers</p> <p>Accounting Servers</p> <p>Address Pools</p> <p>Client Update</p> <p>Bandwidth Assignment</p> <p>WebVPN Servers and URLs</p> <p>WebVPN Port Forwarding</p>

Choisissez le type de serveur **RADIUS** et ajoutez ces paramètres pour votre serveur Cisco Secure ACS pour Windows RADIUS. Laissez tous les autres paramètres dans leur état par défaut. **Authentication Server** : saisissez l'adresse IP de votre serveur Cisco Secure ACS pour Windows RADIUS. **Server Secret** : saisissez le secret du serveur RADIUS. Ce doit être le même secret que celui que vous utilisez lorsque vous configurez le concentrateur VPN 3000 dans la configuration de Cisco Secure ACS pour Windows. **Verify** : saisissez à nouveau le mot de passe pour vérification.

5. Choisissez **Configuration > System > Address Management > Assignment** et cochez **Use Address from Authentication Server** afin d'attribuer l'adresse IP aux clients VPN à partir du pool d'adresses IP créé dans le serveur RADIUS une fois le client authentifié.

The screenshot shows the 'Assignment' configuration page in Cisco Secure ACS. The breadcrumb navigation at the top reads 'Configuration | System | Address Management | Assignment'. Below the breadcrumb, a descriptive text states: 'This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.' The configuration options are as follows:

- Use Client Address** Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server** Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP** Check to use DHCP to obtain an IP address for the client.
- Use Address Pools** Check to use internal address pool configuration to obtain an IP address for the client.

Below these options is the **IP Reuse Delay** field, which is a text input box containing the value '0'. To its right, the text reads: 'Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.' At the bottom of the configuration area, there are two buttons: 'Apply' and 'Cancel'.

[Configuration du serveur RADIUS](#)

Cette section du document décrit la procédure requise pour configurer Cisco Secure ACS en tant que serveur RADIUS pour l'authentification des utilisateurs du client VPN transmise par le concentrateur de la gamme Cisco VPN 3000 - client AAA.

Double-cliquez sur l'icône **ACS Admin** afin de démarrer la session admin sur le PC qui exécute le serveur Cisco Secure ACS pour Windows RADIUS. Connectez-vous avec le nom d'utilisateur et le mot de passe appropriés, si nécessaire.

1. Complétez ces étapes afin d'ajouter le concentrateur VPN 3000 à la configuration du serveur Cisco Secure ACS pour Windows. Choisissez **Network Configuration** et cliquez sur **Add Entry** afin d'ajouter un client AAA au serveur RADIUS.



Network Configuration

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
nm-wlc	192.168.11.24	RADIUS (Cisco Aironet)
WLC	172.16.1.30	RADIUS (Cisco Airespace)

Add Entry

Search

Ajoutez ces paramètres à votre concentrateur VPN 3000

:

Network Configuration

Edit

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Key

Authenticate Using

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port info with Username from this AAA Client

Submit

Submit + Apply

Cancel

AAA Client Hostname : saisissez le nom d'hôte de votre concentrateur VPN 3000 (pour la résolution DNS).**AAA Client IP Address** : saisissez l'adresse IP de votre concentrateur VPN 3000.**Key** : saisissez le secret du serveur RADIUS. Il doit s'agir du même secret que celui que vous avez configuré lorsque vous avez ajouté le serveur d'authentification sur le concentrateur VPN.**Authenticate Using** : choisissez **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**. Cela permet aux VSA VPN 3000 de s'afficher dans la fenêtre de configuration du

groupe. Cliquez sur Submit. Choisissez **Interface Configuration**, cliquez sur **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** et cochez **Group [26] Vendor-Specific**.

Interface Configuration

Edit

RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

User Group

- [026/3076/001] Access-Hours
- [026/3076/002] Simultaneous-Logins
- [026/3076/005] Primary-DNS
- [026/3076/006] Secondary-DNS
- [026/3076/007] Primary-WINS
- [026/3076/008] Secondary-WINS
- [026/3076/009] SEP-Card-Assignment
- [026/3076/011] Tunneling-Protocols
- [026/3076/012] IPSec-Sec-Association
- [026/3076/013] IPSec-Authentication
- [026/3076/015] IPSec-Banner1
- [026/3076/016] IPSec-Allow-Passwd-Store

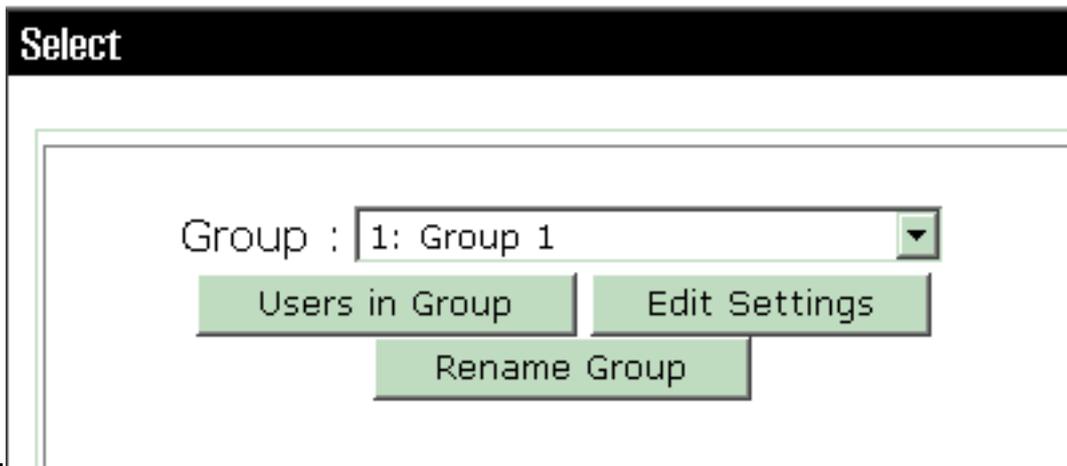
Submit

Cancel

Remarque : 'attribut RADIUS 26' fait référence à tous les attributs spécifiques au fournisseur. Par exemple, choisissez **Interface Configuration > RADIUS (Cisco VPN 3000)** et voyez que tous les attributs disponibles commencent par 026. Cela montre que tous ces attributs spécifiques au fournisseur sont conformes à la norme IETF RADIUS 26. Ces attributs ne s'affichent pas par défaut dans la configuration de l'utilisateur ou du groupe. Afin d'apparaître dans la configuration du groupe, créez un client AAA (dans ce cas, un concentrateur VPN 3000) qui s'authentifie avec RADIUS dans la configuration réseau. Vérifiez ensuite les attributs qui doivent apparaître dans Configuration utilisateur, Configuration de groupe ou les deux dans la configuration de l'interface. Référez-vous à [Attributs RADIUS](#) pour plus d'informations sur les attributs disponibles et leur utilisation. Cliquez sur Submit.

2. Complétez ces étapes afin d'ajouter des groupes à la configuration Cisco Secure ACS pour Windows. Choisissez **Configuration du groupe**, puis sélectionnez l'un des groupes de modèles, par exemple Groupe 1, et cliquez sur **Renommer le**

Group Setup



groupe.

Rempl

acez le nom par un nom approprié pour votre organisation. Par exemple, ipsecgroup. Puisque les utilisateurs sont ajoutés à ces groupes, faites en sorte que le nom du groupe reflète l'objectif réel de ce groupe. Si tous les utilisateurs sont placés dans le même groupe, vous pouvez l'appeler Groupe d'utilisateurs VPN. Cliquez sur **Modifier les paramètres** afin de modifier les paramètres de votre nouveau groupe

Group Setup

Jump To

Group Settings : ipsecgroup

Access Restrictions

Group Disabled 

Members of this group will be denied access to the network.

Callback 

No callback allowed
 Dialup client specifies callback number
 Use Windows Database callback settings (where possible)

renommé.

Cliquez sur **Cisco VPN 3000 RADIUS** et configurez ces attributs recommandés. Cela permet aux utilisateurs affectés à ce groupe d'hériter des attributs RADIUS Cisco VPN 3000, ce qui vous permet de centraliser les stratégies pour tous les utilisateurs de Cisco Secure ACS pour

Group Setup

Jump To

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes 

[3076\001] Access-Hours

[3076\002] Simultaneous-Logins

[3076\005] Primary-DNS

[3076\006] Secondary-DNS

[3076\007] Primary-WINS

[3076\008] Secondary-WINS

[3076\009] SEP-Card-Assignment

Windows.

Re

marque : Techniquement, les attributs RADIUS VPN 3000 ne doivent pas être configurés tant que le groupe de tunnels est configuré à l'étape 3 de la [configuration du concentrateur VPN 3000](#) et que le groupe de base du concentrateur VPN ne change pas des paramètres par défaut d'origine. **Attributs VPN 3000 recommandés** : **Primary-DNS** : saisissez l'adresse IP de votre serveur DNS principal. **Secondary-DNS** : saisissez l'adresse IP de votre serveur DNS secondaire. **Primary-WINS** : saisissez l'adresse IP de votre serveur WINS principal. **Secondary-WINS** : saisissez l'adresse IP de votre serveur WINS secondaire. **Tunneling-Protocols** : choisissez **IPsec**. Ceci autorise *uniquement* les connexions client IPsec. PPTP ou L2TP ne sont pas autorisés. **IPsec-Sec-Association** - Entrez **ESP-3DES-MD5**. Cela garantit que tous vos clients IPsec se connectent avec le chiffrement le plus élevé disponible. **IPsec-Allow-Password-Store** - Choisissez **Disallow** afin que les utilisateurs *ne soient pas* autorisés à enregistrer leur mot de passe dans le client VPN. **IPsec-Banner** : saisissez une bannière de message de bienvenue à présenter à l'utilisateur lors de la connexion. Par exemple, « Bienvenue dans l'accès VPN des employés de MyCompany ! » **IPsec-Default Domain** : saisissez le nom de domaine de votre société. Par exemple, «

mycompany.com ». Cet ensemble d'attributs n'est pas nécessaire. Mais si vous n'êtes pas certain que les attributs de groupe de base du concentrateur VPN 3000 ont changé, Cisco vous recommande de configurer ces attributs : **Simultanée-Logins** : saisissez le nombre de fois où vous autorisez un utilisateur à se connecter simultanément avec le même nom d'utilisateur. La recommandation est 1 ou 2. **SEP-Card-Assignment** : choisissez **Any-SEP**. **IPsec-Mode-Config** : choisissez **ON**. **IPsec over UDP** - Choisissez **OFF**, à moins que vous ne souhaitiez que les utilisateurs de ce groupe se connectent à l'aide d'IPsec via le protocole UDP. Si vous sélectionnez **ON**, le client VPN a toujours la possibilité de désactiver localement IPsec sur UDP et de se connecter normalement. **IPsec over UDP Port** : sélectionnez un numéro de port UDP compris entre 4001 et 49151. Ceci est utilisé uniquement si IPsec sur UDP est activé. L'ensemble d'attributs suivant nécessite que vous configuriez quelque chose sur le concentrateur VPN avant de pouvoir les utiliser. Ceci est recommandé uniquement pour les utilisateurs avancés. **Access-Hours** : vous devez configurer une plage d'heures d'accès sur le concentrateur VPN 3000 sous **Configuration > Policy Management**. Utilisez plutôt les heures d'accès disponibles dans Cisco Secure ACS pour Windows pour gérer cet attribut. **IPsec-Split-Tunnel-List** : vous devez configurer une liste réseau sur le concentrateur VPN sous **Configuration > Policy Management > Traffic Management**. Il s'agit d'une liste de réseaux envoyés au client qui lui demandent de chiffrer les données uniquement vers les réseaux de la liste. Choisissez **l'affectation IP dans la configuration du groupe** et cochez **Assigned from AAA server Pool** afin d'attribuer les adresses IP aux utilisateurs du client VPN une fois qu'ils ont été

Group Setup

Jump To

IP Assignment

No IP address assignment
 Assigned by dialup client
 Assigned from AAA Client pool

 Assigned from AAA server pool

Available Pools	Selected Pools
	pool1

authentifiés.

C

Choisissez **Configuration du système > Pools d'adresses IP** afin de créer un pool d'adresses IP pour les utilisateurs du client VPN et cliquez sur **Envoyer**

System Configuration

Edit

New Pool 	
Name	<input type="text" value="pool1"/>
Start Address	<input type="text" value="10.1.1.1"/>
End Address	<input type="text" value="10.1.1.10"/>

Submit

Cancel

System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
pool1	10.1.1.1	10.1.1.10	0%

Choisissez

Submit > Restart afin d'enregistrer la configuration et d'activer le nouveau groupe. Répétez ces étapes afin d'ajouter d'autres groupes.

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

User Setup

Select

User:

Find

Add/Edit

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

List all users

Remove Dynamic Users

Add/Edit.

ces paramètres dans la section de configuration de l'utilisateur

:

Configurez

User Setup

User: ipsecuser1 (New User)

Account Disabled

Supplementary User Info 

Real Name

Description

User Setup 

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Authentification par mot de passe : sélectionnez **ACS Internal Database**. **Cisco Secure PAP - Password** : saisissez un mot de passe pour l'utilisateur. **Cisco Secure PAP - Confirmer le mot de passe** : saisissez à nouveau le mot de passe du nouvel utilisateur. **Groupe auquel l'utilisateur est affecté** : sélectionnez le nom du groupe que vous avez créé à l'étape précédente. Cliquez sur **Submit** afin d'enregistrer et d'activer les paramètres utilisateur. Répétez ces étapes afin d'ajouter des utilisateurs supplémentaires.

[Attribuer une adresse IP statique à l'utilisateur du client VPN](#)

Procédez comme suit :

1. Créez un nouveau groupe VPN IPSECGRP.
2. Créez un utilisateur qui souhaite recevoir l'adresse IP statique et choisissez **IPSECGRP**. Choisissez **Affecter une adresse IP statique** avec l'adresse IP statique qui est attribuée sous Attribution d'adresse IP du

User Setup

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm
Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IPSECGRP

Callback

- Use group setting
- No callback allowed
- Callback using this number
- Dialup client specifies callback number
- Use Windows Database callback settings

Client IP Address Assignment

- Use group settings
- No IP address assignment
- Assigned by dialup client
- Assign static IP address
- Assigned by AAA client pool

Submit

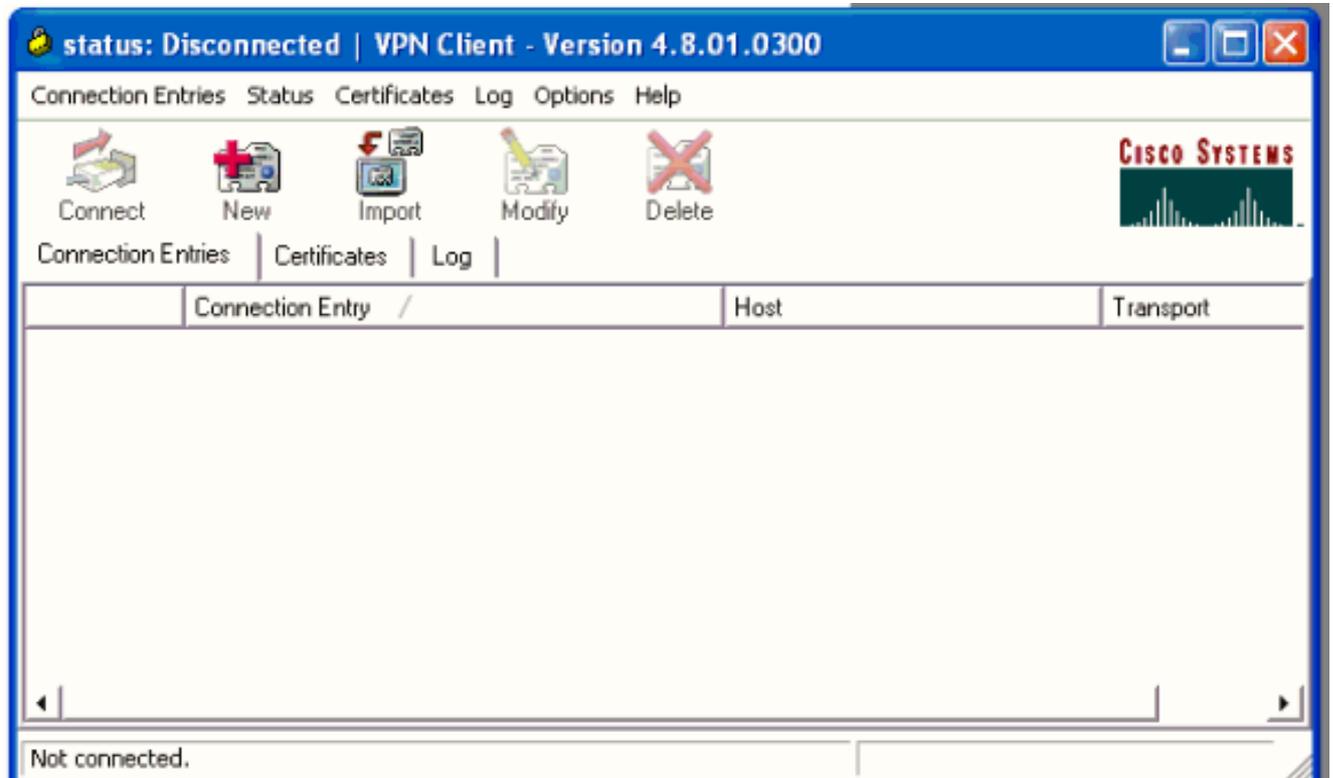
Delete

Cancel

client.

Cette section décrit la configuration côté client VPN.

1. Sélectionnez **Start > Programs > Cisco Systems VPN Client > VPN Client** (démarrer > programmes > client VPN Cisco Systems > client VPN).
2. Cliquez sur New [nouveau] pour ouvrir la fenêtre servant à créer une nouvelle entrée pour la connexion VPN.



3. Lorsque vous y êtes invité, attribuez un nom à votre entrée. Vous pouvez également entrer une description si vous le souhaitez. Spécifiez l'adresse IP de l'interface publique du concentrateur VPN 3000 dans la colonne Hôte et choisissez **Authentification de groupe**. Indiquez ensuite le nom et le mot de passe du groupe. Cliquez sur **Save** afin de terminer la nouvelle entrée de connexion

VPN Client | Create New VPN Connection Entry

Connection Entry: vpnuser

Description: Headoffice

Host: 10.0.0.1

Authentication | Transport | Backup Servers | Dial-Up

Group Authentication Mutual Group Authentication

Name: ipsecgroup

Password: *****

Confirm Password: *****

Certificate Authentication

Name: [dropdown]

Send CA Certificate Chain

Erase User Password Save Cancel

VPN.

Rema

re : assurez-vous que le client VPN est configuré pour utiliser le même nom de groupe et le même mot de passe configurés dans le concentrateur de la gamme Cisco VPN 3000.

[Ajoutez la gestion des comptes](#)

Une fois que l'authentification fonctionne, vous pouvez ajouter la comptabilité.

1. Sur le VPN 3000, choisissez **Configuration > System > Servers > Accounting Servers**, puis ajoutez le serveur **Cisco Secure ACS pour Windows**.
2. Vous pouvez ajouter des serveurs de comptabilité individuels à chaque groupe lorsque vous choisissez **Configuration > User Management > Groups**, mettez en surbrillance un groupe et cliquez sur **Modify Acct. Serveurs**. Saisissez ensuite l'adresse IP du serveur de comptabilité avec le secret du serveur.

Remote Access Sessions

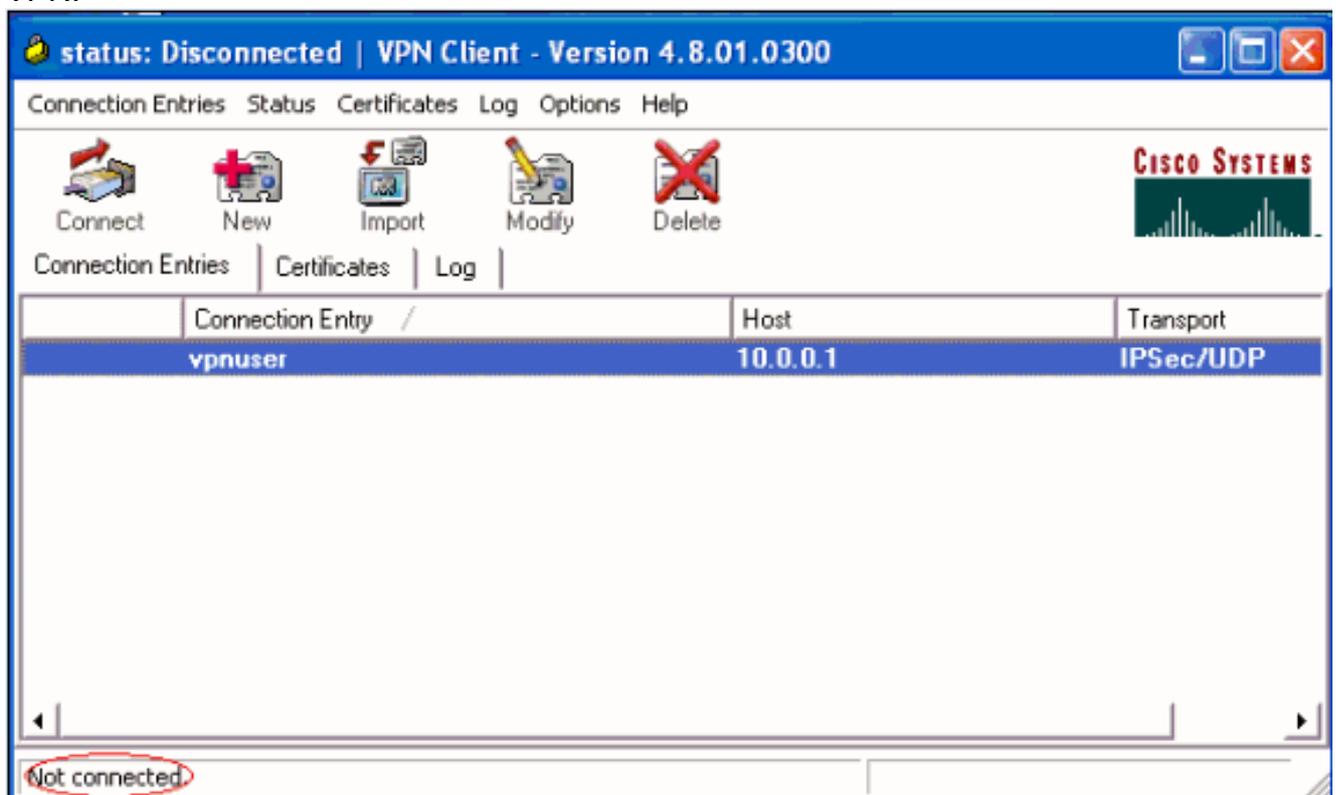
[[LAN-to-LAN Sessions](#) | [Management Sessions](#)]

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
ipseccuser1	10.1.1.9 192.168.1.2	ipseccgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout Ping]

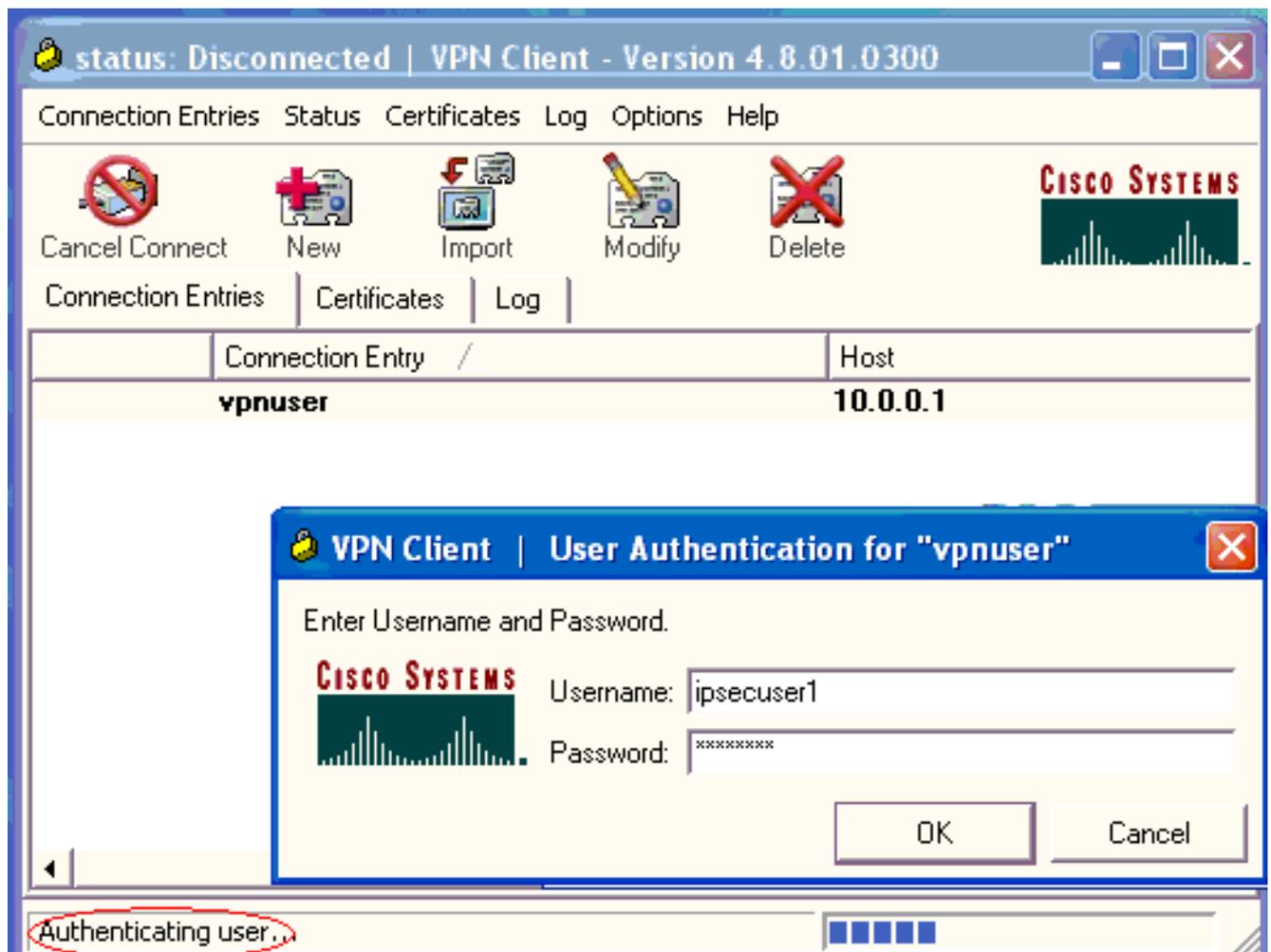
Vérifier le client VPN

Complétez ces étapes afin de vérifier le client VPN.

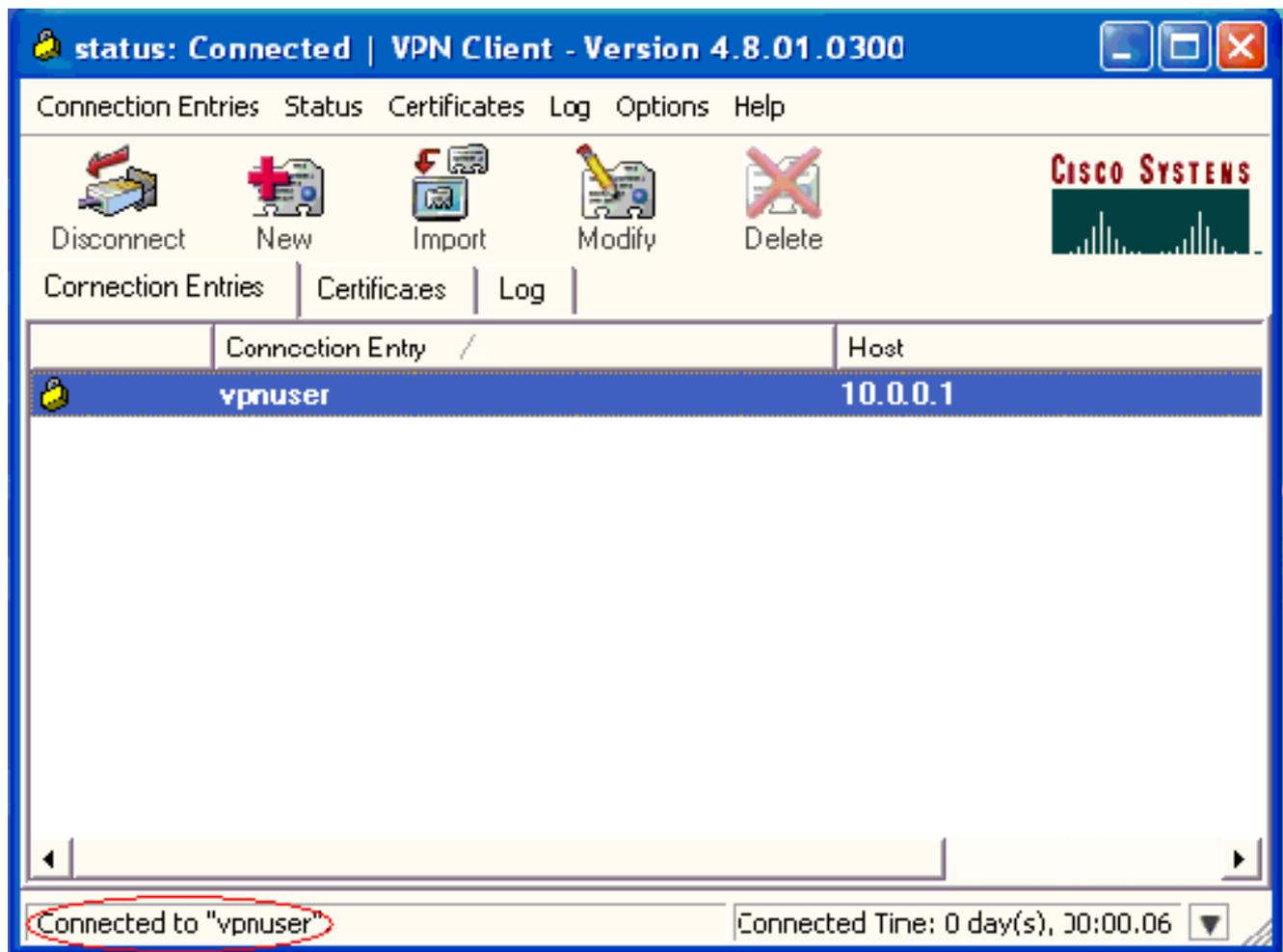
1. Cliquez sur **Connect** afin d'initier une connexion VPN.



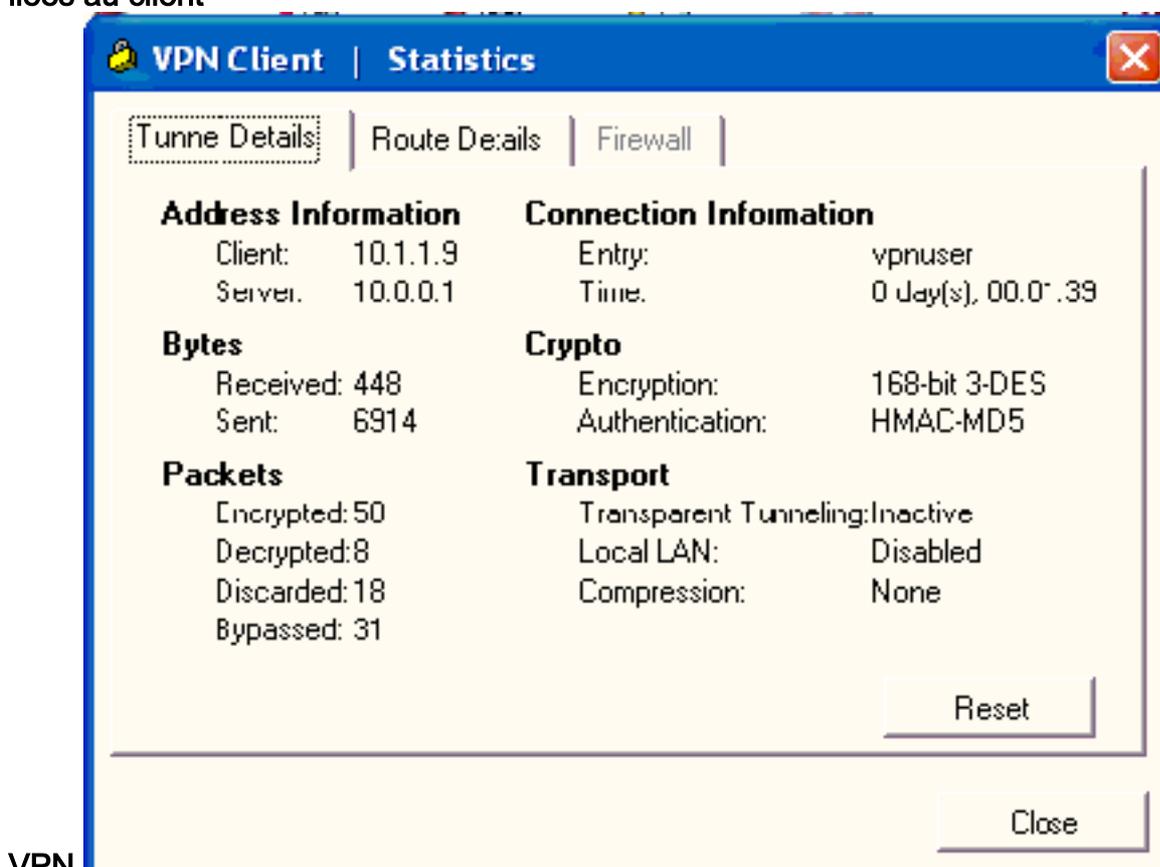
2. Cette fenêtre s'affiche pour l'authentification des utilisateurs. Entrez un nom d'utilisateur et un mot de passe valides afin d'établir la connexion VPN.



3. Le client VPN est connecté au concentrateur VPN 3000 du site central.



4. Sélectionnez **Status > Statistics** (état > statistiques) pour consulter les statistiques du tunnel liées au client



VPN.

Success

 Authentication Successful

Continue

Une authentification réussie apparaît.

2. En cas d'échec, un problème de configuration ou de connectivité IP se produit. Vérifiez les messages liés à l'échec de la connexion sur le serveur ACS. Si aucun message n'apparaît dans ce journal, il y a probablement un problème de connectivité IP. La requête RADIUS n'atteint pas le serveur RADIUS. Vérifiez que les filtres appliqués à l'interface du concentrateur VPN 3000 appropriée permettent l'entrée et la sortie de paquets RADIUS (1645). Si l'authentification de test réussit, mais que les connexions au concentrateur VPN 3000 continuent à échouer, vérifiez le journal des événements filtrables via le port de console. Si les connexions ne fonctionnent pas, vous pouvez ajouter des classes d'événements AUTH, IKE et IPsec au concentrateur VPN lorsque vous sélectionnez **Configuration > System > Events > Classes > Modify (Severity to Log=1-9, Severity to Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG et IPSECDECODE sont également disponibles, mais peuvent fournir trop d'informations. Si des informations détaillées sont nécessaires sur les attributs transmis à partir du serveur RADIUS, AUTHDECODE, IKEDECODE et IPSECDECODE fournissent ceci au niveau Severity to Log=1-13.
3. Récupérez le journal des événements à partir de **Monitoring > Event Log**.

Monitoring | Live Event Log

```
1513 10/27/2006 18:37:25.330 SEV=8 IKEDBG/81 RPT=47 192.168.1.2
SENDING Message (msgid=6679165e) with payloads :
HDR + HASH (8) + NOTIFY (11)
total length : 80

1515 10/27/2006 18:37:35.830 SEV=8 IKEDBG/81 RPT=48 192.168.1.2
RECEIVED Message (msgid=8575be96) with payloads :
HDR + HASH (8) + NOTIFY (11) + NONE (0)
total length : 80

1517 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=120 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
processing hash

1518 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=121 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Processing Notify payload

1519 10/27/2006 18:37:35.830 SEV=9 IKEDBG/36 RPT=10 192.168.1.2
Group [ipsecgroup] User [ipsecuser1]
Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x653e486d)

1521 10/27/2006 18:37:35.830 SEV=9 IKEDBG/0 RPT=122 192.168.1.2
```

Pause Display

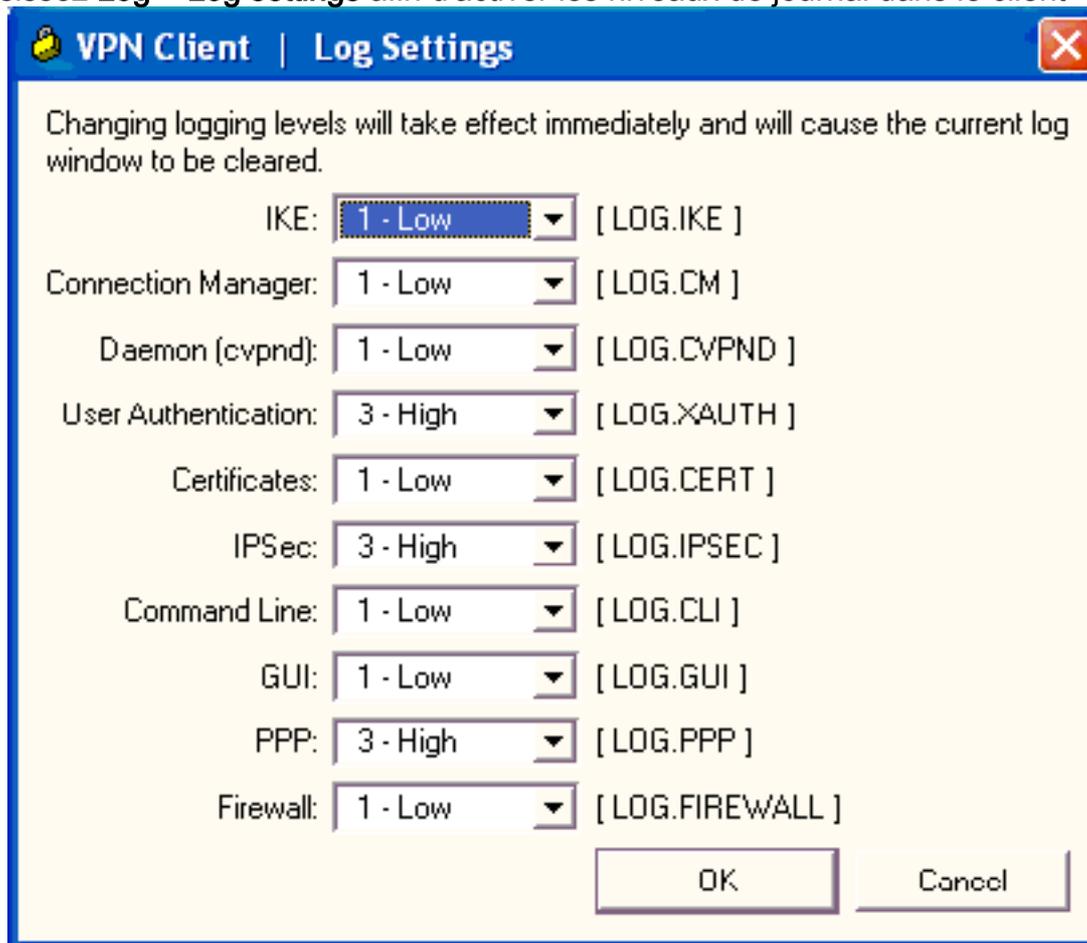
Clear Display

Restart

Receiving.....

Complétez ces étapes afin de dépanner le client VPN 4.8 pour Windows.

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



VPN.

2. Choisissez **Log > Log Window** afin d'afficher les entrées de journal dans le client VPN.

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:26:29.234 10/31/06 Sev=Warning/2 IKE/0xA3000067
Received an IPC message during invalid state (IKE_MAIN:507)

2 13:26:36.109 10/31/06 Sev=Warning/2 CVPND/0xE3400013
AddRoute failed to add a route: code 87
Destination 192.168.1.255
Netmask 255.255.255.255
Gateway 10.1.1.9
Interface 10.1.1.9

3 13:26:36.109 10/31/06 Sev=Warning/2 CM/0xA3100024
Unable to add route. Network: c0a801ff, Netmask: ffffffff, Interface: a010109, Gateway: a010109

Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2
Config file directory: C:\Program Files\Cisco Systems\VPN Client

1 13:27:31.640 10/31/06 Sev=Info/4IPSEC/0x63700019
Activate outbound key with SPI=0x2c9afd45 for inbound key with SPI=0xc9c1b7d5

2 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0xc9c1b7d5

3 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0xc9c1b7d5

4 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x63700013
Delete internal key with SPI=0x2c9afd45

5 13:27:42.656 10/31/06 Sev=Info/4IPSEC/0x6370000C
Key deleted by SPI 0x2c9afd45

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](#)
- [Configuration des filtres dynamiques sur un serveur RADIUS](#)
- [Support et documentation techniques - Cisco Systems](#)