

# 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](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Diagramme du réseau](#)

[Groupes d'utilisation sur le concentrateur VPN 3000](#)

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

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

[Configuration du serveur RADIUS](#)

[Assignez une adresse IP statique à l'utilisateur de client vpn](#)

[Configuration de client vpn](#)

[Ajoutez la gestion des comptes](#)

[Vérifiez](#)

[Vérifiez le concentrateur VPN](#)

[Vérifiez le client vpn](#)

[Dépannez](#)

[Dépannez le client vpn 4.8 pour Windows](#)

[Informations connexes](#)

## [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 RADIUS 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](#).

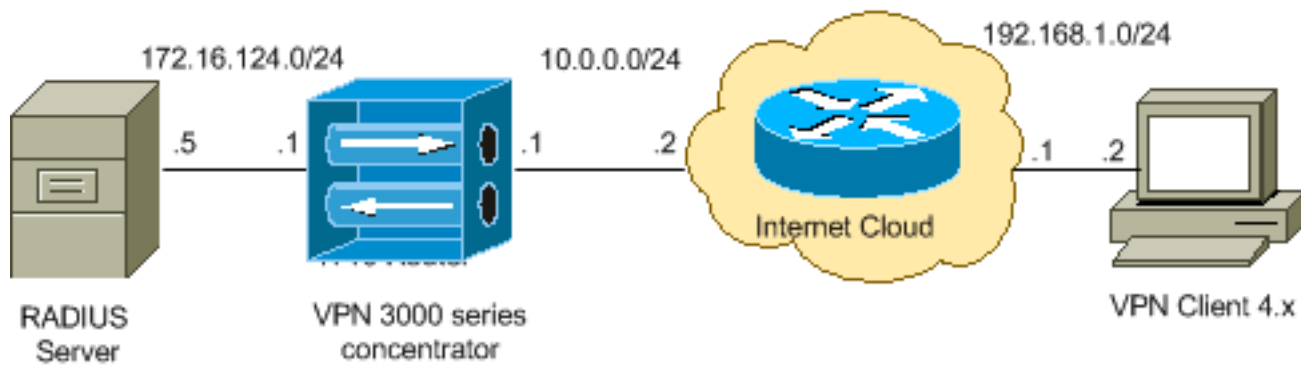
## Configurez

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 vérifier les interfaces après que vous apportiez le GUI.

Configuration | Interfaces Friday, 27 October 2006  
Save Needed

This section lets you configure the VPN 3000 Concentrator's network interfaces and power supplies.

In the table below, or in the picture, select and click the interface you want to configure:

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

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.

Configure and add a user authentication server.

<b>Server Type</b>	<input type="text" value="RADIUS"/>	Selecting <i>Internal Server</i> will let you add users to database. If you are using RADIUS authenticator additional authorization check, do not configure at
<b>Authentication Server</b>	<input type="text" value="172.16.124.5"/>	Enter IP address or hostname.
<b>Used For</b>	<input type="text" value="User Authentication"/>	Select the operation(s) for which this RADIUS se
<b>Server Port</b>	<input type="text" value="0"/>	Enter 0 for default port (1645).
<b>Timeout</b>	<input type="text" value="4"/>	Enter the timeout for this server (seconds).
<b>Retries</b>	<input type="text" value="2"/>	Enter the number of retries for this server.
<b>Server Secret</b>	<input type="text" value="aAaAaAaAaA"/>	Enter the RADIUS server secret.
<b>Verify</b>	<input type="text" value="aAaAaAaAaA"/>	Re-enter the secret.

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.

- 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**

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 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</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

**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**

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	<input type="text" value="ESP-3DES-MD5"/>	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	<input type="text" value="If supported by certificate"/>	<input checked="" type="checkbox"/>	Select whether or not to validate the identity.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives.
Confidence Interval	<input type="text" value="300"/>	<input checked="" type="checkbox"/>	(seconds) Enter how long a peer is permitted to remain idle before the concentrator checks to see if it is still connected.
Tunnel Type	<input type="text" value="Remote Access"/>	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Upstream concentrator configuration may be needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	<input type="text" value="RADIUS"/>	<input type="checkbox"/>	Select the authentication method for members of this group. This method only applies to <b>Individual User Authentication</b> .
Authorization Type	<input type="text" value="None"/>	<input checked="" type="checkbox"/>	If members of this group need authorization, select the authorization method. If you configure this method, you must also configure an Authorization Server.

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

- 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.

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
<input type="button" value="Add Group"/> <input type="button" value="Modify Group"/> <input type="button" value="Delete Group"/>	ipsecgroup (Internally Configured)	<input type="button" value="Authentication Servers"/> <input type="button" value="Authorization Servers"/> <input type="button" value="Accounting Servers"/> <input type="button" value="Address Pools"/> <input type="button" value="Client Update"/> <input type="button" value="Bandwidth Assignment"/> <input type="button" value="WebVPN Servers and URLs"/> <input type="button" value="WebVPN Port Forwarding"/>

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.

- 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 | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

**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.

IP Reuse Delay  Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

## [Configuration du serveur RADIUS](#)

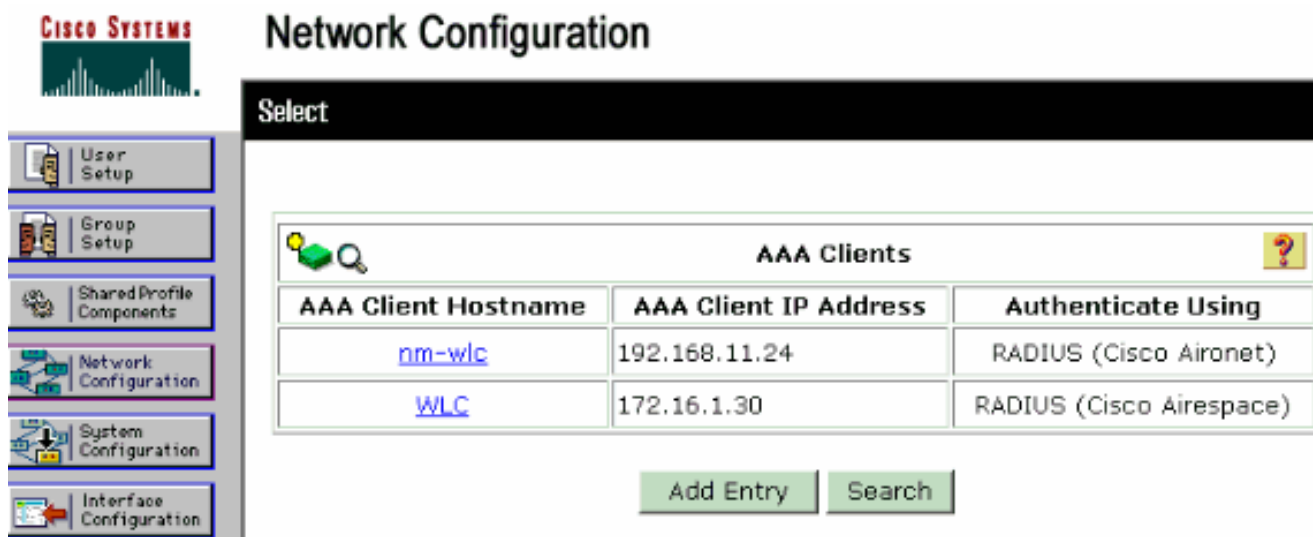
Cette section du document décrit la procédure exigée pour configurer le Cisco Secure ACS en tant que serveur de RAYON pour l'authentification d'utilisateur de client VPN expédié par le



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.



The screenshot shows the Cisco Systems Network Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, and Interface Configuration. The main area is titled 'Network Configuration' and has a 'Select' header. Below this is a table titled 'AAA Clients' with a search icon and a help icon. The table has three columns: 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using'. It contains two entries: one for 'nm-wlc' with IP '192.168.11.24' and authentication 'RADIUS (Cisco Aironet)', and another for 'WLC' with IP '172.16.1.30' and authentication 'RADIUS (Cisco Airespace)'. Below the table are 'Add Entry' and 'Search' buttons.

AAA Client Hostname	AAA Client IP Address	Authenticate Using
<a href="#">nm-wlc</a>	192.168.11.24	RADIUS (Cisco Aironet)
<a href="#">WLC</a>	172.16.1.30	RADIUS (Cisco Airespace)

Ajoutez ces paramètres pour votre concentrateur VPN 3000

:

# Network Configuration

Edit

## Add AAA Client

AAA Client Hostname	<input type="text" value="VPN3000"/>
AAA Client IP Address	<input type="text" value="172.16.124.1"/>
Key	<input type="text" value="cisco123"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	

Submit

Submit + Apply

Cancel

**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].

# 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

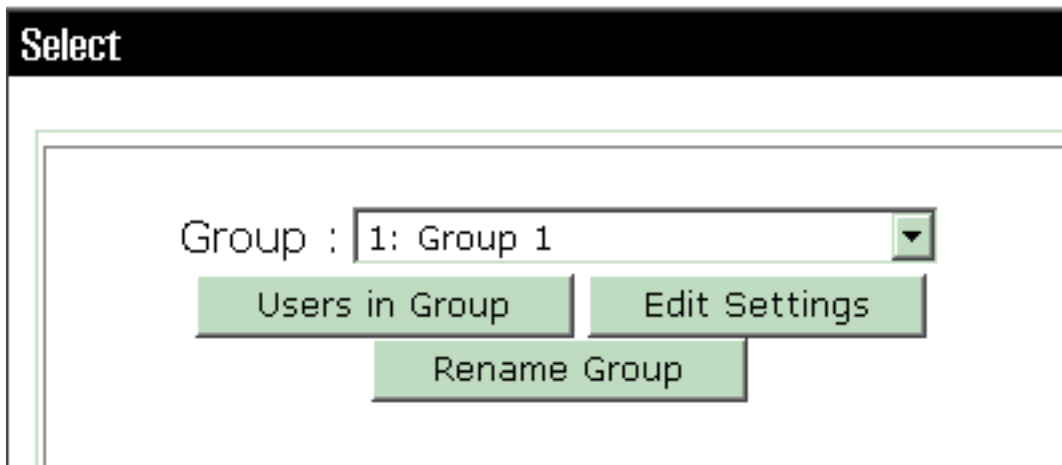
Submit

Cancel

**Remarque:** 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**

# Group Setup



groupe.

Chang

ez 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


# 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 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

# Group Setup

Jump To IP Address Assignment

**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 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 **rejetent** 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

vosre 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 obtenent

# Group Setup

**Jump To** IP Address Assignment

### 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

-.>  
<-.  
Up Down

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

## 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.

Submit Cancel



# System Configuration

Select

AAA Server IP Pools 			
Pool Name	Start Address	End Address	In Use
<a href="#">pool1</a>	10.1.1.1	10.1.1.10	0%

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

## 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/l'éditez.

rez ces paramètres sous la section User Setup


:

Configu

## 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 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

## 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

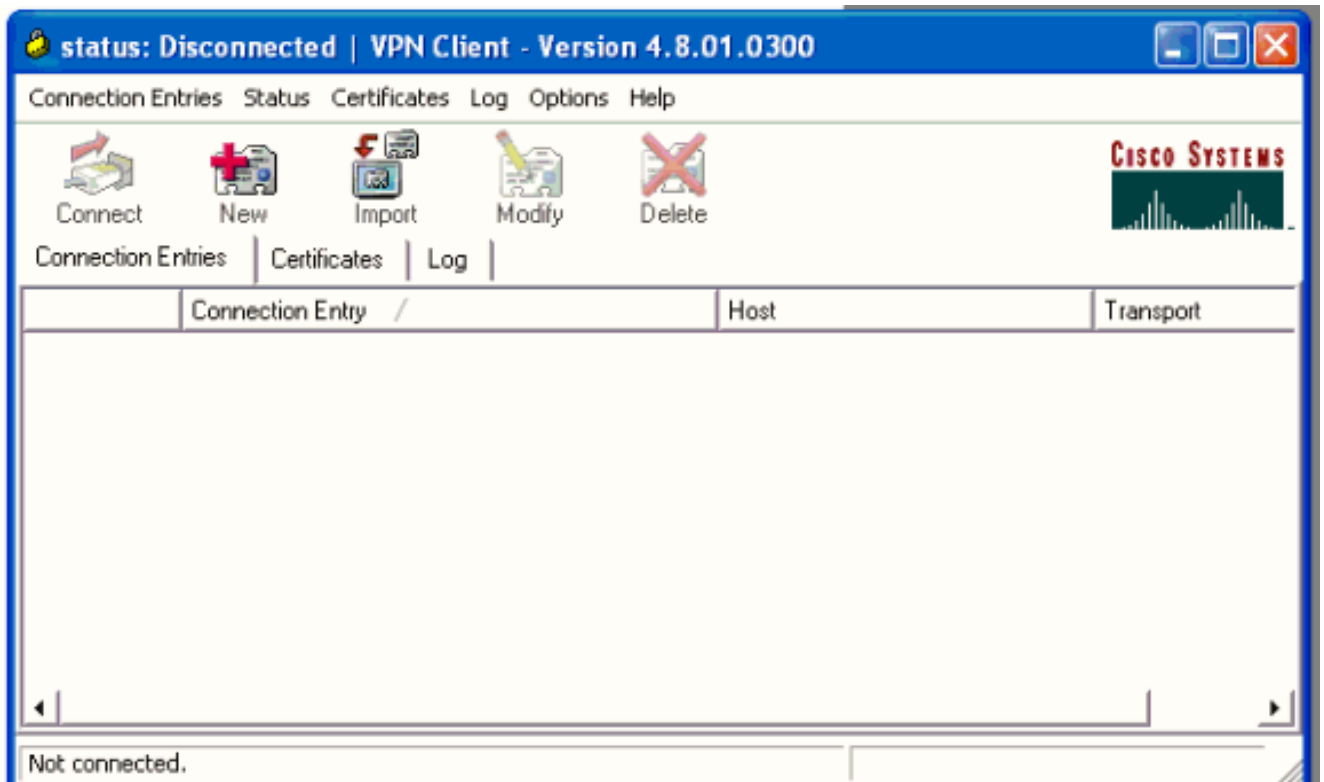
Delete

Cancel

client.

Cette section décrit la configuration 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 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

**reque:** 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 **modifiez Acct. Serveurs**. Écrivez alors l'adresse IP du serveur de comptabilité avec le secret de serveur.

Configure and add a RADIUS user accounting server.

**Accounting Server**  Enter IP address or hostname.

**Server Port**  Enter the server UDP port number.

**Timeout**  Enter the timeout for this server (se

**Retries**  Enter the number of retries for this

**Server Secret**  Enter the RADIUS server secret.

**Verify**  Re-enter the server secret.

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

Select

RADIUS Accounting active.csv

Regular Expression  Start Date & Time  End Date & Time  Rows per Page

Filtering is not applied.

Date	Time	User-Name	Group-Name	Calling-Station-Id	Acct-Status-Type	Acct-Session-Id	Acct-Session-Time	Service-Type	Framed-Protocol	Acct-Input-Octets	Acct-Output-Octets	Acct-Input-Packets	Acct-Output-Packets
10/27/2006	18:38:20	ipseuser1	ipsegroup	192.168.1.2	Start	E8700001	..	Framed	PPP	..	..	..	..
10/27/2006	18:38:20	VPN 3000 Concentrator	Default Group	..	Accounting On	..	..	..	..	..	..	..	..
10/27/2006	13:17:10	VPN 3000 Concentrator	Default Group	..	Accounting Off	..	..	..	..	..	..	..	..

## 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

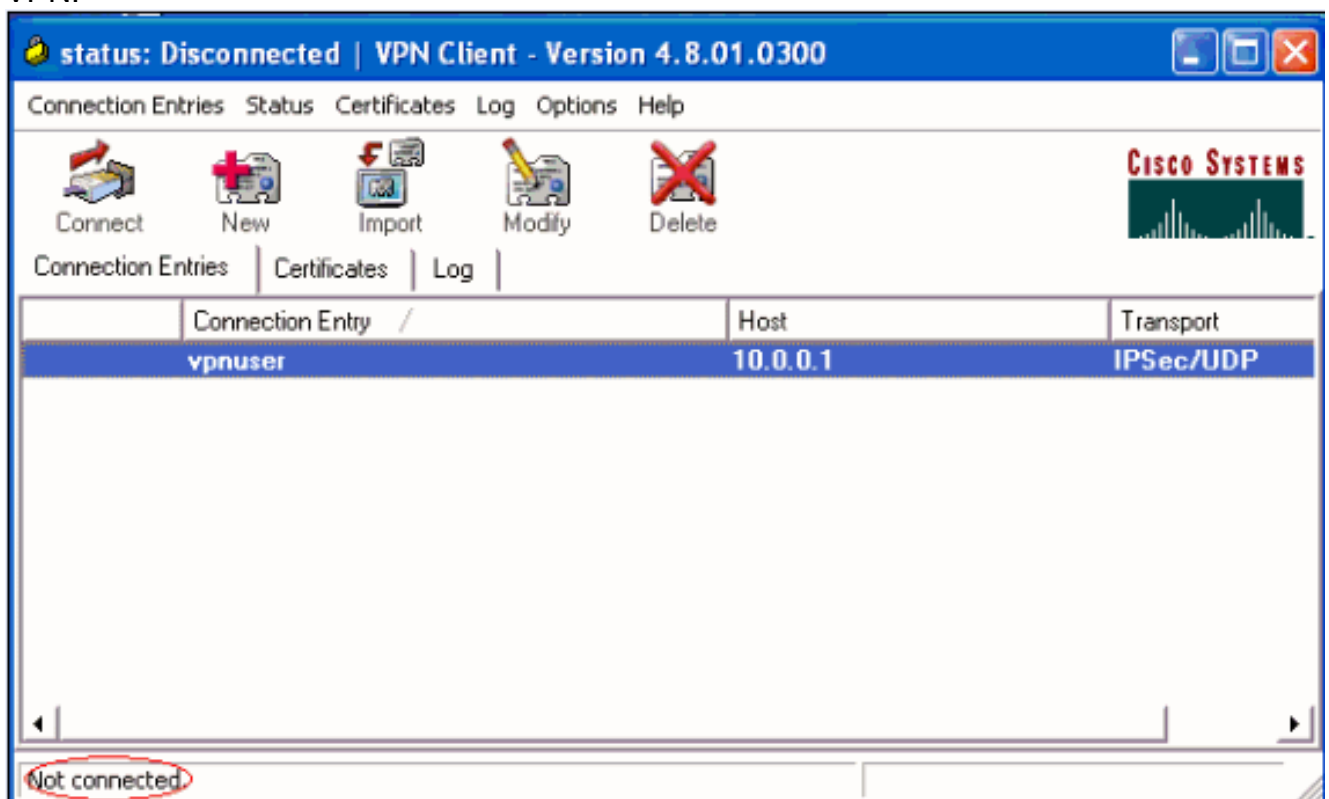
[ [LAN-to-LAN Sessions](#) | [Management Sessions](#) ]

<a href="#">Username</a>	<a href="#">Assigned IP Address</a> <a href="#">Public IP Address</a>	<a href="#">Group</a>	<a href="#">Protocol Encryption</a>	<a href="#">Login Time Duration</a>	<a href="#">Client Type Version</a>	<a href="#">Bytes Tx</a> <a href="#">Bytes Rx</a>	<a href="#">NAC Result Posture Token</a>	<a href="#">Actions</a>
<a href="#">ipsecuser1</a>	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	[ <a href="#">Logout</a>   <a href="#">Ping</a> ]

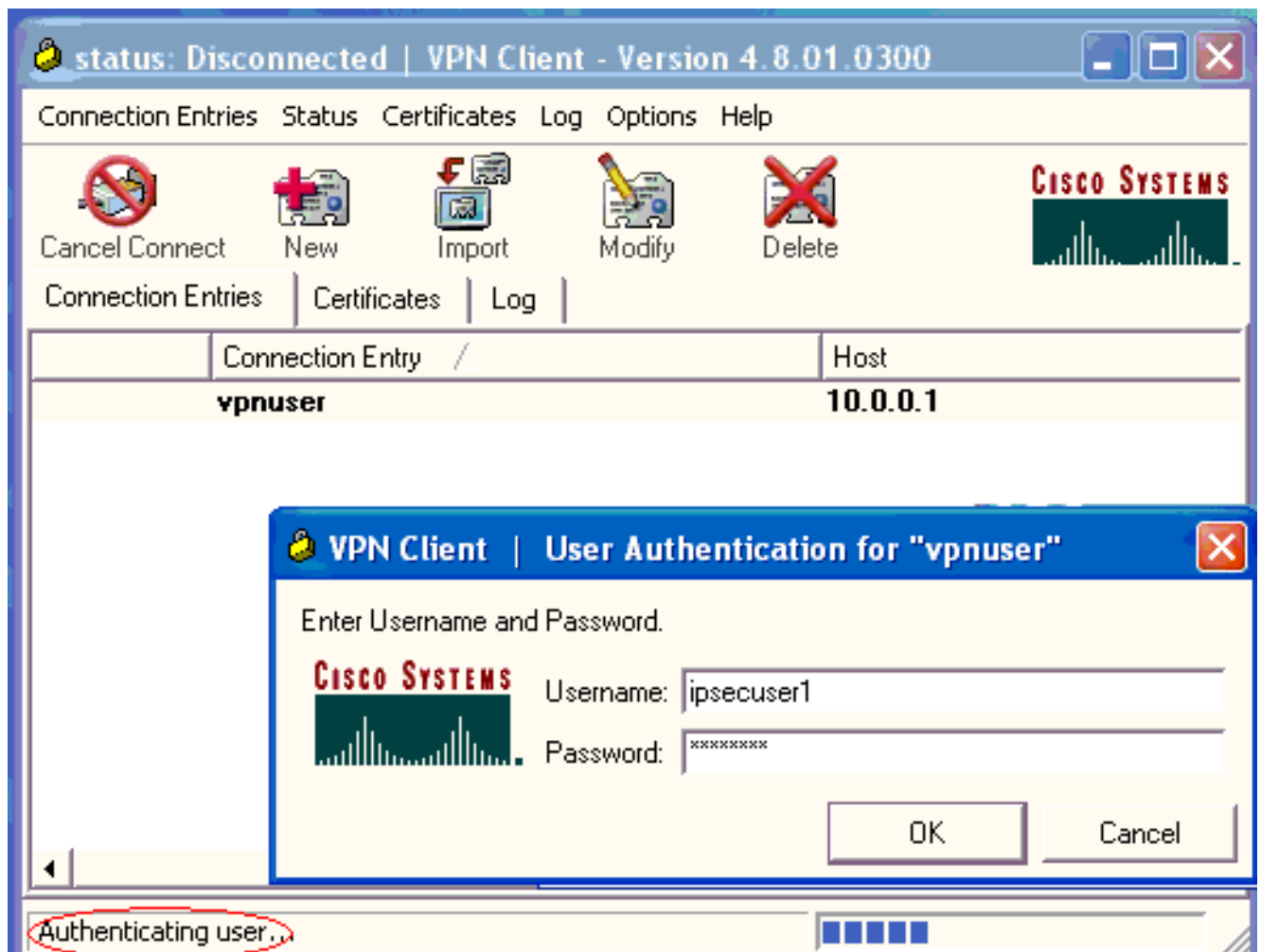
## Vérifiez le client vpn

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

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

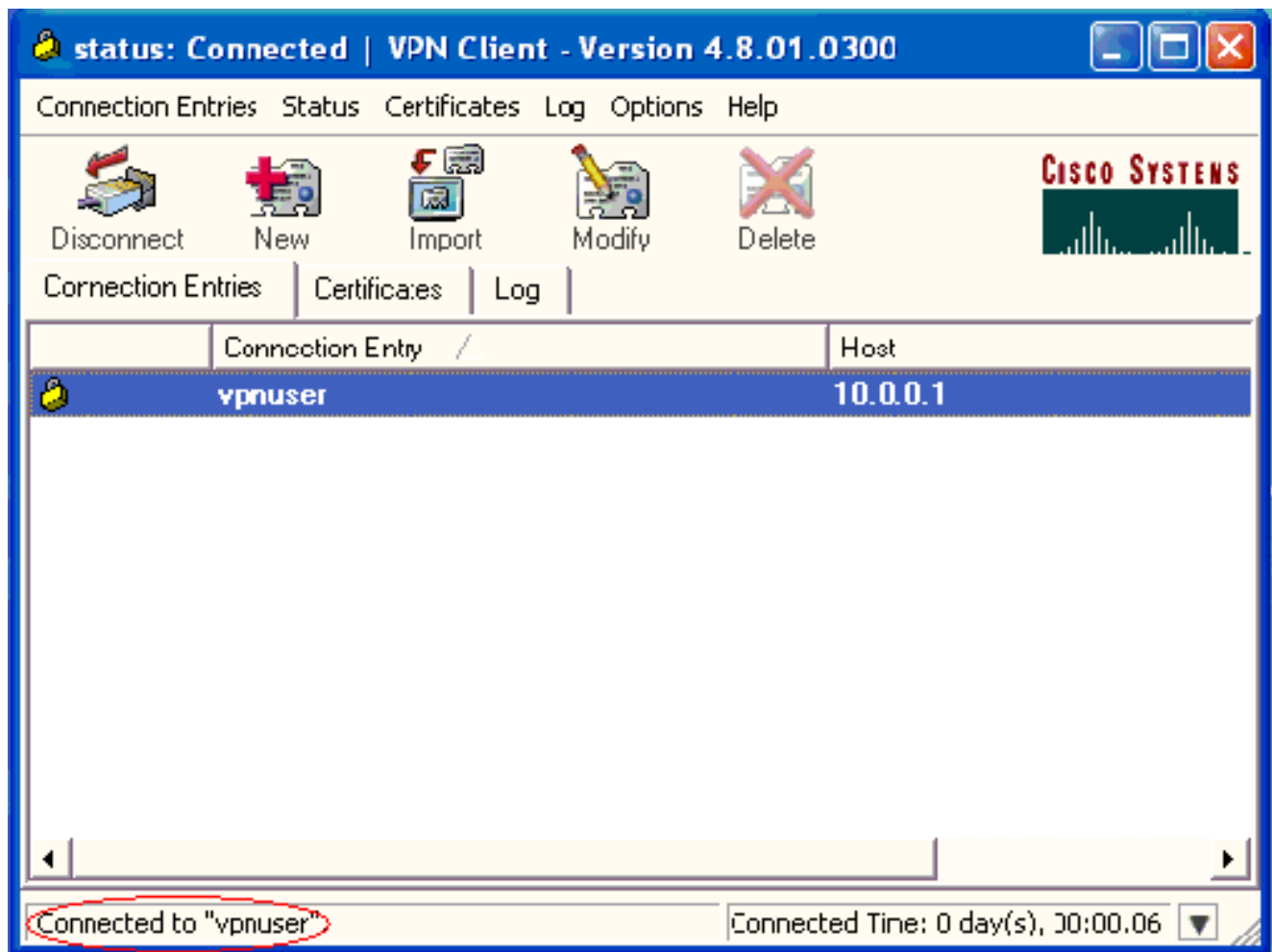


2. Cette fenêtre apparaît pour l'authentification de l'utilisateur. Entrez un nom d'utilisateur valide et un mot de passe afin d'établir la connexion VPN.

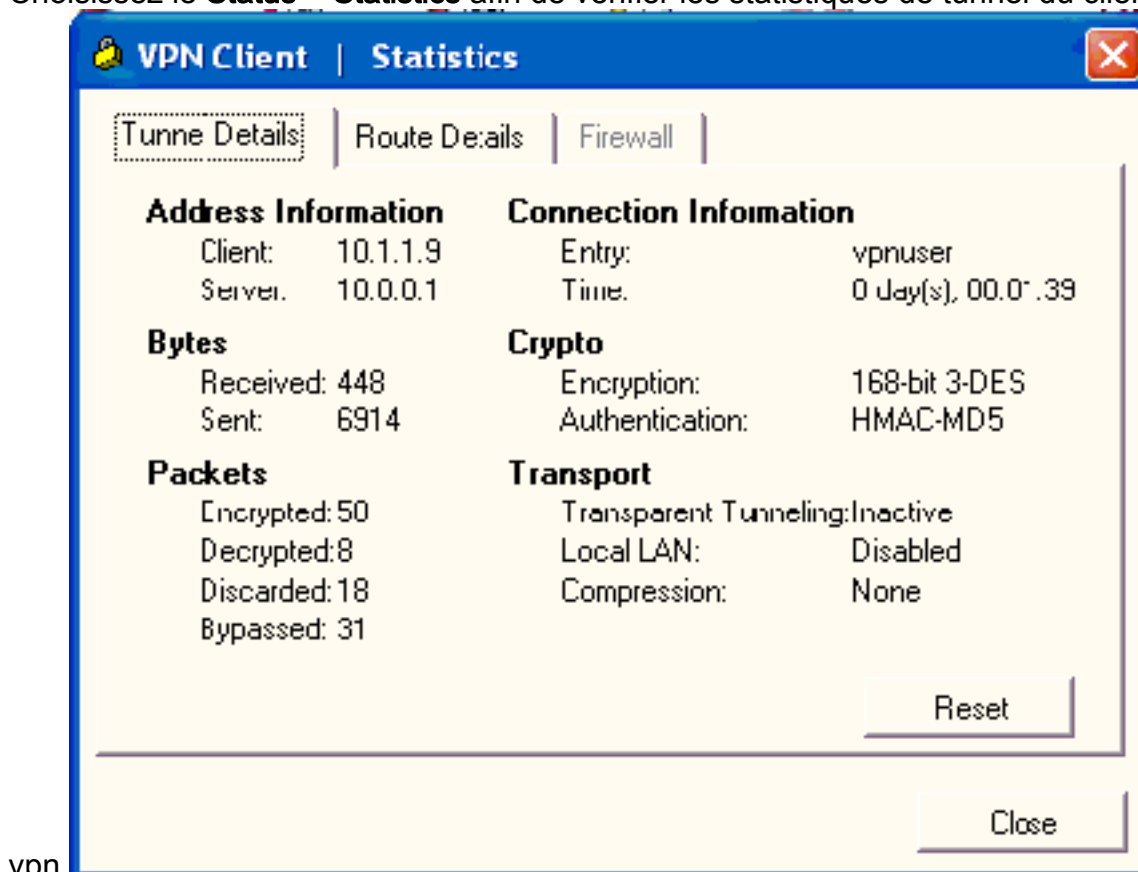


3. Le client vpn obtient lié au concentrateur VPN 3000 au lieu d'exploitation principal.





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**.

Configuration | System | Servers | Authentication

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Direct configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or

Authentication Servers	Actions
172.16.124.5 (Radius/User Authentication) Internal (Internal)	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test"/>

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


Configuration | System | Servers | Authentication | Test

Enter a username and password with which to test. **Please wait for the operation**

Username

Password

Success

 Authentication Successful

Une authentification réussie apparaît.

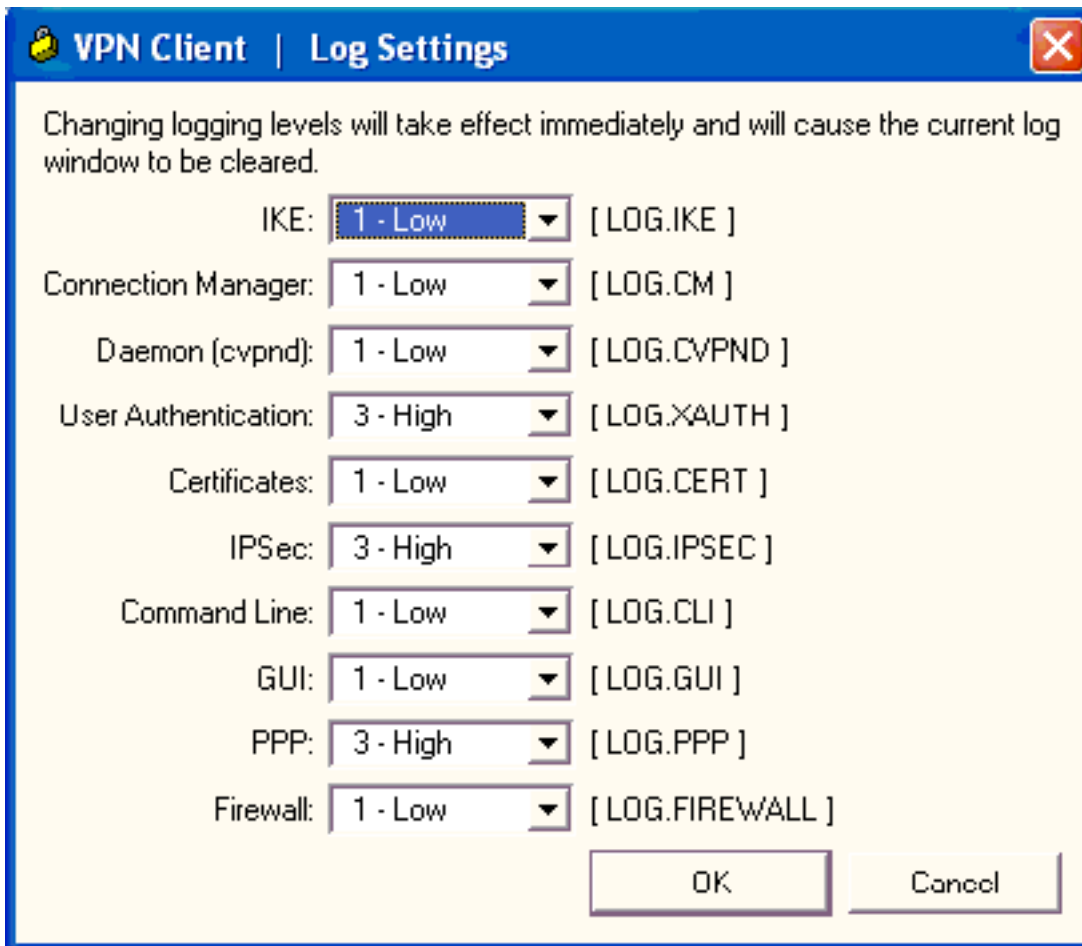
2. S'il échoue, il y a un problème de configuration ou un problème de connectivité IP. Vérifiez le login d'essais ratés le serveur ACS pour des messages liés à la panne. Si message n'apparaît pas dans ce log puis il y a probablement un problème de connectivité IP. La demande RADIUS n'atteint pas le serveur 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 > modifiez (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

```
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
```

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](#)