Comment configurer le PPTP du concentrateur VPN 3000 avec l'authentification locale

Contenu

Introduction

Le concentrateur Cisco VPN 3000 prend en charge la méthode de tunnellisation PPTP (Point-to-Point Tunnel Protocol) pour les clients Windows natifs. Il existe une prise en charge du cryptage 40 bits et 128 bits sur ces concentrateurs VPN pour une connexion sécurisée et fiable.

Référez-vous à Configuration du concentrateur VPN 3000 PPTP avec Cisco Secure ACS pour l'authentification RADIUS Windows afin de configurer le concentrateur VPN pour les utilisateurs PPTP avec une authentification étendue à l'aide du serveur Cisco Secure Access Control Server (ACS).

Conditions préalables

Conditions requises

Assurez-vous que vous remplissez les conditions requises mentionnées à la section Quand le chiffrement PPTP est-il pris en charge sur un concentrateur Cisco VPN 3000 ? avant de tenter cette configuration.

Components Used

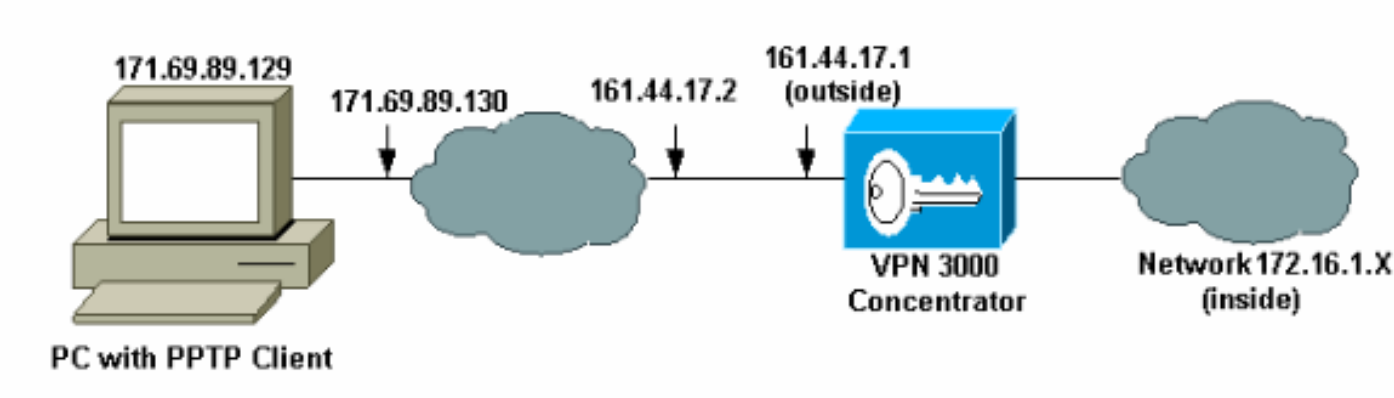
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur VPN 3015 avec version 4.0.4.A
- PC Windows avec client PPTP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



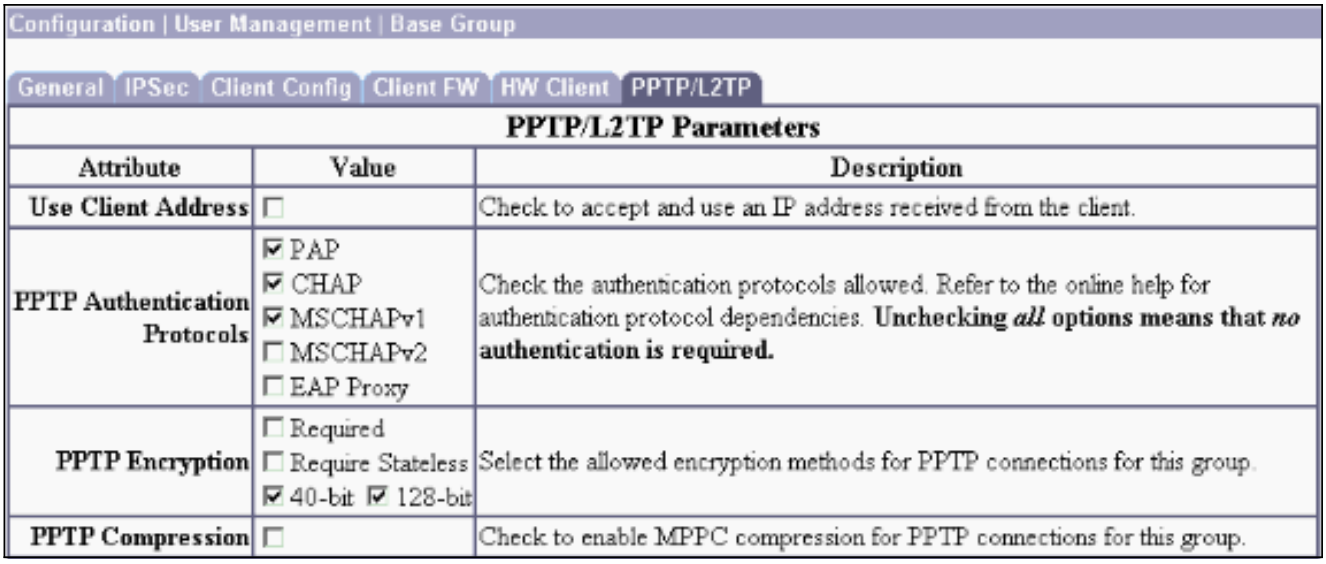
Conventions

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

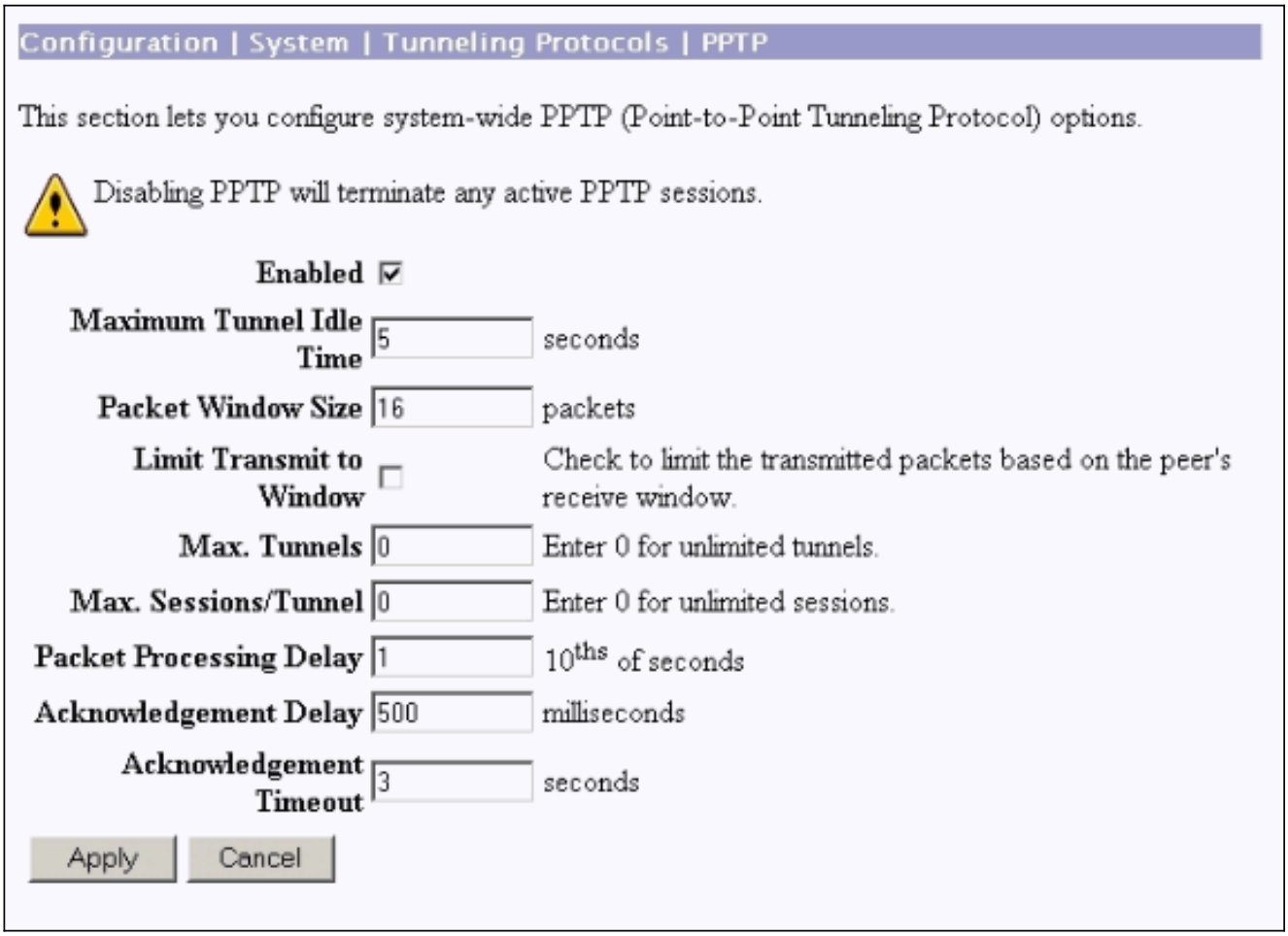
Configuration du concentrateur VPN 3000 avec authentification locale

Complétez ces étapes pour configurer le concentrateur VPN 3000 avec l'authentification locale.

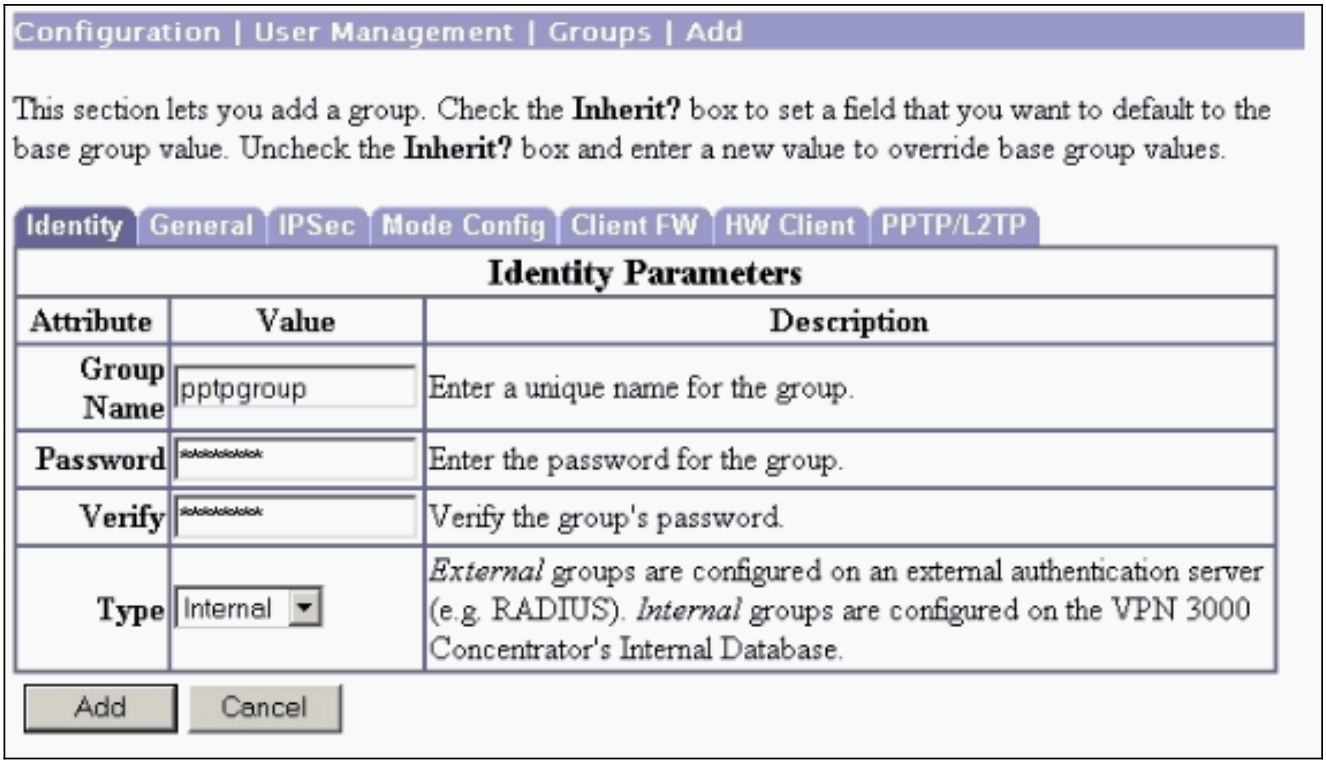
1. Configurez les adresses IP respectives dans le concentrateur VPN et assurez-vous que vous disposez d'une connectivité.
2. Assurez-vous que **l'authentification PAP** est sélectionnée dans l'onglet **Configuration > User Management > Base Group**
   PPTP/L2TP.



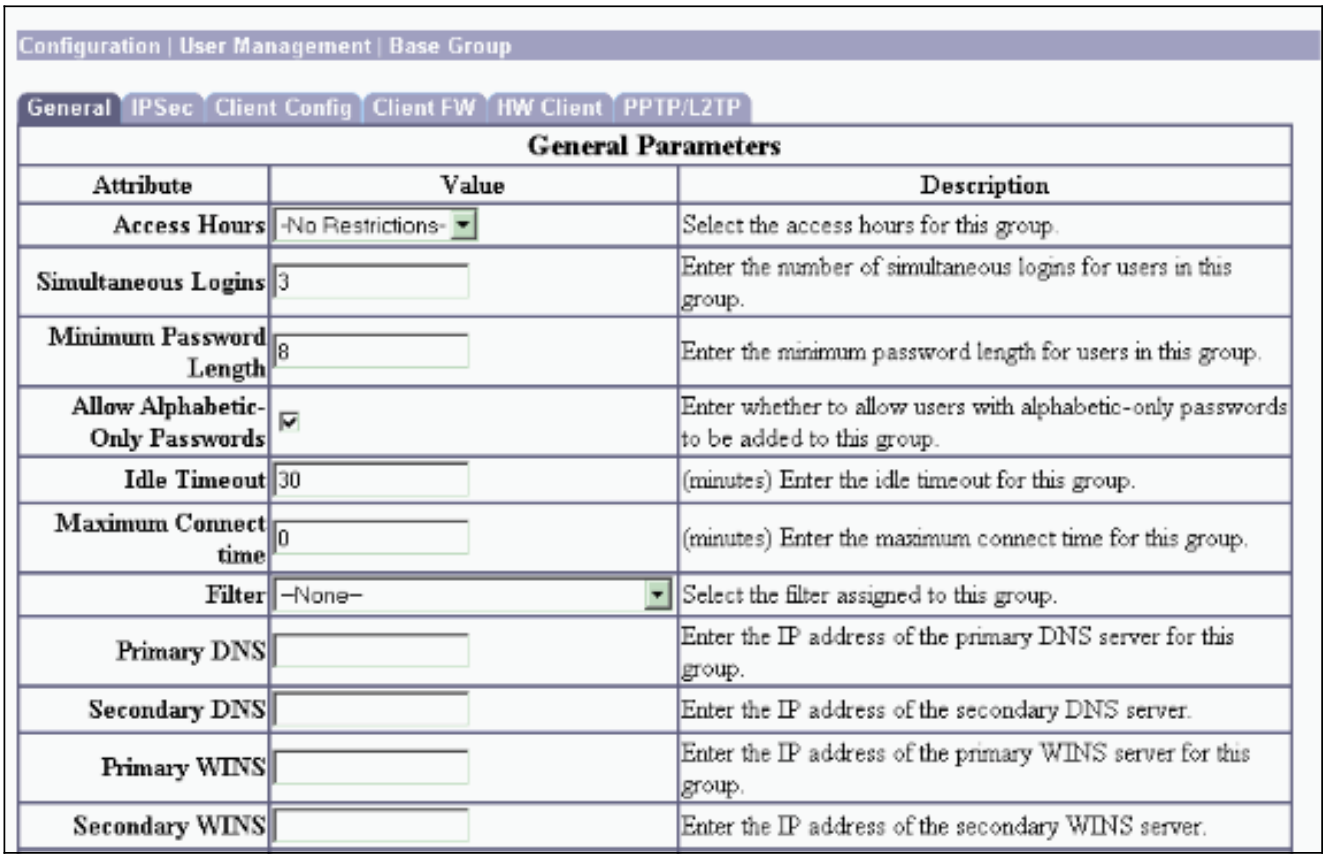
3. Sélectionnez **Configuration > System > Tunneling Protocols > PPTP** et assurez-vous que **Enabled** est
coché.



4. Sélectionnez **Configuration > User Management > Groups > Add**, puis configurez un groupe PPTP. Dans cet exemple, le nom du groupe est pptpgroup et le mot de passe (et le mot de passe de vérification) est
cisco123.



5. Sous l'onglet Général du groupe, vérifiez que l'option **PPTP** est activée dans les protocoles d'authentification.



SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	☐	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

6. Sous l'onglet PPTP/L2TP, activez l'authentification **PAP** et désactivez le **chiffrement** (le chiffrement peut être activé à tout moment dans le futur).

Configuration | User Management | Groups | Modify pptpgroup

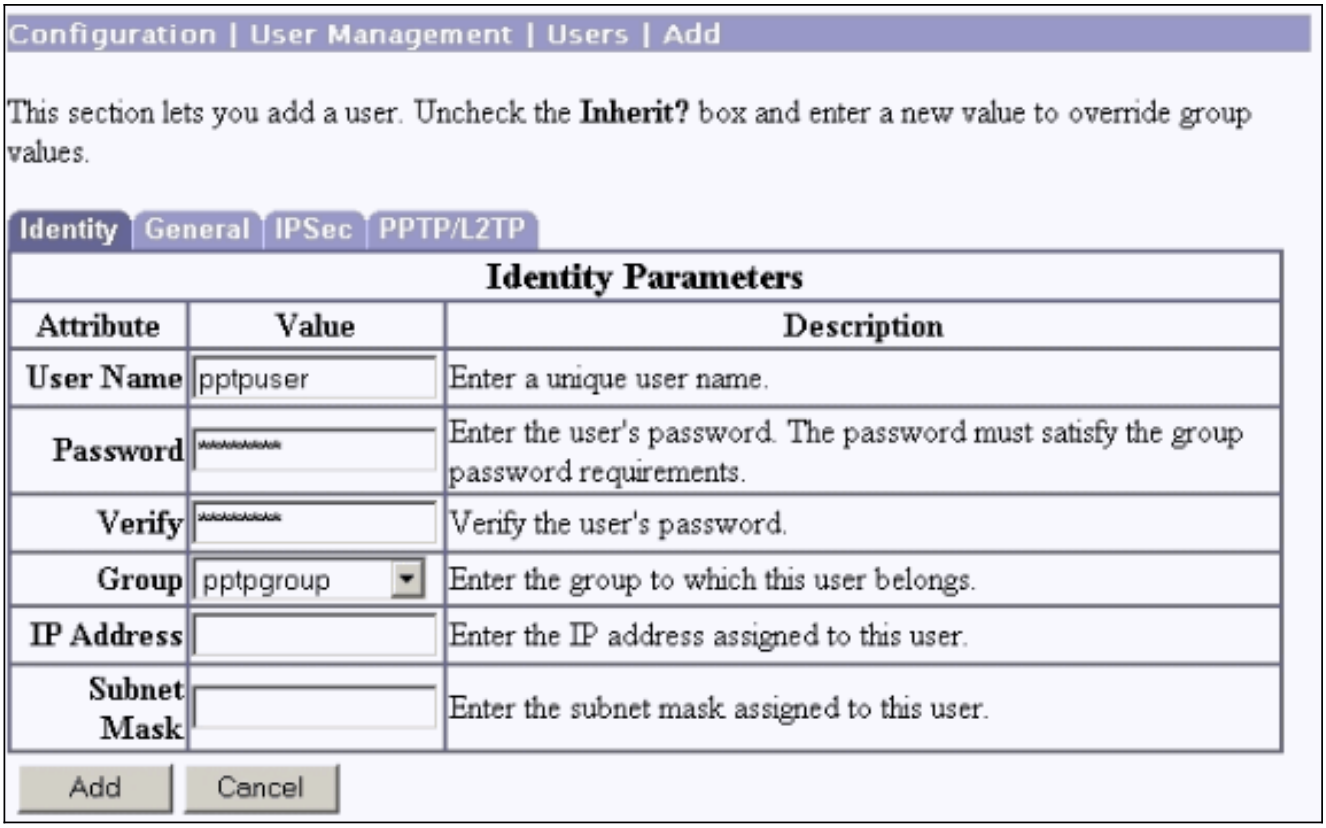
Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

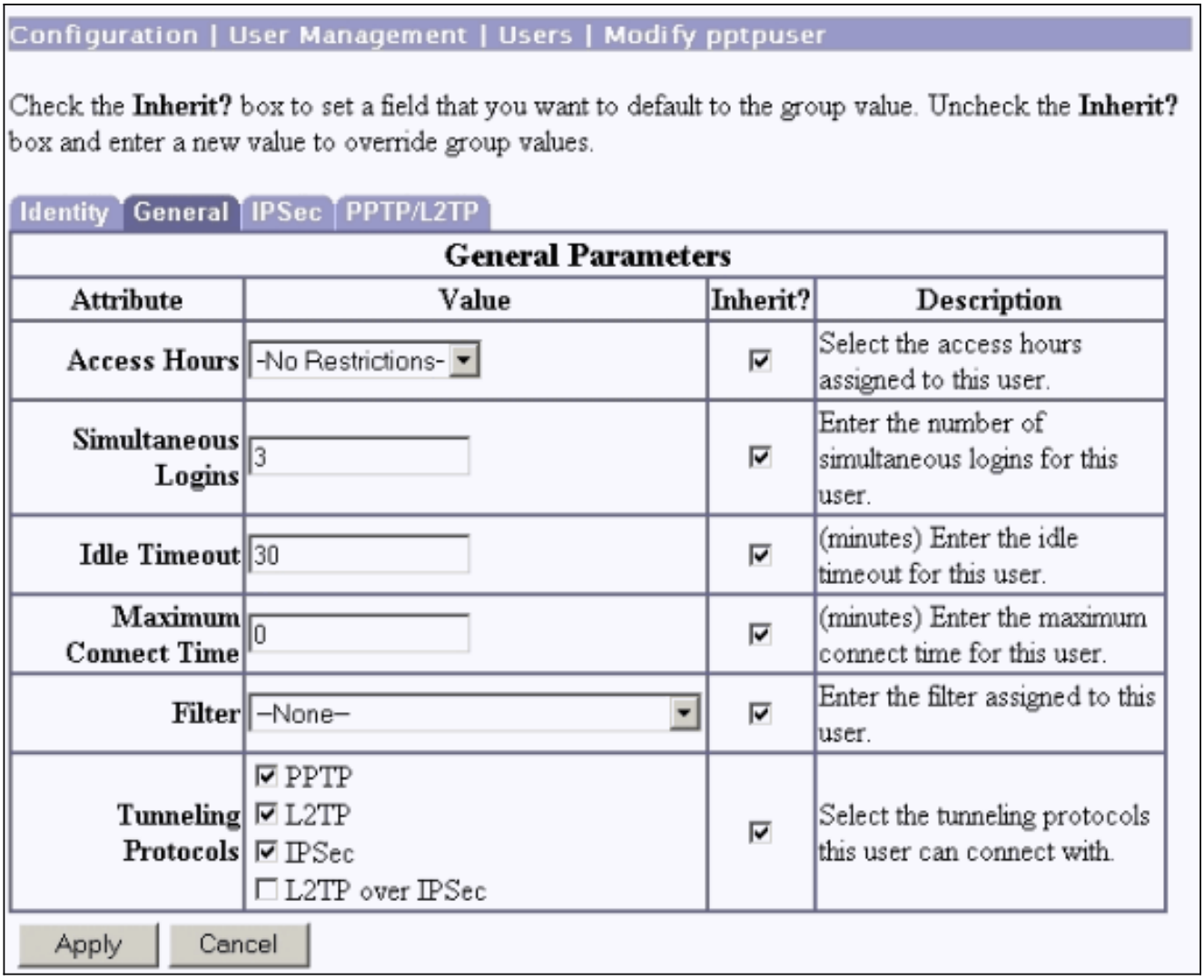
PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☑	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☐ Required ☐ Require Stateless ☐ 40-bit ☐ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

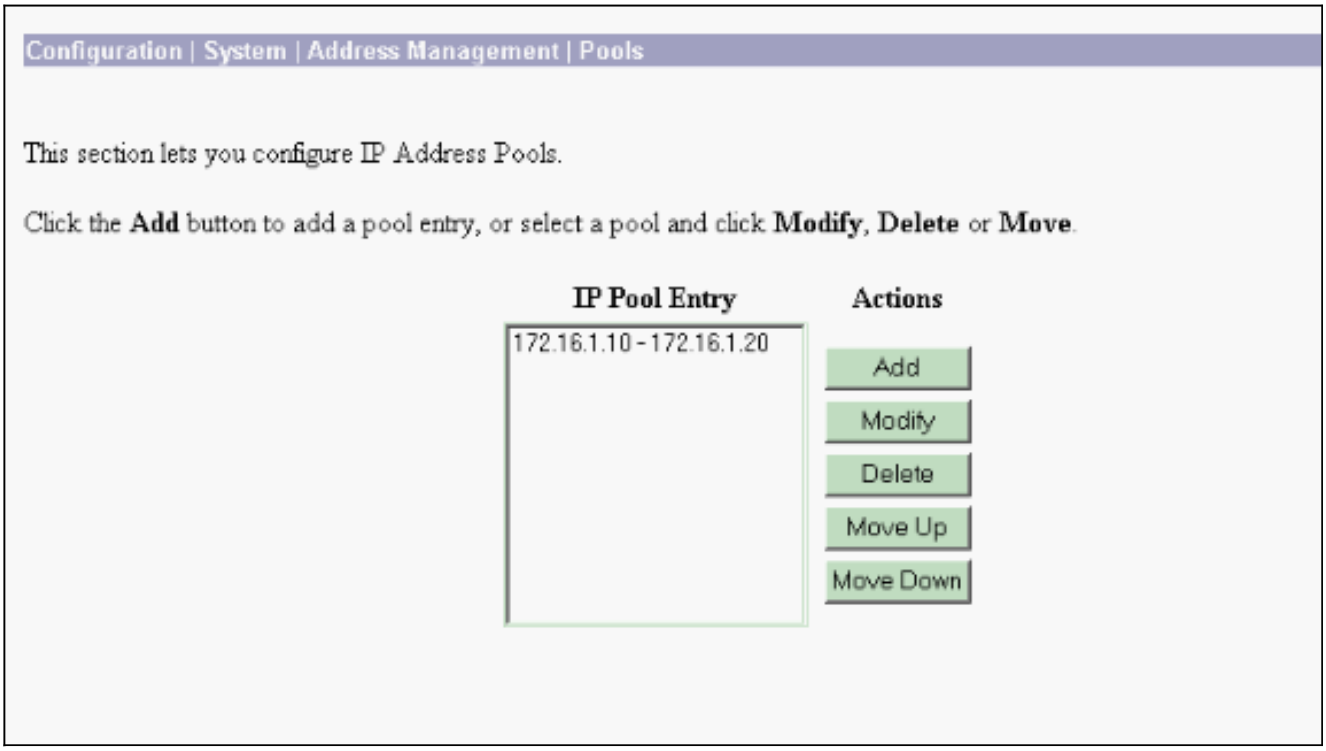
7. Sélectionnez **Configuration > User Management > Users > Add**, et configurez un utilisateur local (appelé « pptpuser ») avec le mot de passe **cisco123** pour l'authentification PPTP. Placez l'utilisateur dans le groupe pptpgroup précédemment défini :



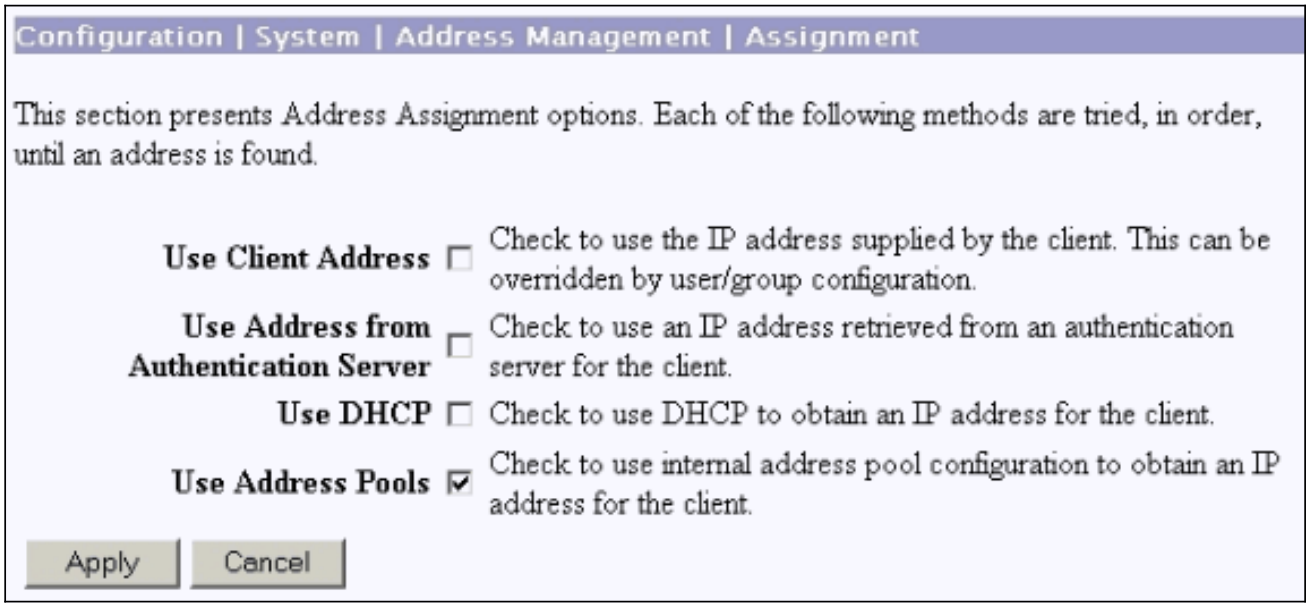
8. Sous l'onglet Général de l'utilisateur, vérifiez que l'option **PPTP** est activée dans les protocoles de tunnellisation.



9. Sélectionnez **Configuration > System > Address Management > Pools** pour définir un pool d'adresses pour la gestion des adresses.



10. Sélectionnez **Configuration > System > Address Management > Assignment** et demandez au concentrateur VPN d'utiliser le pool d'adresses.



Configuration du client PPTP Microsoft

Remarque : Aucune des informations disponibles ici sur la configuration des logiciels Microsoft ne contient de garantie ou de support pour les logiciels Microsoft. La prise en charge des logiciels Microsoft est disponible auprès de Microsoft .

Windows 98 - Installation et configuration de la fonctionnalité PPTP

Installer

Suivez ces étapes pour installer la fonctionnalité PPTP.

1. Sélectionnez **Démarrer > Paramètres > Panneau de configuration > Ajouter un nouveau matériel (Suivant) > Sélectionner dans la liste > Carte réseau (Suivant)**.
2. Sélectionnez **Microsoft** dans le panneau de gauche et **Microsoft VPN Adapter** dans le panneau de droite.

Configuration

Complétez ces étapes pour configurer la fonctionnalité PPTP.

1. Sélectionnez **Démarrer > Programmes > Accessoires > Communications > Dial Up Networking > Make new connection**.
2. Connectez-vous à l'aide de l'adaptateur VPN Microsoft à l'invite Select a device. L'adresse IP du serveur VPN est le point de terminaison du tunnel 3000.

L'authentification par défaut de Windows 98 utilise le chiffrement par mot de passe (par exemple, CHAP ou MSCHAP). Afin de désactiver initialement ce chiffrement, sélectionnez **Propriétés > Types de serveur**, puis décochez les cases **Mot de passe chiffré** et **Exiger le chiffrement des données**.

Windows 2000 : configuration de la fonctionnalité PPTP

Complétez ces étapes pour configurer la fonctionnalité PPTP.

1. Sélectionnez **Démarrer > Programmes > Accessoires > Communications > Connexions réseau et accès commuté > Créer une nouvelle connexion**.
2. Cliquez sur **Suivant**, puis sélectionnez **Connexion à un réseau privé via Internet > Composer une connexion avant** (ne sélectionnez pas cette option si vous utilisez un réseau local).
3. Cliquez de nouveau sur **Suivant**, puis saisissez le nom d'hôte ou l'adresse IP du point de terminaison du tunnel, qui est l'interface externe du concentrateur VPN 3000. Dans cet exemple, l'adresse IP est 161.44.17.1.

Sélectionnez **Propriétés > Sécurité pour la connexion > Avancé** pour ajouter un type de mot de passe en tant que PAP. La valeur par défaut est MSCHAP et MSCHAPv2, et non CHAP ou PAP.

Le chiffrement des données est configurable dans cette zone. Vous pouvez le désactiver initialement.

Windows NT

Vous pouvez accéder aux informations relatives à la configuration des clients Windows NT pour PPTP sur le site Web de Microsoft.

Windows Vista

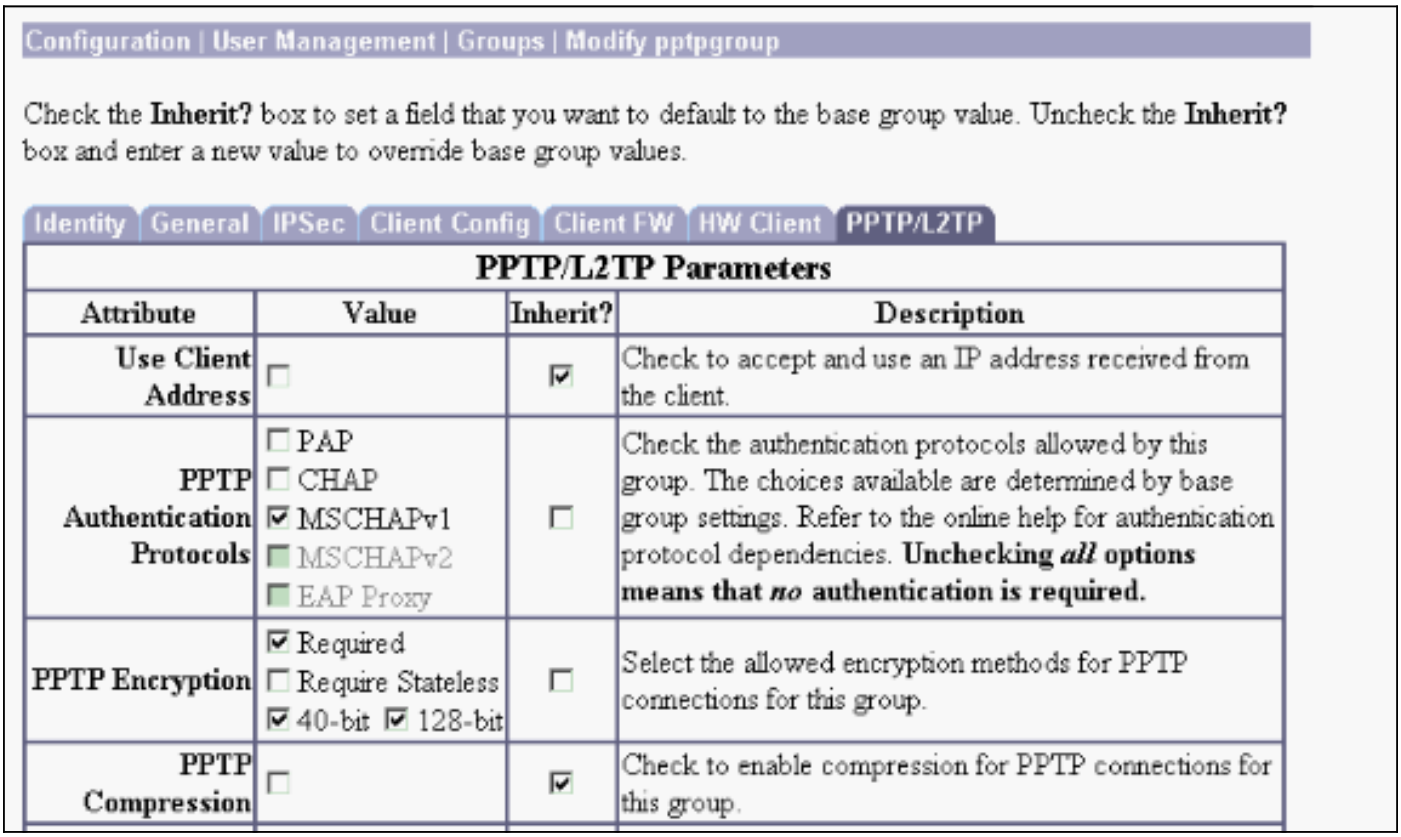
Complétez ces étapes pour configurer la fonctionnalité PPTP.

1. Àpartir du bouton **Démarrer**, sélectionnez **Se connecter à**.
2. Choisissez **Configurer une connexion ou un réseau**.
3. Choisissez **Se connecter à un lieu de travail** et cliquez sur **Suivant**.

4. Choisissez **Utiliser ma connexion Internet (VPN)**.**Remarque :** Si vous êtes invité à indiquer « Voulez-vous utiliser une connexion déjà existante », sélectionnez **Non, créez une nouvelle connexion** et cliquez sur **Suivant**.
5. Dans le champ **Adresse Internet**, tapez **pptp.vpn.univ.edu**, par exemple.
6. Dans le champ **Nom de la destination**, tapez **UNIVVPN**, par exemple.
7. Dans le champ **Nom d'utilisateur**, saisissez votre ID de connexion UNIV. Votre ID de connexion UNIV fait partie de votre adresse e-mail avant **@univ.edu**.
8. Dans le champ **Mot de passe**, saisissez votre mot de passe UNIV Logon ID.
9. Cliquez sur le bouton **Créer**, puis sur le bouton **Fermer**.
10. Afin de vous connecter au serveur VPN après avoir créé la connexion VPN, cliquez sur Démarrer, puis sur **Se connecter à**.
11. Choisissez la connexion VPN dans la fenêtre et cliquez sur **Connect**.

Ajouter MPPE (Encryption)

Assurez-vous que la connexion PPTP fonctionne sans chiffrement avant d'ajouter le chiffrement. Par exemple, cliquez sur le bouton **Connect** sur le client PPTP pour vous assurer que la connexion est terminée. Si vous décidez d'exiger le chiffrement, l'authentification MSCHAP doit être utilisée. Sur le VPN 3000, sélectionnez **Configuration > User Management > Groups**. Ensuite, sous l'onglet PPTP/L2TP du groupe, décochez **PAP**, cochez **MSCHAPv1** et cochez **Obligatoire pour le chiffrement PPTP**.



Configuration | User Management | Groups | Modify pptpgroup

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

PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☐ PAP ☐ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☐	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. **Unchecking *all* options means that *no* authentication is required.**
PPTP Encryption	☑ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

Le client PPTP doit être reconfiguré pour le chiffrement de données facultatif ou obligatoire et MSCHAPv1 (s'il s'agit d'une option).

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

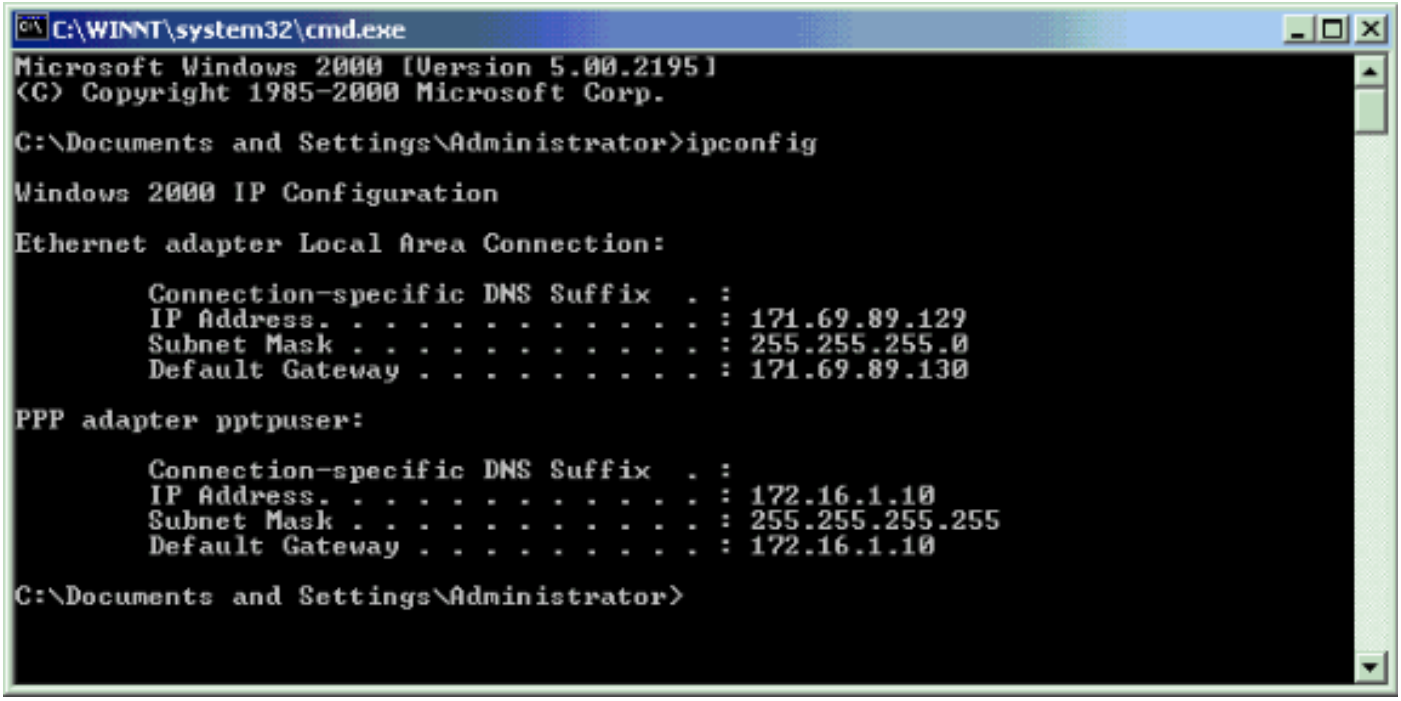
Vérifier le concentrateur VPN

Vous pouvez démarrer la session PPTP en composant le client PPTP créé précédemment dans la section Configuration du client PPTP Microsoft.

Utilisez la fenêtre Administration >Admin Sessions sur le concentrateur VPN pour afficher les paramètres et les statistiques de toutes les sessions PPTP actives.

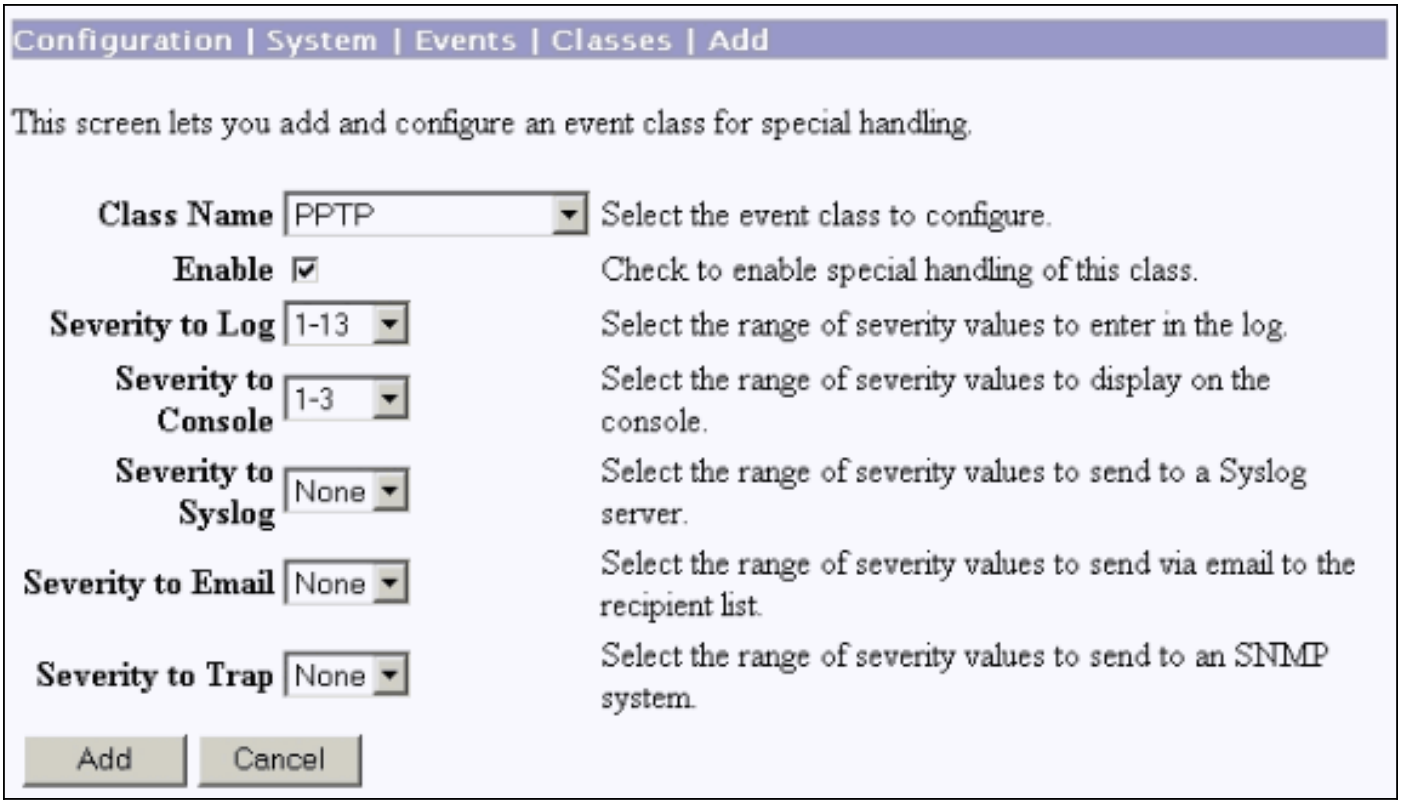
Vérification du PC

Exécutez la commande **ipconfig** en mode de commande du PC pour vérifier que le PC a deux adresses IP. L'une est sa propre adresse IP et l'autre est attribuée par le concentrateur VPN à partir du pool d'adresses IP. Dans cet exemple, l'adresse IP 172.16.1.10 est l'adresse IP attribuée par le concentrateur VPN.

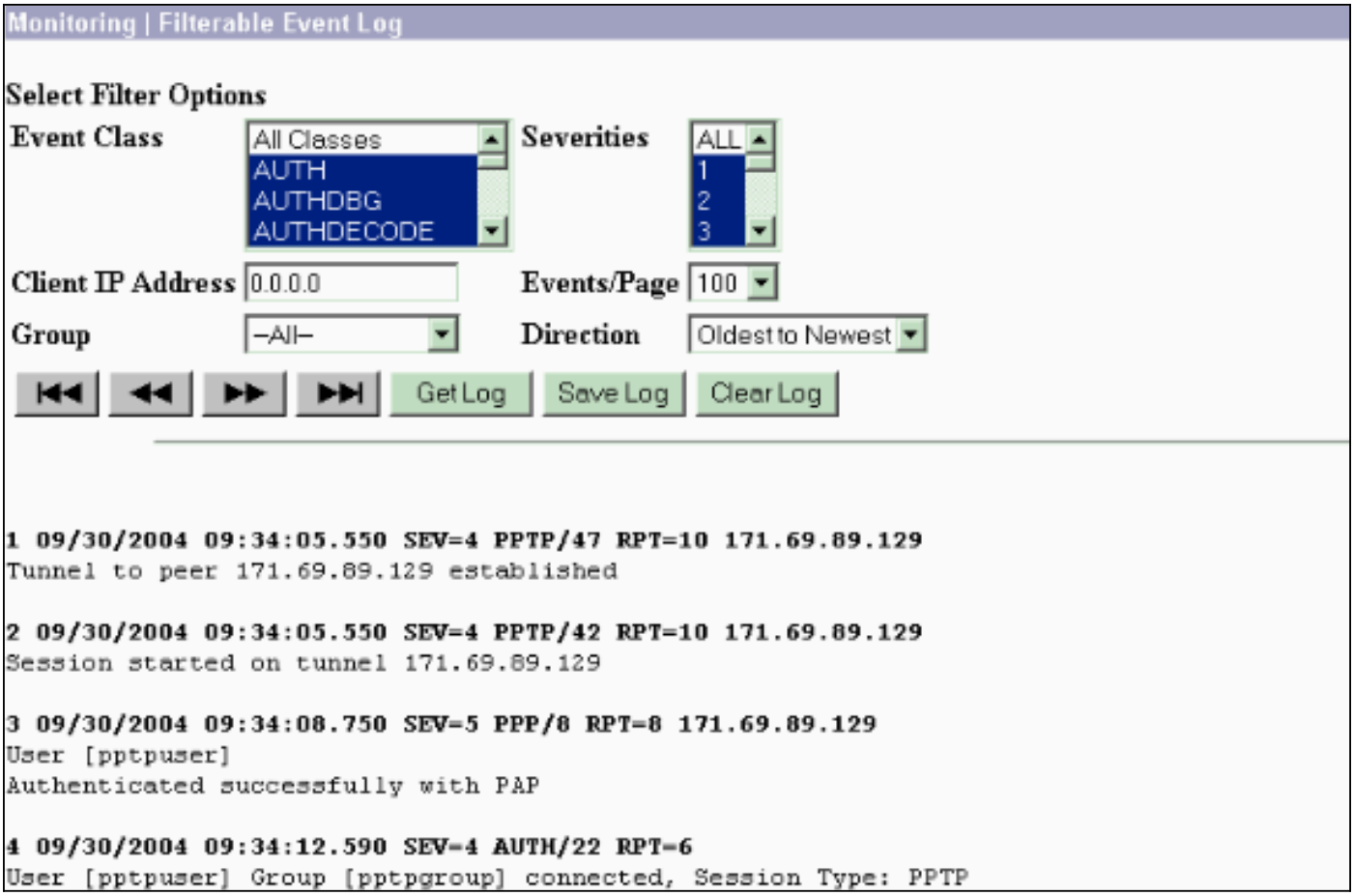


Déboguer

Si la connexion ne fonctionne pas, le débogage de la classe d'événements PPTP peut être ajouté au concentrateur VPN. Sélectionnez **Configuration > System > Events > Classes > Modify** ou **Add** (voir ici). Les classes d'événements PPTPDBG et PPTPDECODE sont également disponibles, mais peuvent fournir trop d'informations.



Le journal des événements peut être extrait de **Monitoring > Filterable Event Log**.



Débogage VPN 3000 - Bonne authentification

```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
```

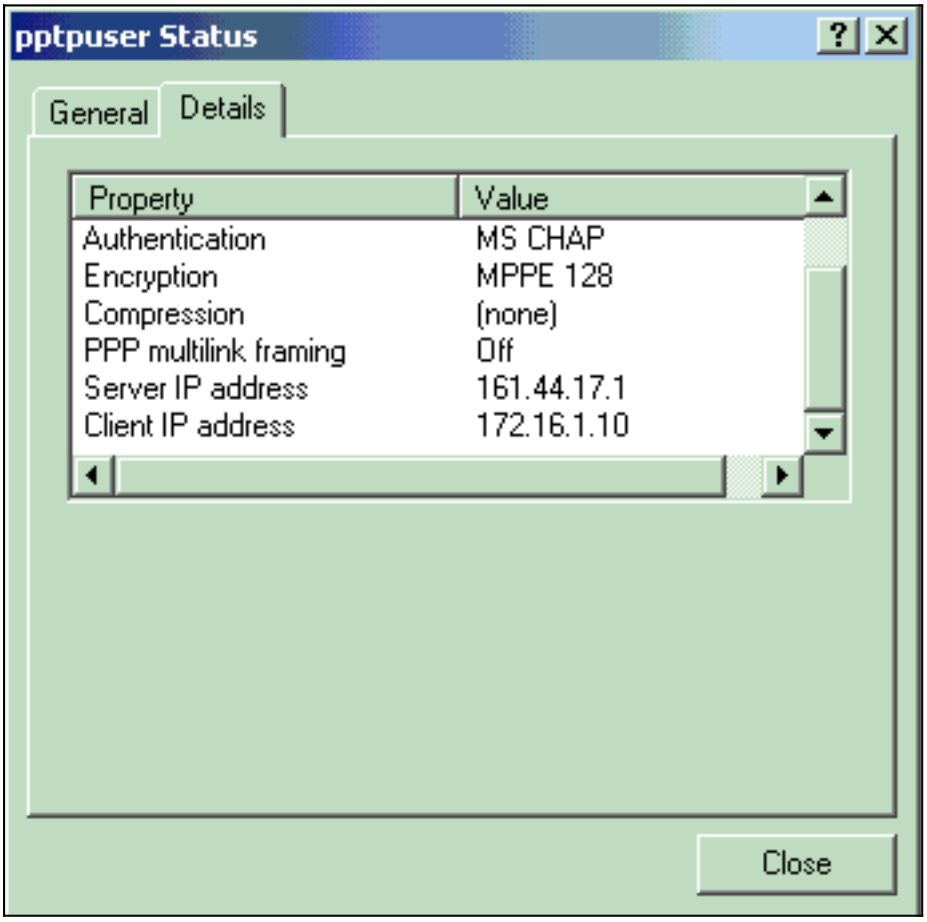
```
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
   User [pptpuser]
   Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
   User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

Cliquez sur la fenêtre **Détails** de l'état utilisateur PPTP pour vérifier les paramètres sur le PC Windows.



Dépannage

Voici quelques erreurs possibles :

- **Nom d'utilisateur ou mot de passe incorrect**Sortie de débogage du concentrateur VPN 3000 :

```
1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 established

2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
   Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
   Authentication rejected: Reason = User was not found
   handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
   User [pptpusers]
```

```
   disconnected.. failed authentication ( MSCHAP-V1 )

6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
   Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
   reason: Error (No additional info)

8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
   Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)
```

Message que l'utilisateur voit (depuis Windows 98) :

```
Error 691: The computer you have dialed in to has denied access
because the username and/or password is invalid on the domain.
```

Message que l'utilisateur voit (depuis Windows 2000) :

```
Error 691: Access was denied because the username and/or
password was invalid on the domain.
```

- **« Encryption Required » est sélectionné sur le PC, mais pas sur le concentrateur VPN**Message que l'utilisateur voit (depuis Windows 98) :

```
Error 742: The computer you're dialing in to does not support the data
encryption requirements specified.
Please check your encryption settings in the properties of the connection.
If the problem persists, contact your network administrator.
```

Message que l'utilisateur voit (depuis Windows 2000) :

```
Error 742: The remote computer does not support
the required data encryption type
```

- **« Encryption Required » (128 bits) est sélectionné sur le concentrateur VPN avec un PC qui prend uniquement en charge le cryptage 40 bits**Sortie de débogage du concentrateur VPN 3000 :

```
4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [ pptpuser ] disconnected.
PPTP Encryption configured as REQUIRED.. remote client not supporting it.
```

Message que l'utilisateur voit (depuis Windows 98) :

```
Error 742:  The remote computer does not support
the required data encryption type.
```

Message que l'utilisateur voit (depuis Windows 2000) :

```
Error 645 Dial-Up Networking could not complete the connection to the server.
Check your configuration and try the connection again.
```

- **Le concentrateur VPN 3000 est configuré pour MSCHAPv1 et le PC est configuré pour PAP, mais ils ne peuvent pas convenir d'une méthode d'authentification**Sortie de débogage du concentrateur VPN 3000 :

```
8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129

User [pptpuser] disconnected. Authentication protocol not allowed.
```

Message que l'utilisateur voit (depuis Windows 2000) :

```
Error 691:  Access was denied because the username and/or password
was invalid on the domain.
```

Problèmes Microsoft possibles à résoudre

- **Comment maintenir des connexions RAS actives après fermeture de session**Lorsque vous vous déconnectez d'un client Windows Remote Access Service (RAS), toutes les connexions RAS sont automatiquement déconnectées. Activez la clé **KeepRasConnections** dans le Registre sur le client RAS pour rester connecté après vous être déconnecté. Référez-vous à l'article de la Base de connaissances Microsoft - 158909 pour plus d'informations.
- **L'utilisateur n'est pas alerté en ouvrant une session avec les informations d'identification mises en cache**Les symptômes de ce problème sont lorsque vous essayez de vous connecter à un domaine à partir d'une station de travail Windows ou d'un serveur membre et qu'un contrôleur de domaine est introuvable et qu'aucun message d'erreur n'est affiché. Au lieu de

cela, vous ouvrez une session sur l'ordinateur local à l'aide des informations d'identification mises en cache. Référez-vous à l'article de la Base de connaissances Microsoft - 242536 pour plus d'informations.

- **Procédures pour écrire un fichier LMHOSTS pour la validation de domaine et autres problèmes de résolution de noms**Il peut y avoir des cas où vous rencontrez des problèmes de résolution de noms sur votre réseau TCP/IP et que vous devez utiliser des fichiers LMHOSTS pour résoudre des noms NetBIOS. Cet article décrit la méthode appropriée utilisée pour créer un fichier LMHOSTS afin d'aider à la résolution de noms et à la validation de domaine. Référez-vous à Article de la Base de connaissances Microsoft - 180094 pour plus d'informations.

Informations connexes

- RFC 2637 : Protocole de tunnellisation point à point (PPTP)
- Cisco Secure ACS pour les pages d'assistance Windows
- À quel moment le chiffrement PPTP est-il pris en charge sur un concentrateur Cisco VPN 3000 ?
- Configuration du concentrateur VPN 3000 et du protocole PPTP avec l'authentification Cisco Secure ACS pour Windows RADIUS
- Pages d'assistance du concentrateur Cisco VPN 3000
- Pages d'assistance client Cisco VPN 3000
- Pages d'assistance produit IPSec (IP Security)
- Pages d'assistance produit PPTP
- Support et documentation techniques - Cisco Systems