Configuration du concentrateur Cisco VPN 3000 avec Microsoft RADIUS

Contenu

Introduction

Microsoft Internet Authentication Server (IAS) et Microsoft Commercial Internet System (MCIS 2.0) sont actuellement disponibles. Le serveur Microsoft RADIUS est pratique car il utilise Active Directory sur le contrôleur de domaine principal pour sa base de données utilisateur. Vous n'avez plus besoin de gérer une base de données distincte. Il prend également en charge le cryptage 40 bits et 128 bits pour les connexions VPN PPTP (Point-to-Point Tunneling Protocol). Reportez-vous à la Liste de contrôle Microsoft : Configuration d'IAS pour la documentation d'accès par ligne commutée et VPN pour plus d'informations.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Installation et configuration du serveur RADIUS sous Windows 2000 et Windows 2003

Installer le serveur RADIUS

Si le serveur RADIUS (IAS) n'est pas déjà installé, procédez comme suit pour l'installer. Si le serveur RADIUS est déjà installé, passez aux étapes de configuration.

1. Insérez le disque compact de Windows Server et démarrez le programme d'installation.
2. Cliquez sur **Installer des composants complémentaires**, puis sur **Ajouter/Supprimer des composants Windows**.
3. Dans Composants, cliquez sur **Services de mise en réseau** (mais ne cochez pas ou ne désactivez pas la case), puis cliquez sur **Détails**.
4. Cochez **Internet Authentication Service** et cliquez sur **OK**.
5. Cliquez sur **Next** (Suivant).

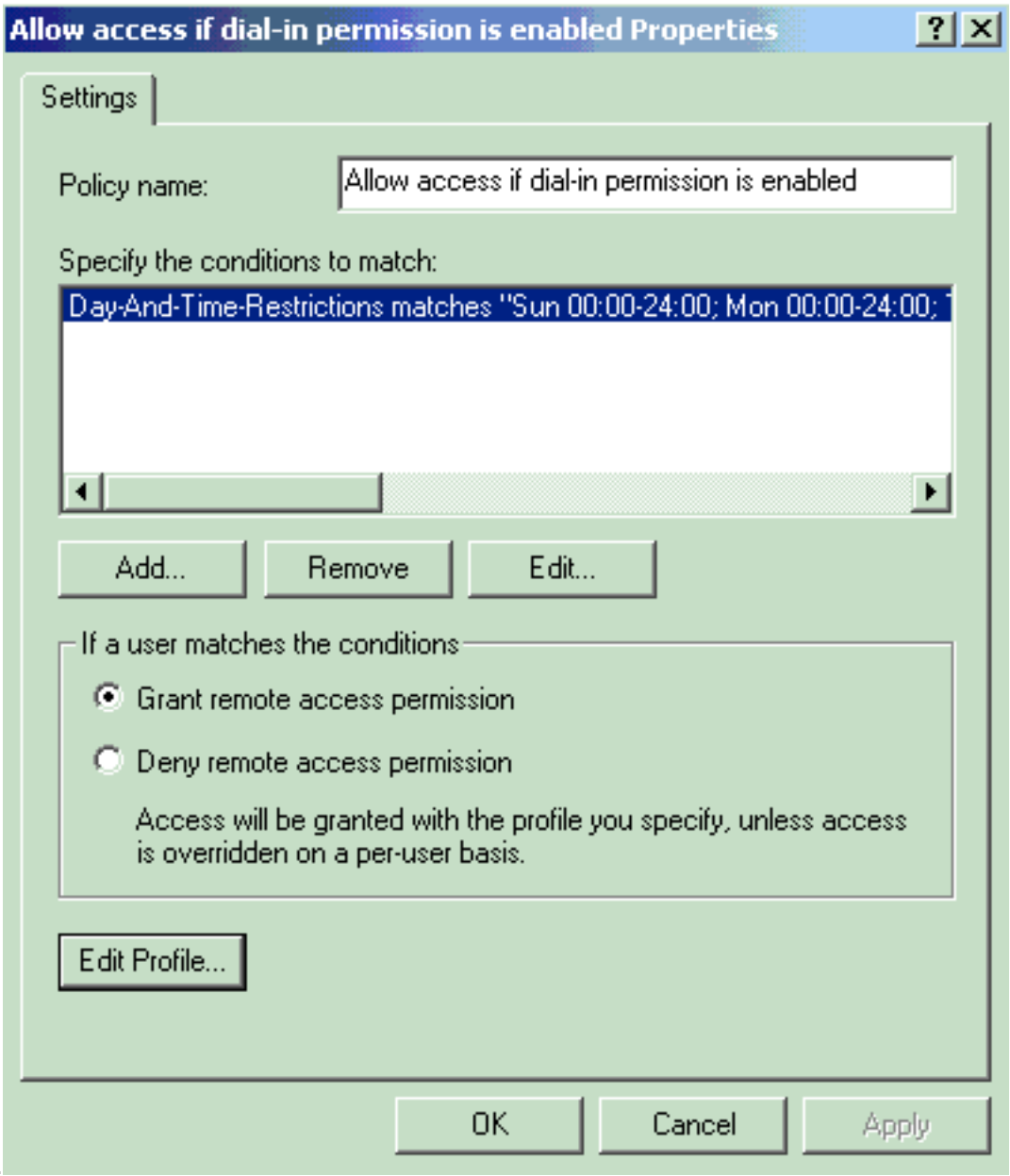
Configurer Microsoft Windows 2000 Server avec IAS

Complétez ces étapes afin de configurer le serveur RADIUS (IAS) et de démarrer le service afin de le rendre disponible pour authentifier les utilisateurs sur le concentrateur VPN.

1. Choisissez **Démarrer > Programmes > Outils d'administration > Service d'authentification Internet**.
2. Cliquez avec le bouton droit sur **Internet Authentication Service**, puis cliquez sur **Properties** dans le sous-menu qui apparaît.
3. Accédez à l'onglet RADIUS afin d'examiner les paramètres des ports.Si vos ports UDP (User Datagram Protocol) d'authentification RADIUS et de comptabilité RADIUS diffèrent des valeurs par défaut fournies (1812 et 1645 pour l'authentification, 1813 et 1646 pour la comptabilité) dans Authentication and Accounting, saisissez vos paramètres de port. Cliquez sur **OK quand vous avez terminé.Remarque :** Ne modifiez pas les ports par défaut. Séparez les ports à l'aide de virgules pour utiliser plusieurs paramètres de port pour les demandes d'authentification ou de comptabilité.
4. Cliquez avec le bouton droit sur **Clients** et choisissez **Nouveau Client** afin d'ajouter le concentrateur VPN en tant que client AAA (Authentication, Authorization, and Accounting) au serveur RADIUS (IAS).**Remarque :** si la redondance est configurée entre deux concentrateurs Cisco VPN 3000, le concentrateur Cisco VPN 3000 de secours doit également être ajouté au serveur RADIUS en tant que client RADIUS.
5. Entrez un nom convivial et sélectionnez **Protocol Radius**.
6. Définissez le concentrateur VPN avec une adresse IP ou un nom DNS dans la fenêtre suivante.
7. Choisissez **Cisco** dans la barre de défilement Client-Vendor.
8. Entrez un secret partagé.**Note :** Vous devez vous rappeler le secret *exact* que vous utilisez.

Vous avez besoin de ces informations pour configurer le concentrateur VPN.

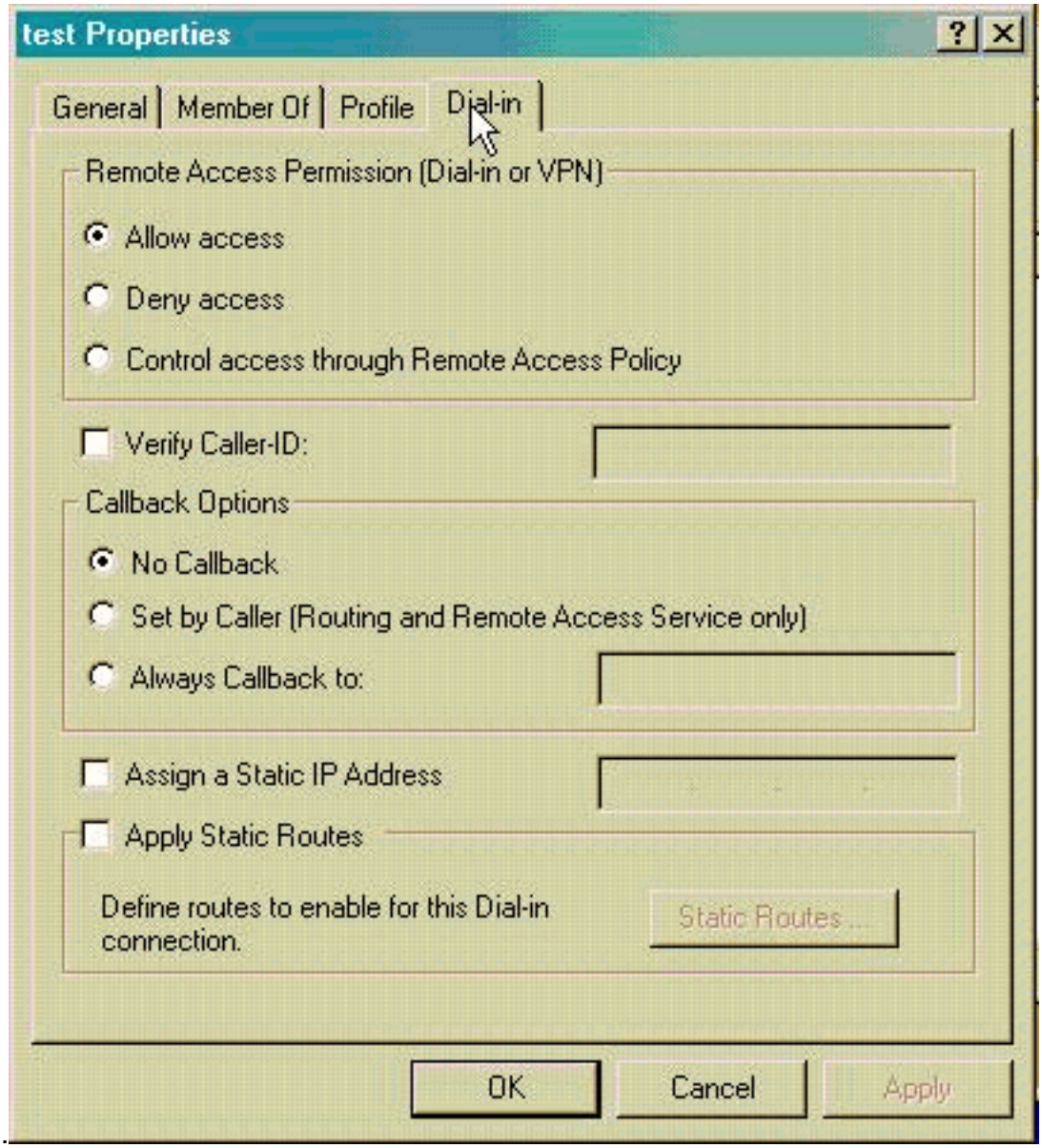
9. **Cliquez sur Finish.**
10. Double-cliquez sur **Stratégies d'accès à distance** et double-cliquez sur la stratégie qui apparaît dans la partie droite de la fenêtre.**Remarque :** après avoir installé IAS, une stratégie d'accès à distance doit déjà exister.Sous Windows 2000, l'autorisation est accordée en fonction des propriétés de connexion d'un compte d'utilisateur et des stratégies d'accès à distance. Les stratégies d'accès à distance sont un ensemble de conditions et de paramètres de connexion qui donnent aux administrateurs réseau plus de flexibilité pour autoriser les tentatives de connexion. Le service Routage et accès à distance de Windows 2000 et le service IAS de Windows 2000 utilisent tous deux des stratégies d'accès à distance pour déterminer s'il faut accepter ou rejeter les tentatives de connexion. Dans les deux cas, les stratégies d'accès à distance sont stockées localement. Reportez-vous à la documentation IAS de Windows 2000 pour plus d'informations sur le traitement des tentatives de connexion.



11. Choisissez **Octroyer l'autorisation d'accès distant** et cliquez sur **Modifier le profil** afin de configurer les propriétés de numérotation.
12. Sélectionnez le protocole à utiliser pour l'authentification dans l'onglet Authentification. Vérifiez **Microsoft Encrypted Authentication version 2** et désélectionnez tous les autres

protocoles d'authentification.**Remarque :** les paramètres de ce profil de numérotation doivent correspondre aux paramètres de la configuration du concentrateur VPN 3000 et du client de numérotation. Dans cet exemple, l'authentification MS-CHAPv2 sans chiffrement PPTP est utilisée.

13. Dans l'onglet Chiffrement, cochez **No Encryption** only.
14. Cliquez sur **OK** afin de fermer le profil de numérotation, puis cliquez sur **OK** afin de fermer la fenêtre de stratégie d'accès à distance.
15. Cliquez avec le bouton droit sur **Internet Authentication Service** et cliquez sur **Start Service** dans l'arborescence de la console.**Remarque :** Vous pouvez également utiliser cette fonction pour arrêter le service.
16. Complétez ces étapes afin de modifier les utilisateurs pour autoriser la connexion.Choisissez **Console > Ajouter/Supprimer un composant logiciel enfichable**.Cliquez sur **Ajouter** et choisissez **le composant logiciel enfichable Utilisateurs et groupes locaux**.Cliquez sur **Add**.Veillez à sélectionner **Ordinateur local**Cliquez sur **Terminer** et **OK**.
17. Développez **Utilisateurs et groupes locaux** et cliquez sur le dossier **Utilisateurs** dans le volet gauche. Dans le volet droit, double-cliquez sur l'utilisateur (utilisateur VPN) auquel vous souhaitez autoriser l'accès.
18. Accédez à l'onglet Composer et sélectionnez **Autoriser l'accès** sous Autorisation d'accès à distance (Composer ou



VPN).

19. Cliquez sur **Apply** et **OK** pour terminer l'action. Vous pouvez fermer la fenêtre Console Management et enregistrer la session, si vous le souhaitez.Les utilisateurs que vous avez modifiés peuvent désormais accéder au concentrateur VPN avec le client VPN. N'oubliez pas que le serveur IAS authentifie uniquement les informations utilisateur. Le concentrateur VPN effectue toujours l'authentification de groupe.

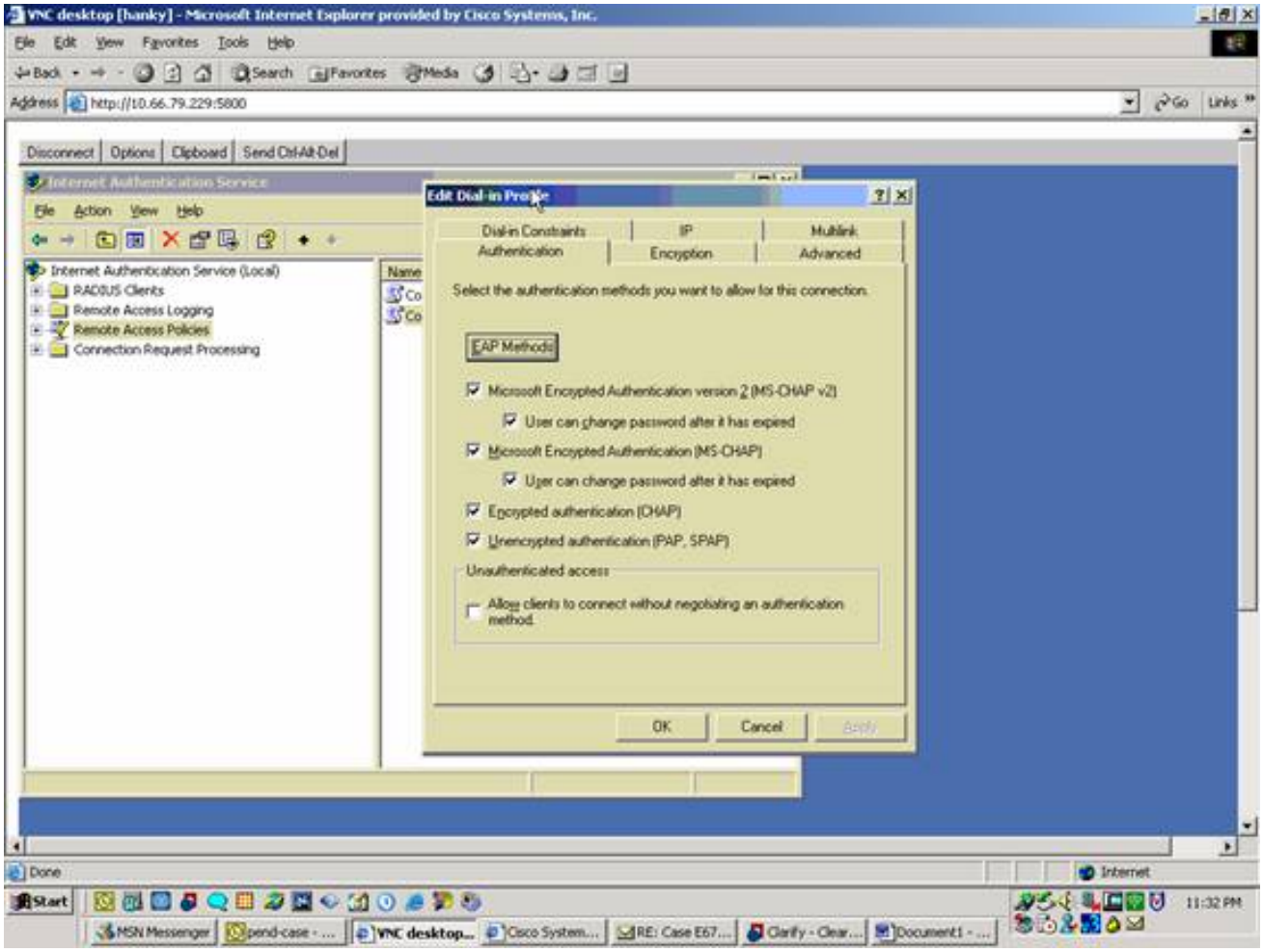
Configurer Microsoft Windows 2003 Server avec IAS

Complétez ces étapes afin de configurer le serveur Microsoft Windows 2003 avec IAS.

Remarque : Ces étapes supposent que IAS est déjà installé sur l'ordinateur local. Sinon, ajoutez ce composant via **Control Panel > Add/Remove Programs**.

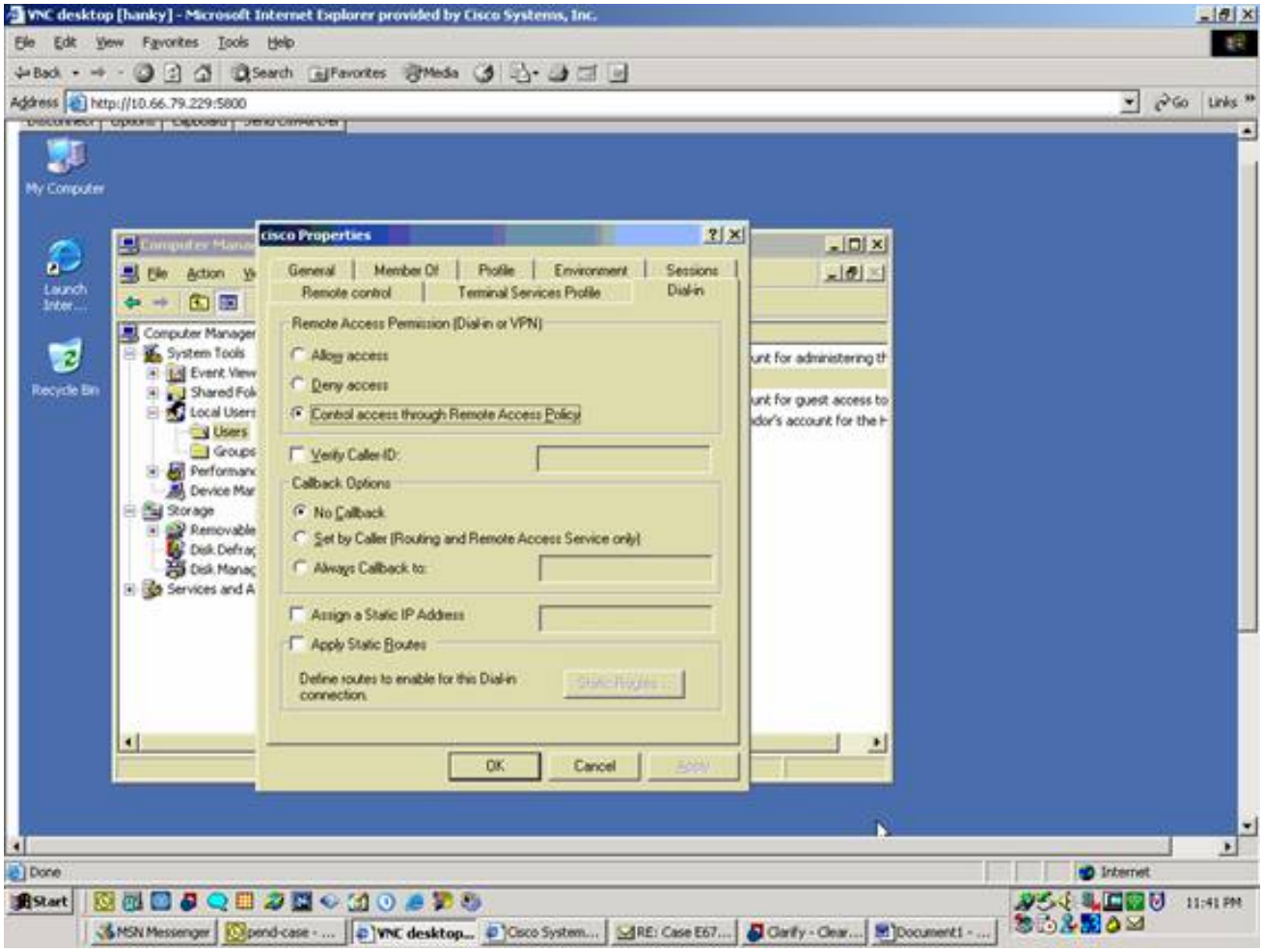
1. Choisissez **Outils d'administration > Service d'authentification Internet** et cliquez avec le bouton droit sur **Client RADIUS** afin d'ajouter un nouveau client RADIUS. Après avoir tapé les informations sur le client, cliquez sur **OK**.
2. Entrez un nom convivial.
3. Définissez le concentrateur VPN avec une adresse IP ou un nom DNS dans la fenêtre suivante.
4. Choisissez **Cisco** dans la barre de défilement Client-Vendor.

5. Entrez un secret partagé.**Note :** Vous devez vous rappeler le secret *exact* que vous utilisez. Vous avez besoin de ces informations pour configurer le concentrateur VPN.
6. Cliquez sur **OK pour terminer.**
7. Accédez à **Stratégies d'accès à distance**, cliquez avec le bouton droit sur **Connexions à d'autres serveurs d'accès**, puis sélectionnez **Propriétés**.
8. Choisissez **Accorder l'autorisation d'accès distant** et cliquez sur **Modifier le profil** afin de configurer les propriétés de numérotation.
9. Sélectionnez le protocole à utiliser pour l'authentification dans l'onglet Authentification. Vérifiez **Microsoft Encrypted Authentication version 2** et désélectionnez tous les autres protocoles d'authentification.**Remarque :** les paramètres de ce profil de numérotation doivent correspondre aux paramètres de la configuration du concentrateur VPN 3000 et du client de numérotation. Dans cet exemple, l'authentification MS-CHAPv2 sans chiffrement PPTP est utilisée.
10. Dans l'onglet Chiffrement, cochez **No Encryption** only.
11. Cliquez sur **OK quand vous avez terminé.**



12. Cliquez avec le bouton droit sur **Internet Authentication Service** et cliquez sur **Start Service** dans l'arborescence de la console.**Remarque :** Vous pouvez également utiliser cette fonction pour arrêter le service.
13. Choisissez **Outils d'administration > Gestion de l'ordinateur > Outils système > Utilisateurs et groupes locaux**, cliquez avec le bouton droit sur **Utilisateurs** et choisissez **Nouveaux utilisateurs** afin d'ajouter un utilisateur au compte d'ordinateur local.
14. Ajoutez un utilisateur avec le mot de passe Cisco vpnpassword et vérifiez ces informations de profil.Dans l'onglet General, assurez-vous que l'option **Password Never Expired** est sélectionnée au lieu de l'option User Must Change Password.Dans l'onglet Composer,

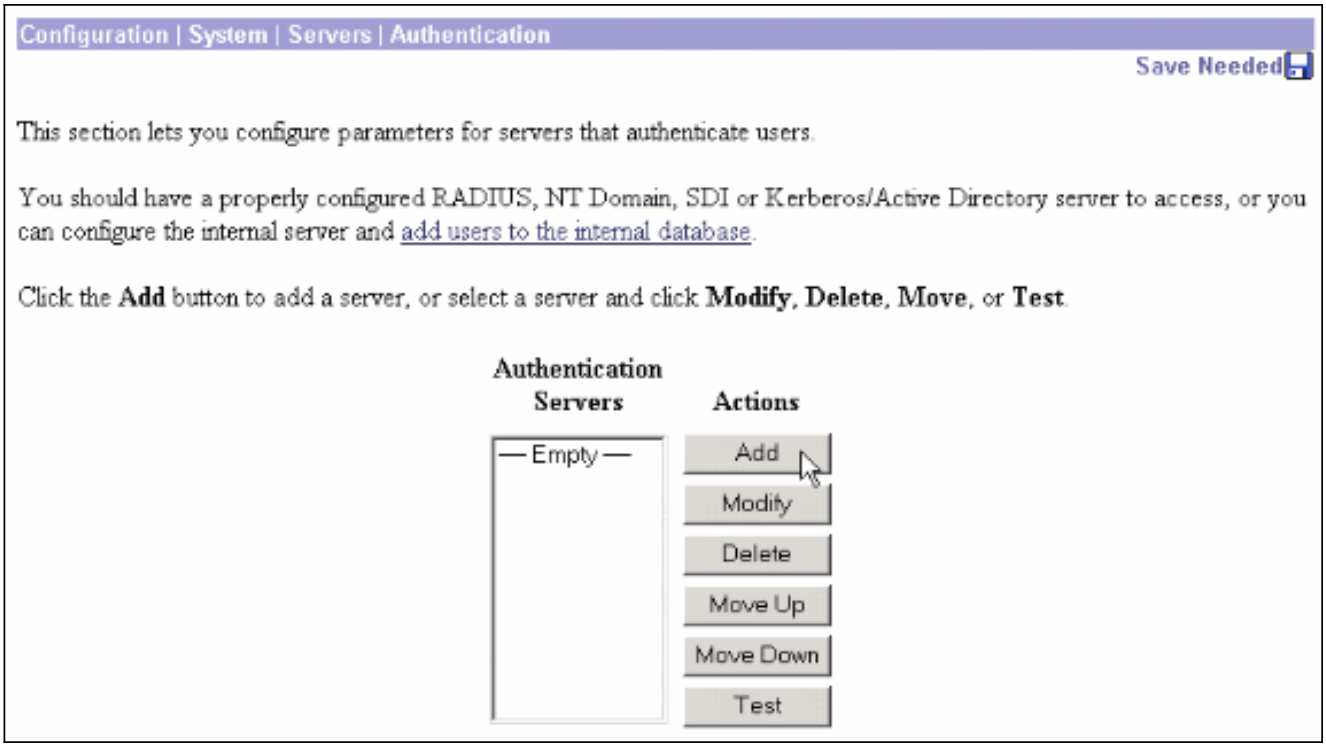
sélectionnez l'option **Autoriser l'accès** (ou laissez le paramètre par défaut de Contrôle de l'accès via la stratégie d'accès à distance).Cliquez sur **OK quand vous avez terminé.**



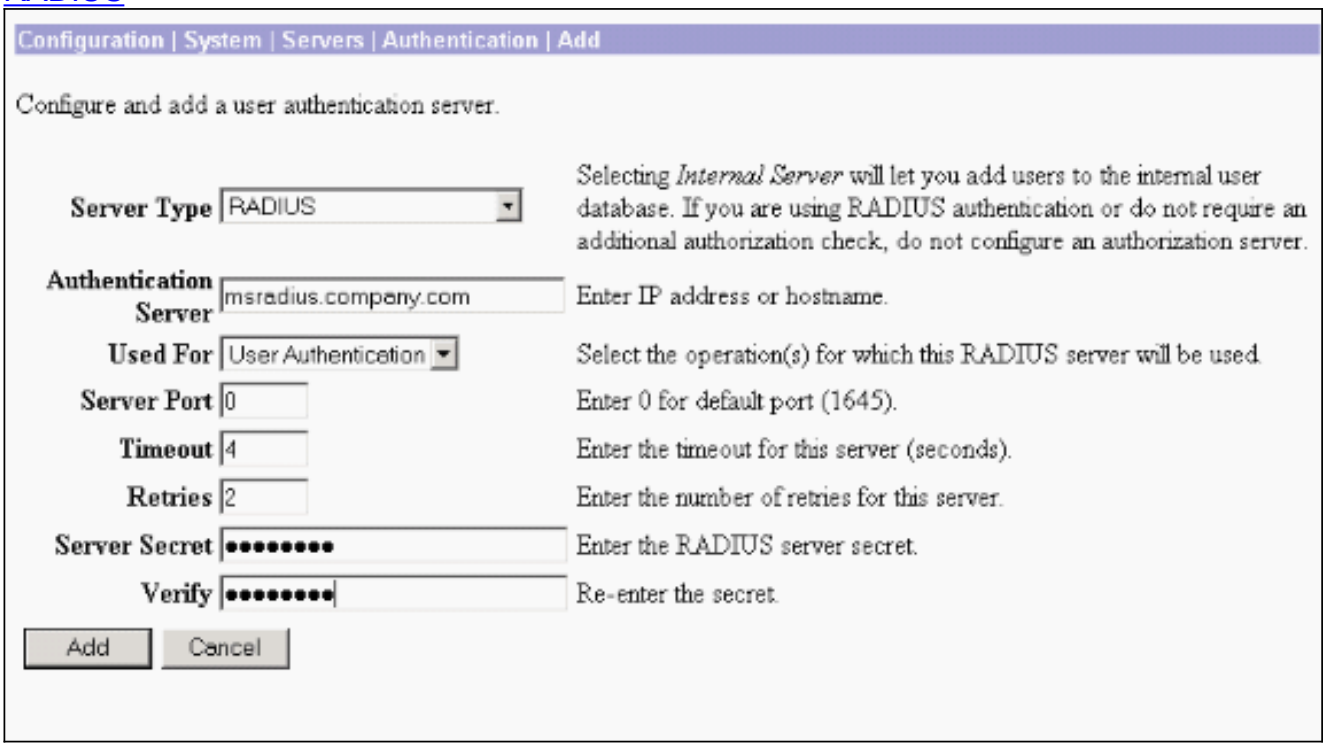
Configurer le concentrateur Cisco VPN 3000 pour l'authentification RADIUS

Complétez ces étapes afin de configurer le concentrateur Cisco VPN 3000 pour l'authentification RADIUS.

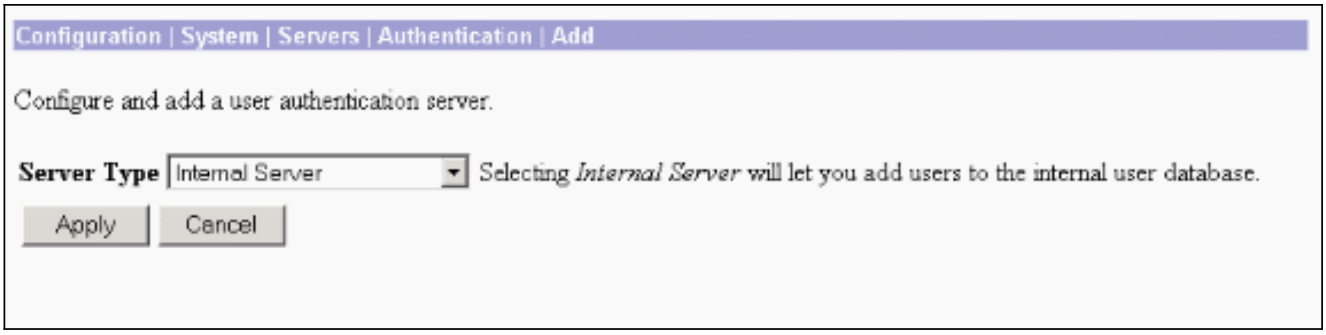
1. Connectez-vous au concentrateur VPN à l'aide de votre navigateur Web, puis sélectionnez **Configuration > System > Servers > Authentication** dans le menu de gauche.



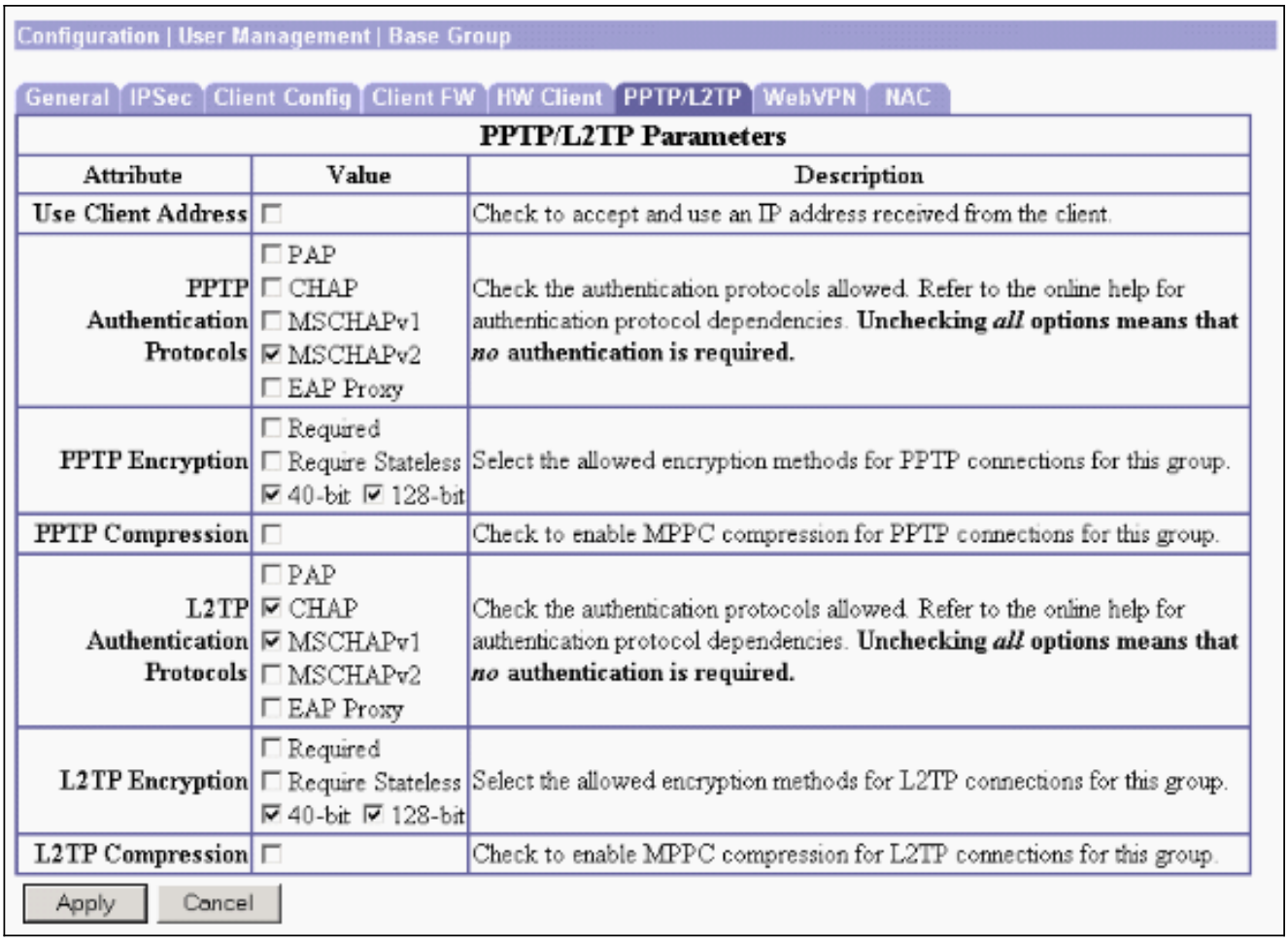
2. Cliquez sur **Add** et configurez ces paramètres.Type de serveur = RADIUSServeur d'authentification = adresse IP ou nom d'hôte de votre serveur RADIUS (IAS)Port du serveur = 0 (0=valeur par défaut=1 645)Secret du serveur = identique à l'étape 8 de la section [Configurer le serveur RADIUS]



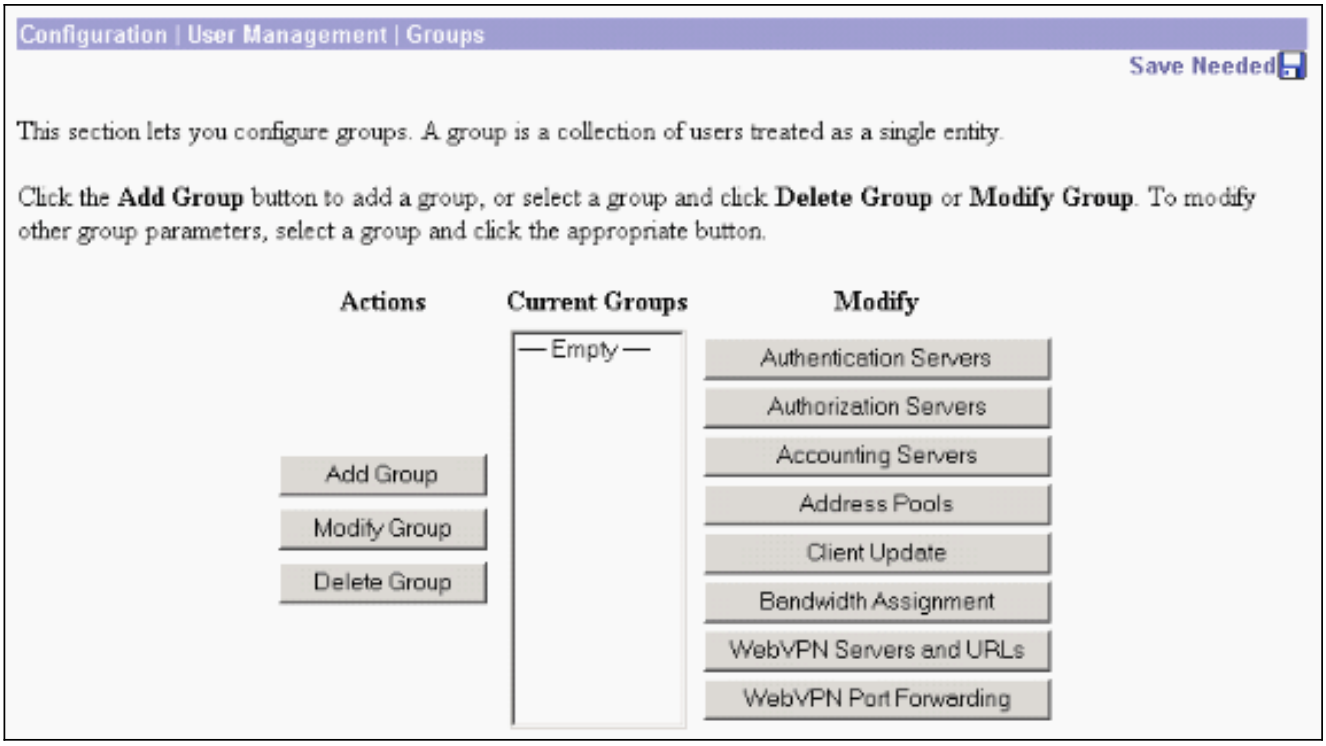
3. Cliquez sur **Add** afin d'ajouter les modifications à la configuration en cours.
4. Cliquez sur **Add**, choisissez **Internal Server** for Server Type, puis cliquez sur **Apply**.Vous en aurez besoin ultérieurement afin de configurer un groupe IPsec (vous n'aurez besoin que du type de serveur = Serveur interne).



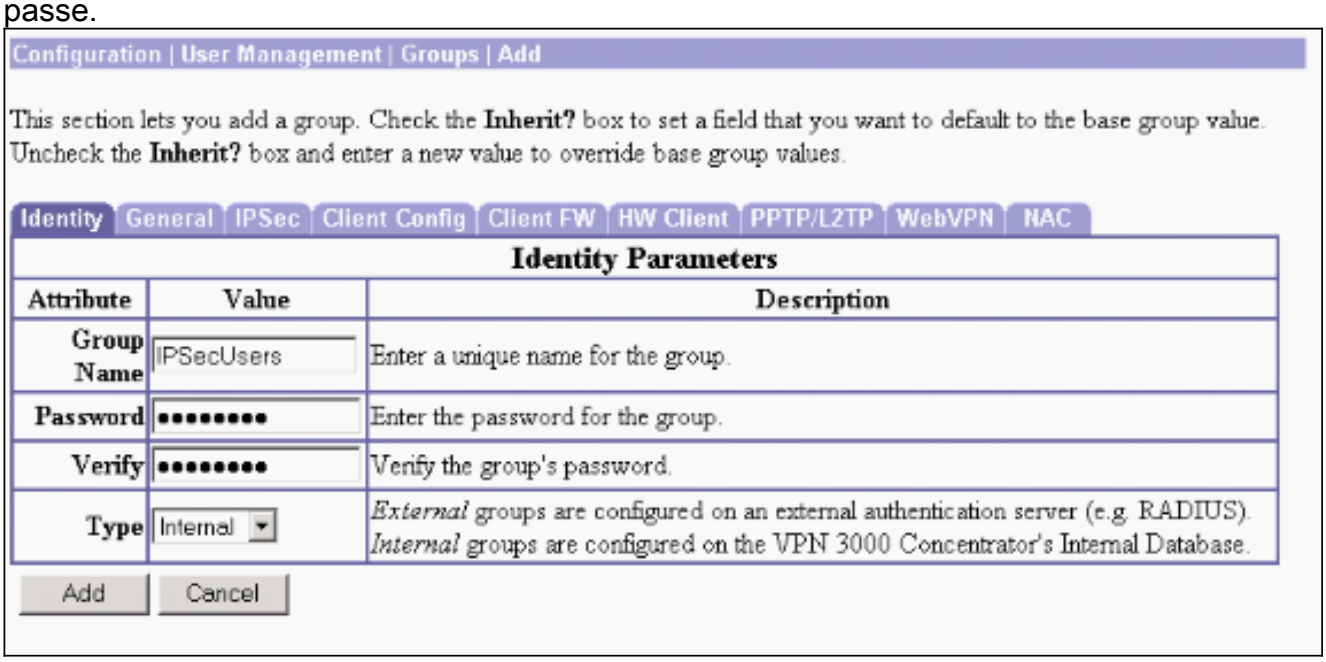
5. Configurez le concentrateur VPN pour les utilisateurs PPTP ou VPN Client.**PPTP**Complétez ces étapes afin de configurer pour les utilisateurs PPTP.Choisissez **Configuration > User Management > Base Group**, puis cliquez sur l'onglet **PPTP/L2TP**.Choisissez **MSCHAPv2** et décochez les autres protocoles d'authentification dans la section Protocoles d'authentification PPTP.



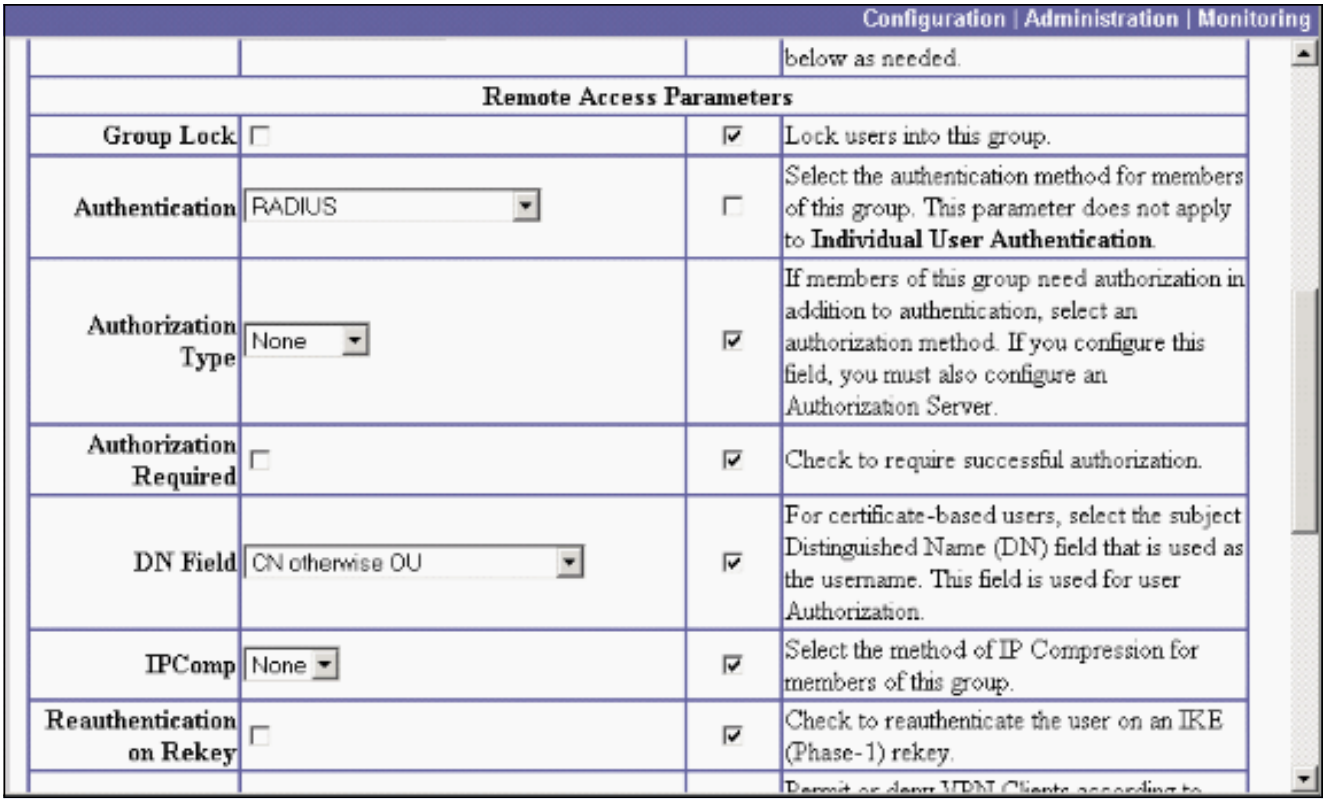
Cliquez sur **Apply** en bas de la page afin d'ajouter les modifications à la configuration en cours.Maintenant, lorsque les utilisateurs PPTP se connectent, ils sont authentifiés par le serveur RADIUS (IAS).**Client VPN**Complétez ces étapes afin de configurer pour les utilisateurs du client VPN.Choisissez **Configuration > User Management > Groups** et cliquez sur **Add** afin d'ajouter un nouveau
groupe.



Tapez un nom de groupe (par exemple, IPsecUsers) et un mot de passe.



Ce mot de passe est utilisé comme clé pré-partagée pour la négociation de tunnel.Accédez à l'onglet IPSec et définissez l'authentification sur **RADIUS**.



Cela permet aux clients IPsec d'être authentifiés via le serveur d'authentification RADIUS.Cliquez sur **Ajouter** en bas de la page afin d'ajouter les modifications à la configuration en cours.Maintenant, lorsque les clients IPsec se connectent et utilisent le groupe que vous avez configuré, ils sont authentifiés par le serveur RADIUS.

Vérification

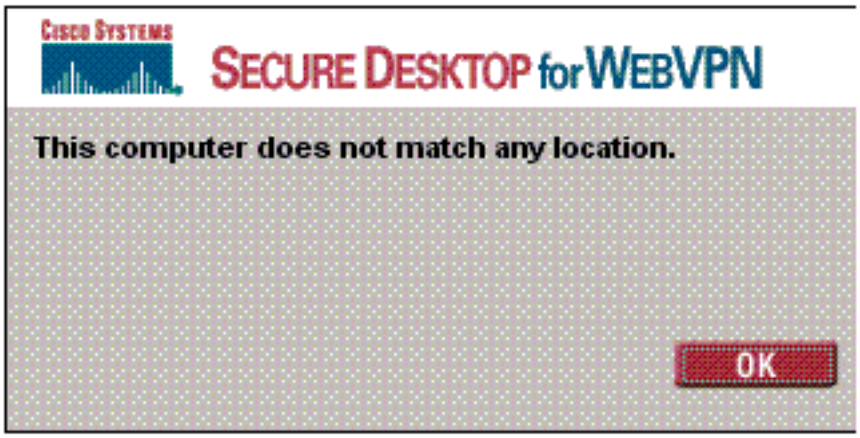
Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Échec de l'authentification WebVPN

Ces sections fournissent des informations que vous pouvez utiliser pour dépanner votre configuration.

- **Problème :** Les utilisateurs WebVPN ne peuvent pas s'authentifier sur le serveur RADIUS, mais peuvent s'authentifier avec succès avec la base de données locale du concentrateur VPN. Ils reçoivent des erreurs telles que « Échec de la connexion » et ce

message. 

Motif: Ce genre de problème se produit souvent lorsque toute base de données autre que la base de données interne du concentrateur est utilisée. Les utilisateurs WebVPN accèdent au groupe de base lorsqu'ils se connectent pour la première fois au concentrateur et doivent utiliser la méthode d'authentification par défaut. Souvent, cette méthode est définie sur la base de données interne du concentrateur et n'est pas un serveur RADIUS ou un autre serveur configuré.**Solution :** Lorsqu'un utilisateur WebVPN s'authentifie, le concentrateur vérifie la liste des serveurs définis à **Configuration > System > Servers > Authentication** et utilise le premier. Veillez à déplacer le serveur avec lequel les utilisateurs WebVPN doivent s'authentifier en haut de cette liste. Par exemple, si RADIUS doit être la méthode d'authentification, vous devez déplacer le serveur RADIUS en haut de la liste pour y insérer l'authentification.**Remarque :** Ce n'est pas parce que les utilisateurs de WebVPN ont atteint le groupe de base qu'ils sont confinés au groupe de base. D'autres groupes WebVPN peuvent être configurés sur le concentrateur et les utilisateurs peuvent être affectés par le serveur RADIUS avec la population de l'attribut 25 avec **OU=*groupname***. Référez-vous à Verrouillage des utilisateurs dans un groupe de concentrateurs VPN 3000 à l'aide d'un serveur RADIUS pour une explication plus détaillée.

Échec de l'authentification utilisateur par rapport à Active Directory

Dans le serveur Active Directory, dans l'onglet Compte des propriétés utilisateur de l'utilisateur défaillant, vous pouvez voir cette case à cocher :

[x] Ne nécessite pas de pré-authentification

Si cette case n'est pas cochée, **cochez-la**, puis essayez de vous authentifier à nouveau auprès de cet utilisateur.

Informations connexes

- Concentrateurs VPN de la gamme Cisco 3000
- Cisco VPN 3002 Hardware Clients
- Négociation IPSec/Protocoles IKE
- Page d'assistance RADIUS (Remote Authentication Dial-In User Service)
- RADIUS (Remote Authentication Dial-In User Service)
- Support et documentation techniques - Cisco Systems