Configuration des concentrateurs de la gamme Cisco VPN 3000 pour une prise en charge de la fonction NT Password Expiration avec le serveur RADIUS

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Diagramme du réseau
Configuration du concentrateur VPN 3000
Configuration de groupe
Configuration RADIUS
Configuration du serveur Cisco Secure NT RADIUS
Configuration d'une entrée pour le concentrateur VPN 3000
Configuration de la stratégie d'utilisateur inconnu pour l'authentification de domaine NT
Test de la fonction d'expiration du mot de passe NT/RADIUS
Test de l'authentification RADIUS
Authentification de domaine NT réelle à l'aide du proxy RADIUS pour tester la fonction d'expiration du mot de passe
Informations connexes

Introduction

Ce document inclut des instructions détaillées sur la façon de configurer les concentrateurs de la gamme Cisco VPN 3000 pour prendre en charge la fonctionnalité d'expiration de mot de passe NT à l'aide du serveur RADIUS.

Référez-vous à VPN 3000 RADIUS avec fonctionnalité d'expiration utilisant Microsoft Internet Authentication Server afin d'en savoir plus sur le même paysage avec Internet Authentication Server (IAS).

Conditions préalables

Conditions requises

- Si votre serveur RADIUS et votre serveur d'authentification de domaine NT se trouvent sur deux machines distinctes, vérifiez que vous avez établi une connectivité IP entre les deux

machines.

- Vérifiez que vous avez établi la connectivité IP du concentrateur au serveur RADIUS. Si le serveur RADIUS se trouve vers l'interface publique, n'oubliez pas d'ouvrir le port RADIUS sur le filtre public.
- Assurez-vous que vous pouvez vous connecter au concentrateur à partir du client VPN à l'aide de la base de données utilisateur interne. Si ce n'est pas configuré, reportez-vous à Configuration d'IPSec - Client VPN Cisco 3000 vers concentrateur VPN 3000.

Remarque : La fonction d'expiration du mot de passe ne peut pas être utilisée avec des clients VPN Web ou VPN SSL.

Components Used

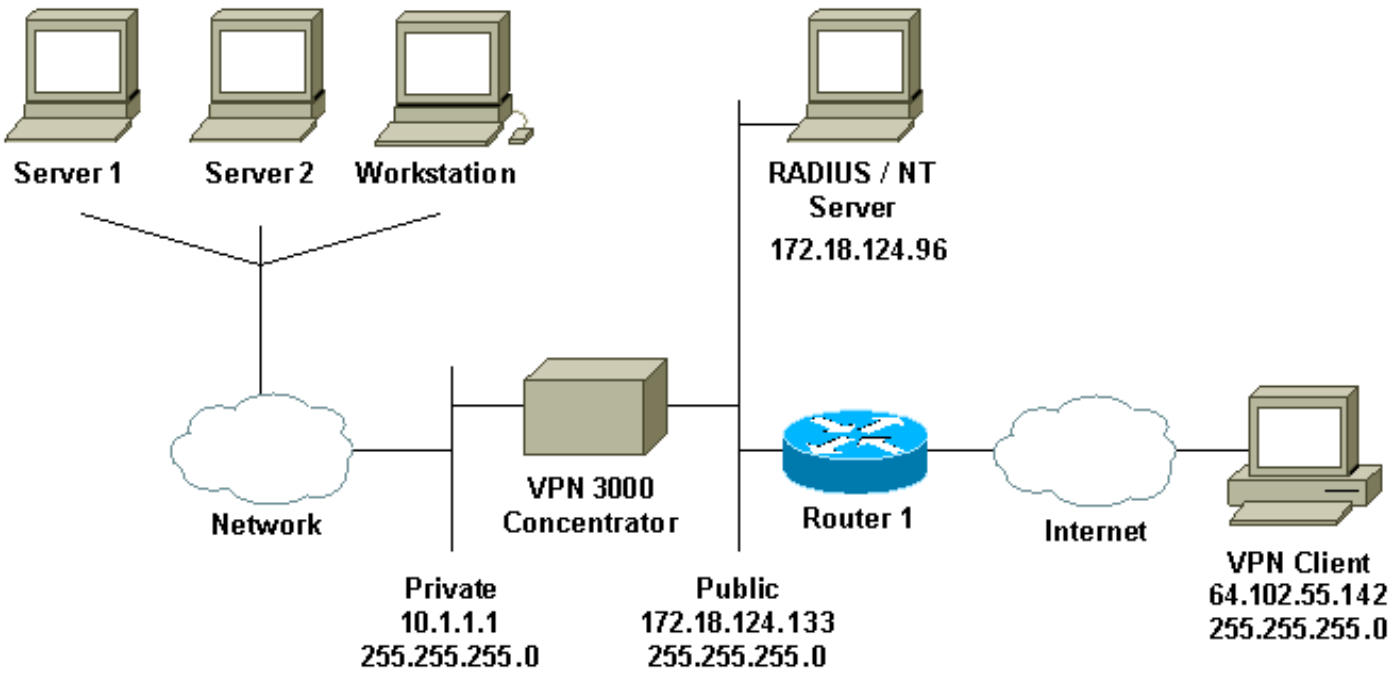
Cette configuration a été développée et testée à l'aide des versions logicielle et matérielle ci-dessous.

- Logiciel du concentrateur VPN 3000 version 4.7
- Client VPN version 3.5
- Cisco Secure pour NT (CSNT) version 3.0 Microsoft Windows 2000 Active Directory Server for User Authentication

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 :



Notes de diagramme

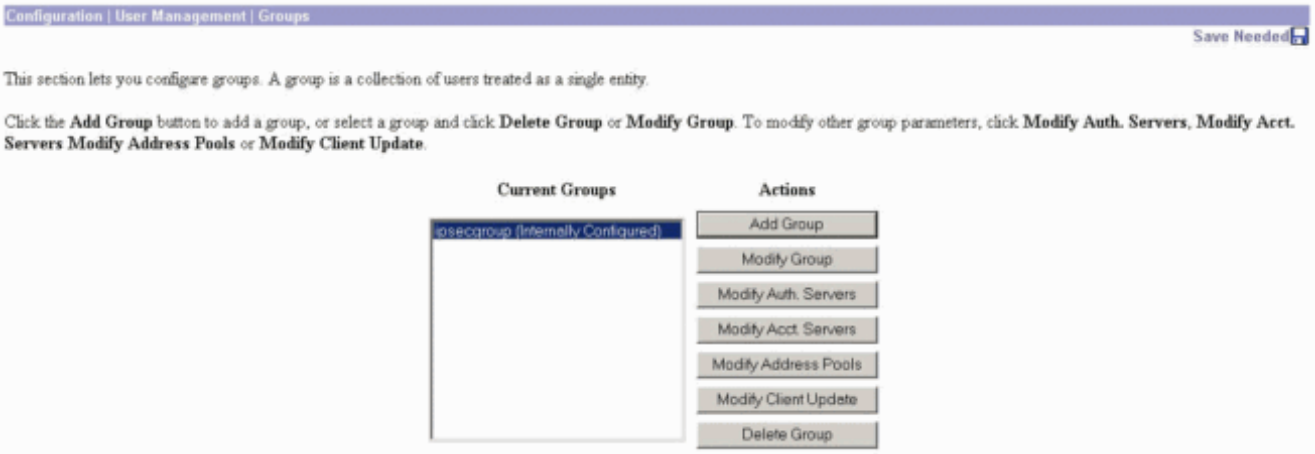
1. Le serveur RADIUS dans cette configuration se trouve sur l'interface publique. Si tel est le cas avec votre configuration spécifique, créez deux règles dans votre filtre public pour autoriser le trafic RADIUS à entrer et à quitter le concentrateur.

2. Cette configuration montre le logiciel CSNT et les services d'authentification de domaine NT exécutés sur la même machine. Ces éléments peuvent être exécutés sur deux machines distinctes si votre configuration l'exige.

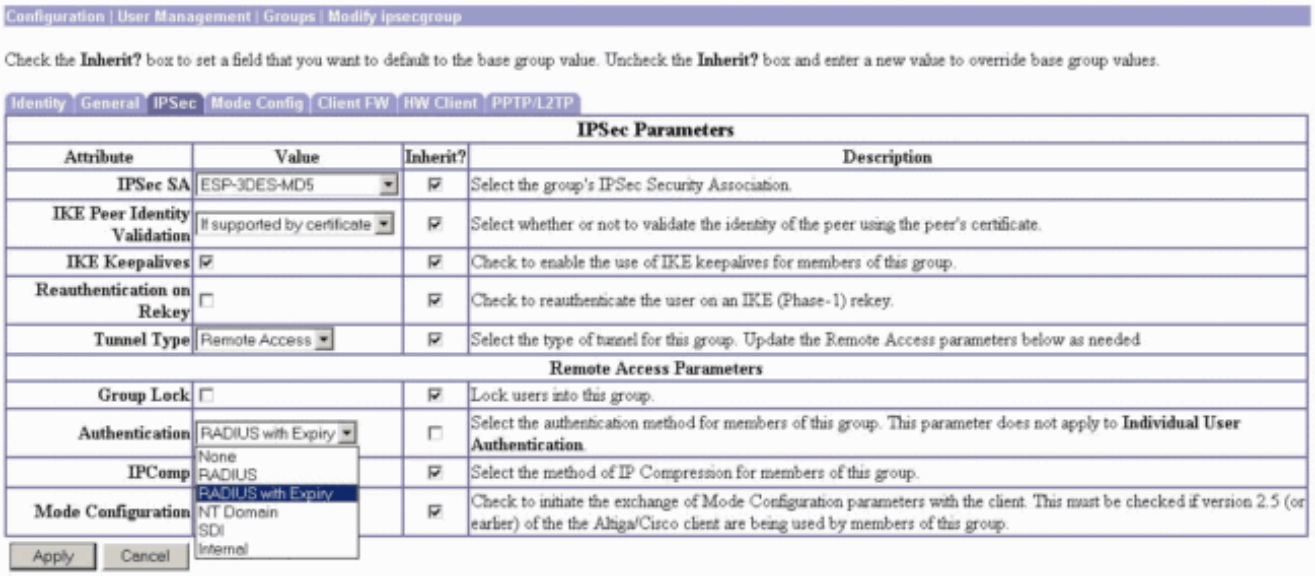
Configuration du concentrateur VPN 3000

Configuration de groupe

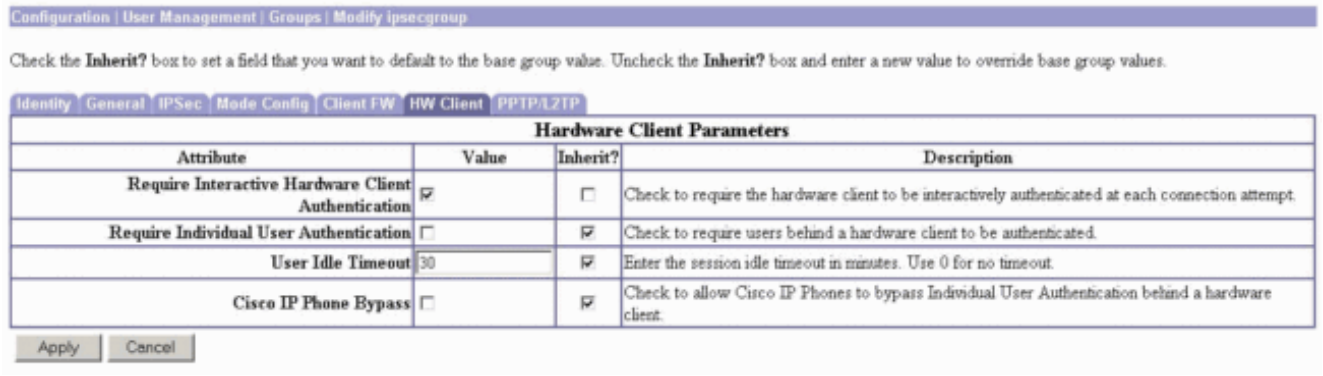
1. Pour configurer le groupe pour qu'il accepte les paramètres d'expiration de mot de passe NT à partir du serveur RADIUS, accédez à **Configuration > User Management > Groups**, sélectionnez votre groupe dans la liste, puis cliquez sur **Modify Group**. L'exemple ci-dessous montre comment modifier un groupe nommé « ipsecgroup
»
.



2. Accédez à l'onglet **IPSec**, vérifiez que **RADIUS avec expiration** est sélectionné pour l'attribut **Authentication**.

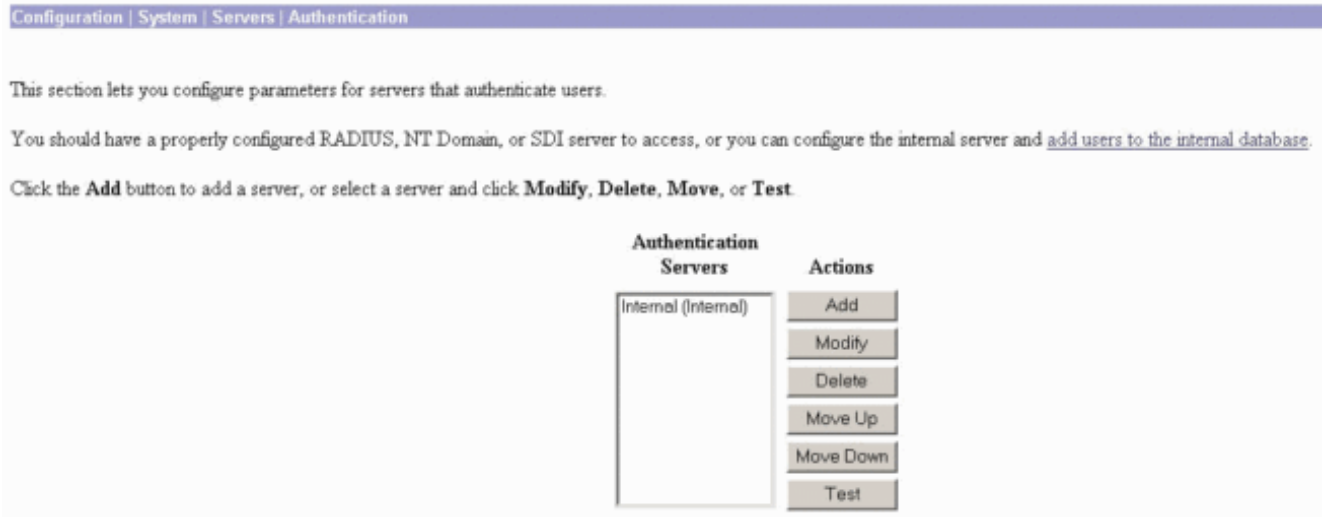


3. Si vous voulez que cette fonctionnalité soit activée sur les clients matériels VPN 3002, accédez à l'onglet **Client matériel**, assurez-vous que l'option **Exiger une authentification client matériel interactive** est activée, puis cliquez sur
Appliquer.



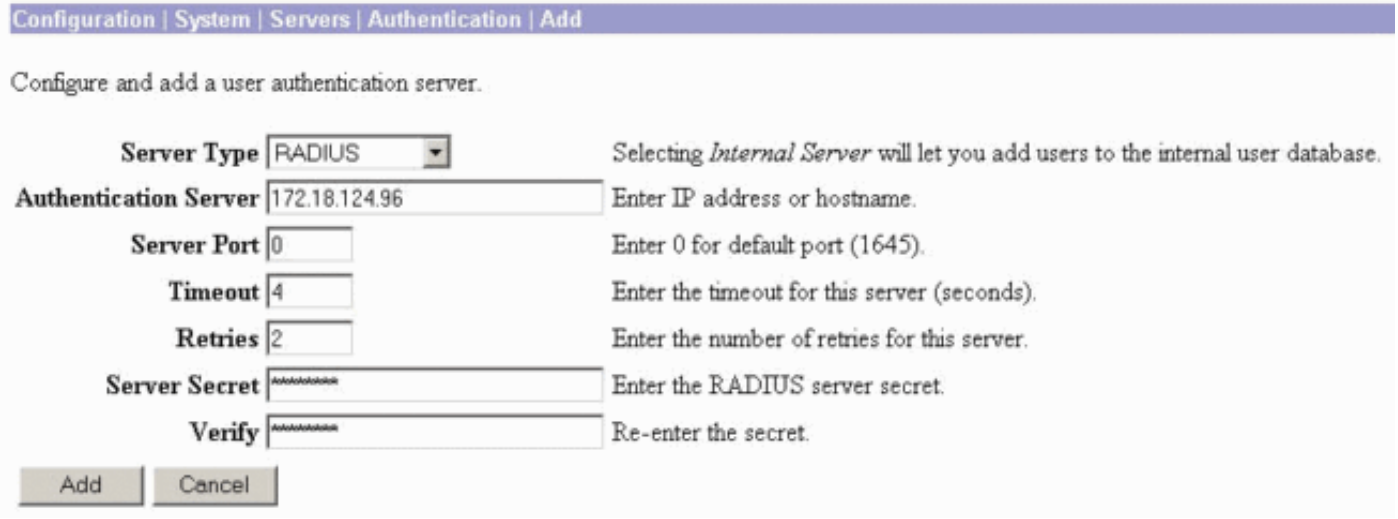
Configuration RADIUS

1. Pour configurer les paramètres du serveur RADIUS sur le concentrateur, accédez à Configuration > **System** > **Servers** > **Authentication** > **Add**.



2. Dans l'écran **Ajouter**, saisissez les valeurs qui correspondent au serveur RADIUS et cliquez sur **Ajouter**.L'exemple ci-dessous utilise les valeurs suivantes.

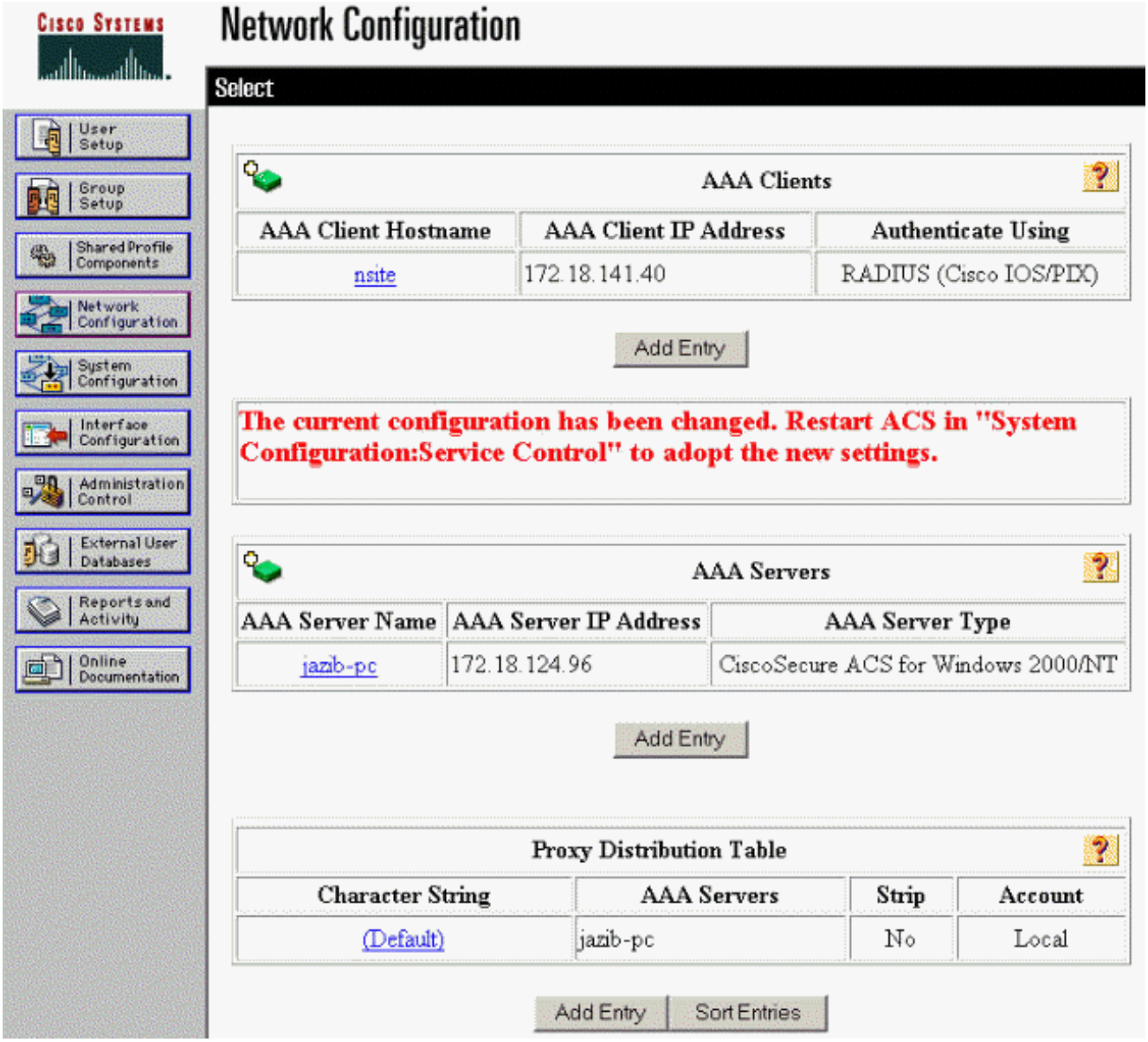
```
Server Type: RADIUS


Authentication Server: 172.18.124.96


Server Port = 0 (for default of 1645)

Timeout = 4


Reties = 2


Server Secret = cisco123


Verify: cisco123
```



Configuration du serveur Cisco Secure NT RADIUS

Configuration d'une entrée pour le concentrateur VPN 3000

1. Connectez-vous à CSNT et cliquez sur **Configuration réseau** dans le panneau de gauche. Sous « Clients AAA », cliquez sur **Ajouter une entrée**.



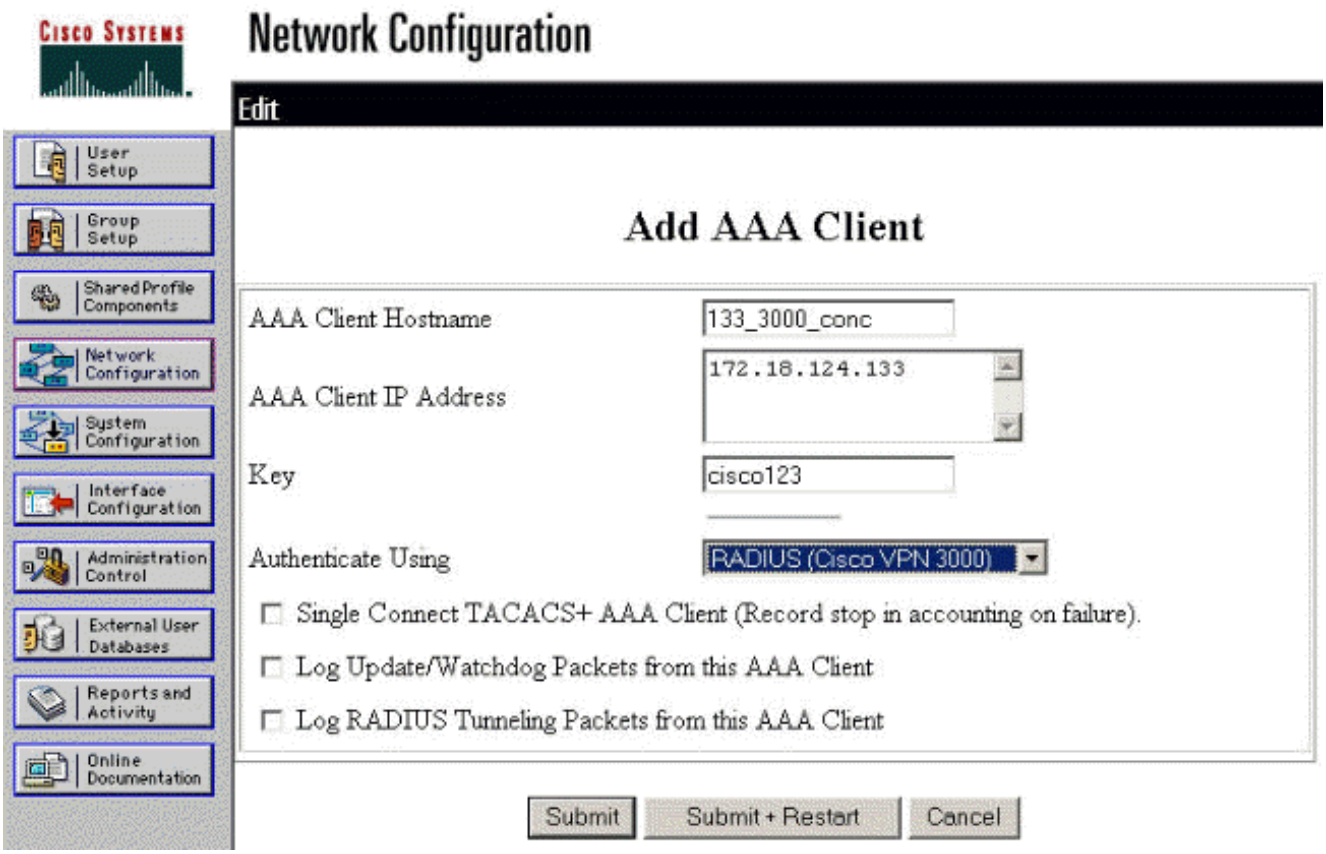
2. Dans l'écran « Ajouter un client AAA », saisissez les valeurs appropriées pour ajouter le concentrateur en tant que client RADIUS, puis cliquez sur **Soumettre + Redémarrer**.L'exemple ci-dessous utilise les valeurs suivantes.

AAA Client Hostname = **133_3000_conc**

AAA Client IP Address = **172.18.124.133**

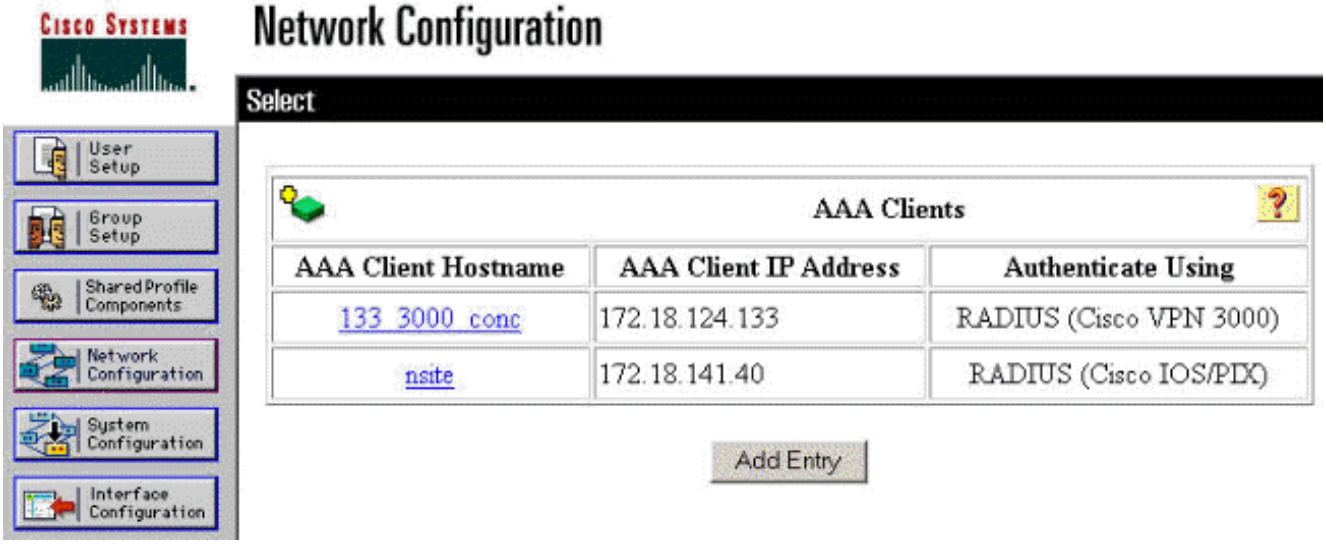
Key = **cisco123**

Authenticate using = **RADIUS (Cisco VPN 3000)**



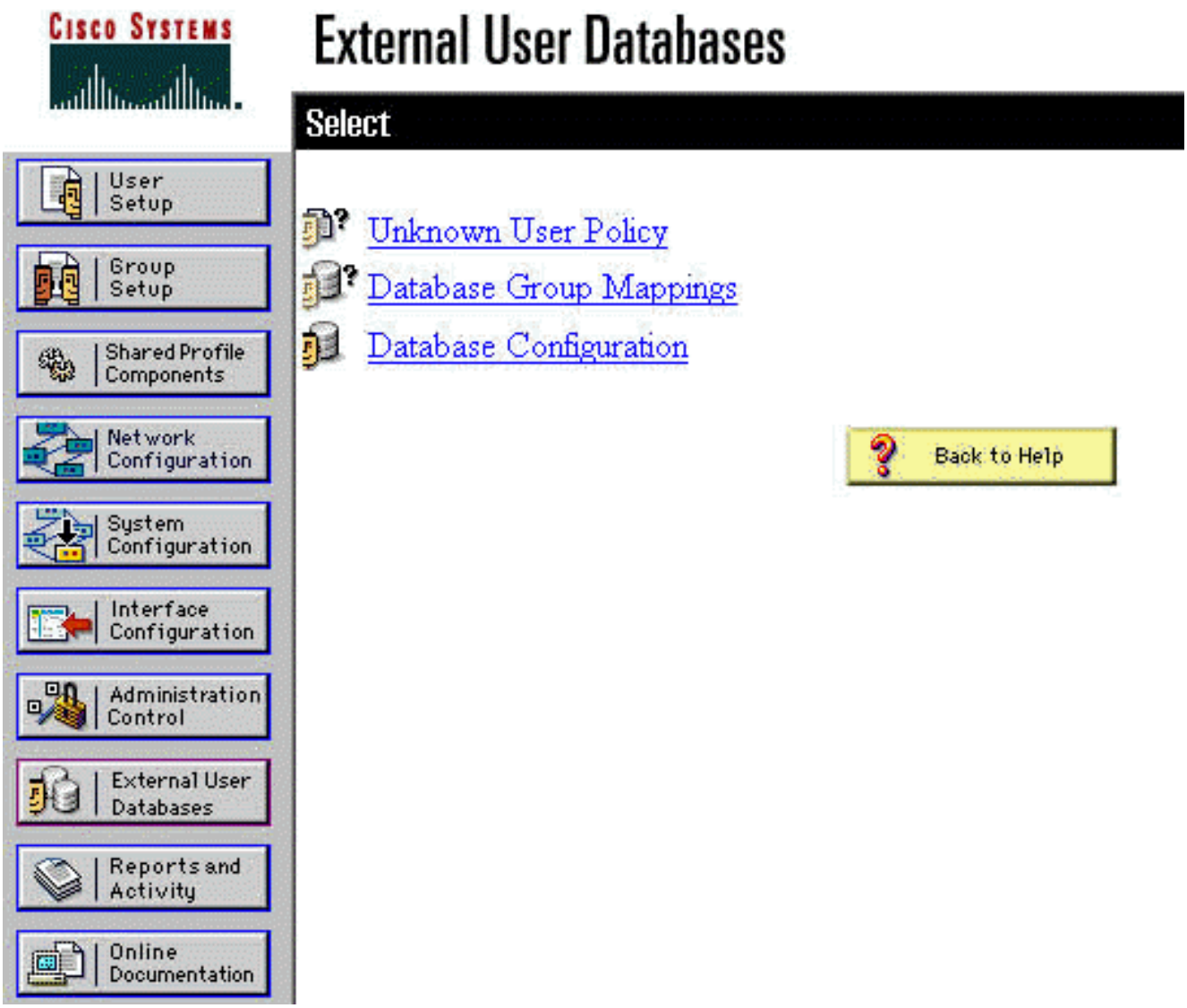
Une entrée pour votre concentrateur 3000 apparaîtra sous la section "**Clients AAA**«

.

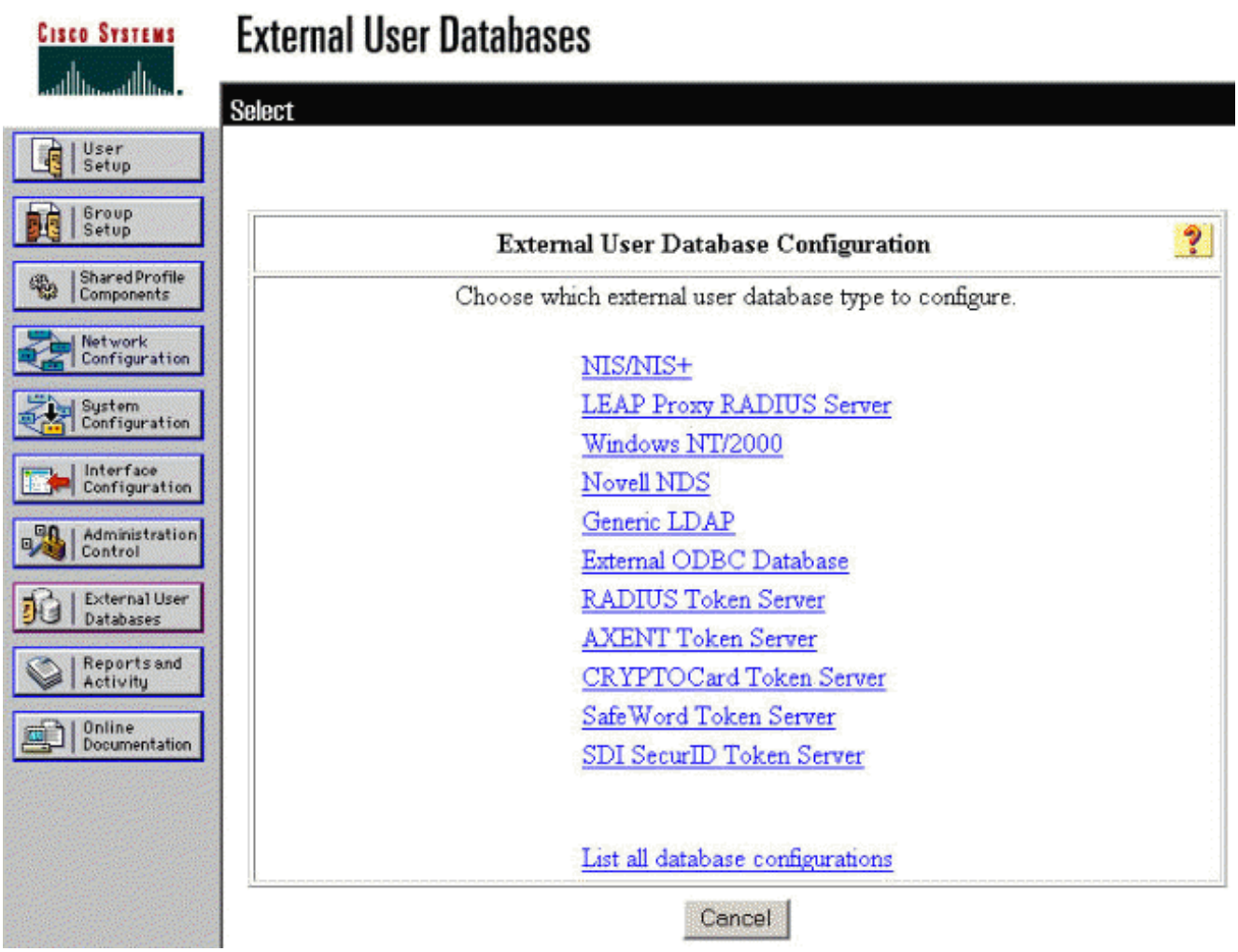


Configuration de la stratégie d'utilisateur inconnu pour l'authentification de domaine NT

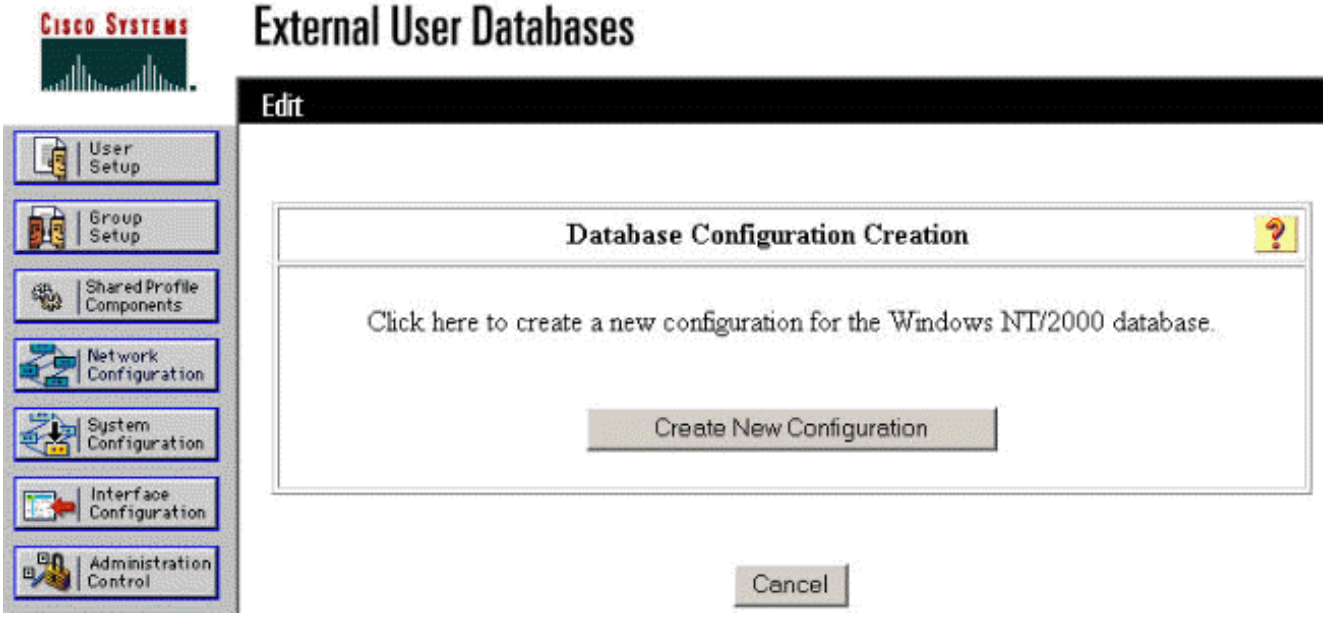
1. Pour configurer l'authentification utilisateur sur le serveur RADIUS dans le cadre de la stratégie utilisateur inconnu, cliquez sur **Base de données utilisateur externe** dans le panneau de gauche, puis cliquez sur le lien pour **Configuration de base de données**.



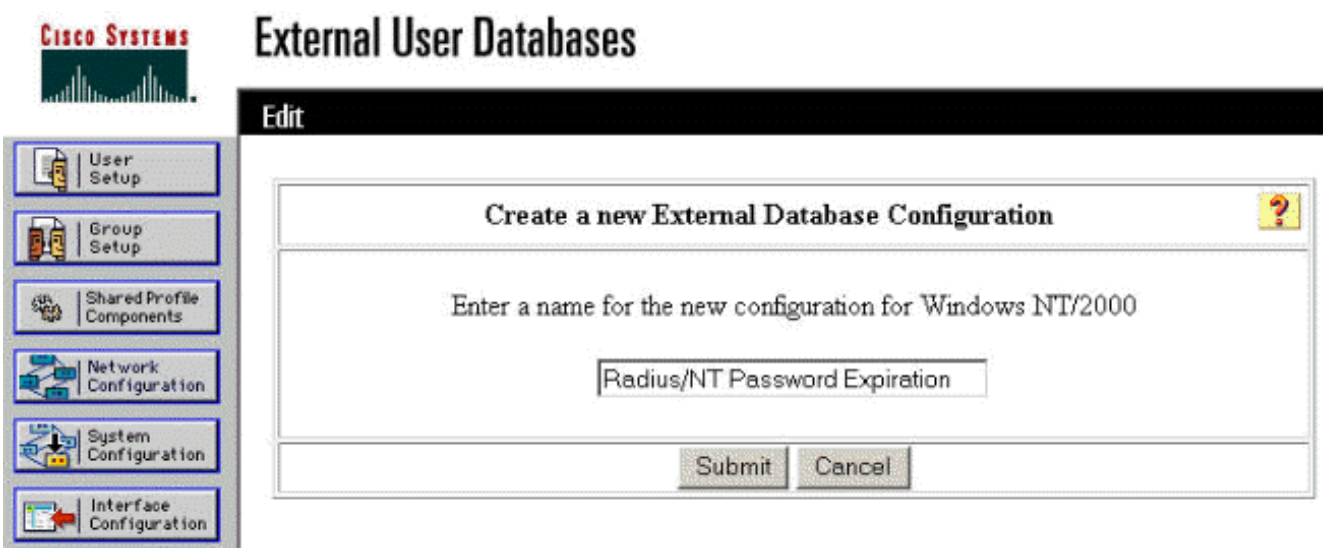
2. Sous Configuration de base de données utilisateur externe, cliquez sur **Windows NT/2000**.



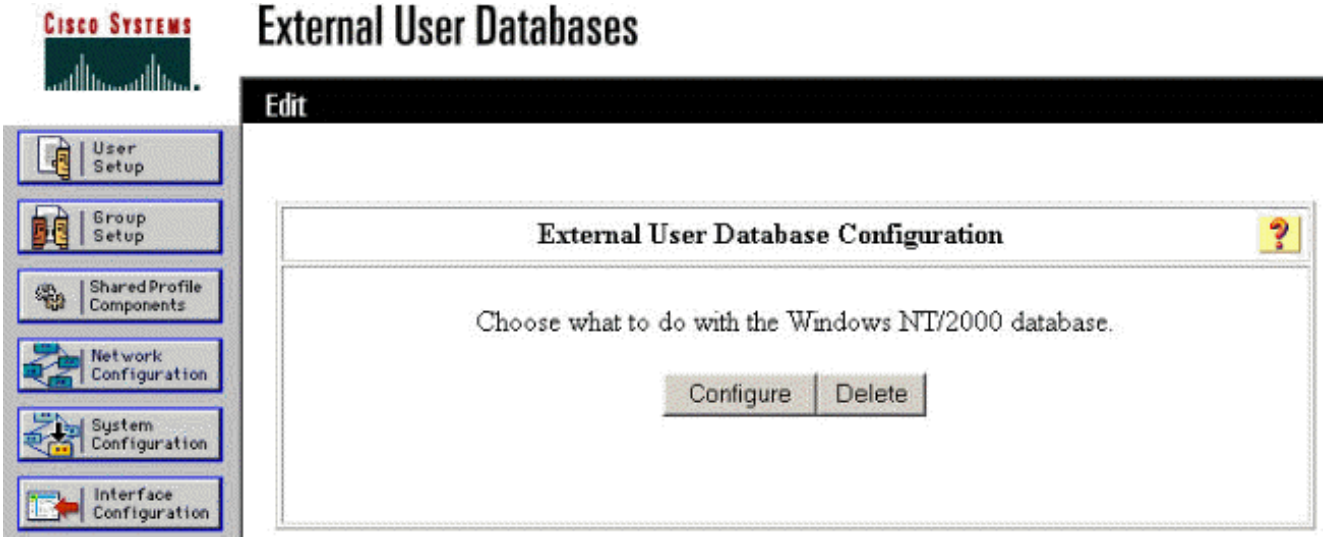
3. Dans l'écran Création de la configuration de base de données, cliquez sur **Créer une configuration**.



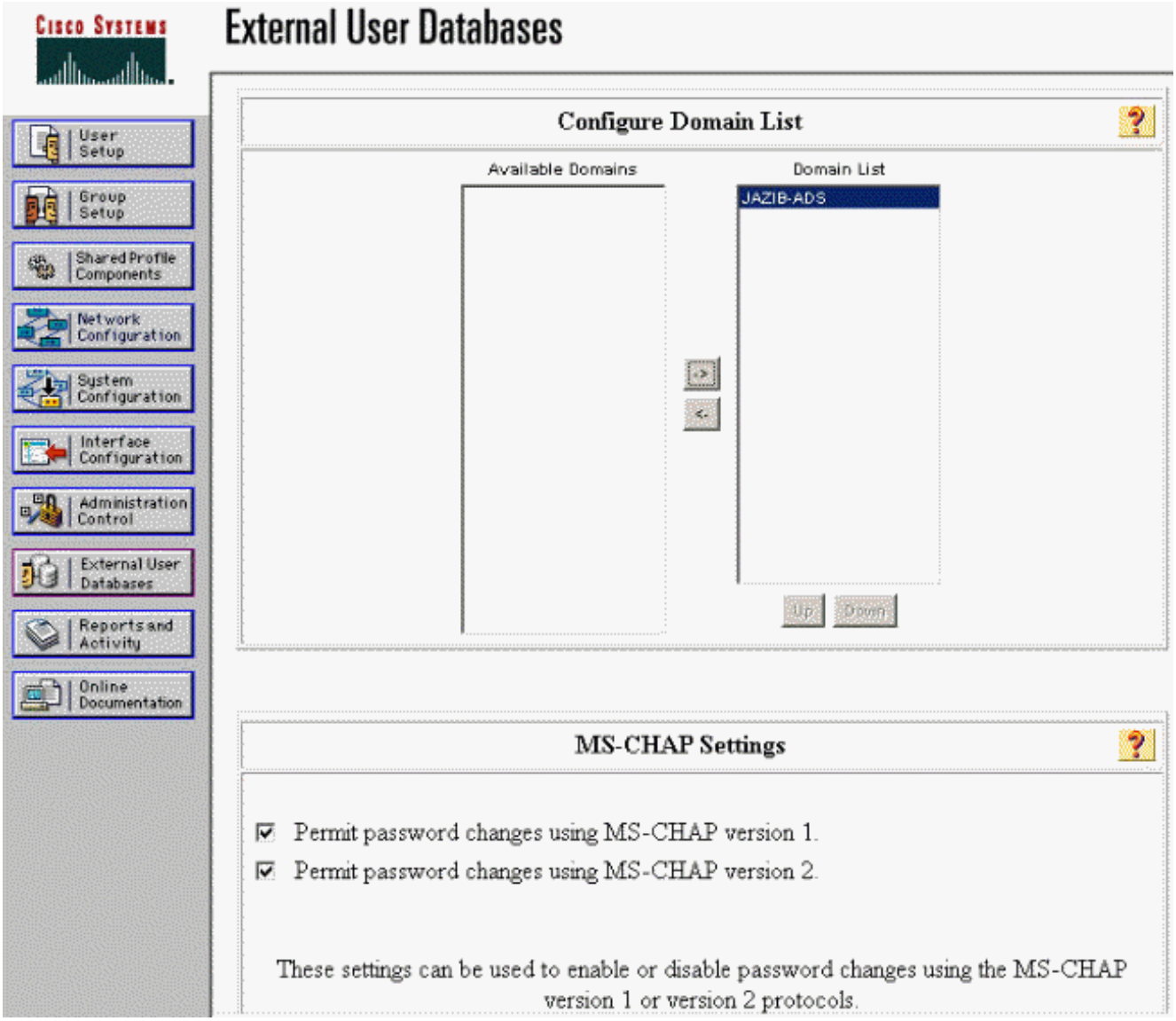
4. Lorsque vous y êtes invité, tapez un nom pour l'authentification NT/2000 et cliquez sur **Submit**. L'exemple ci-dessous montre le nom « Radius/NT Password Expiration. »



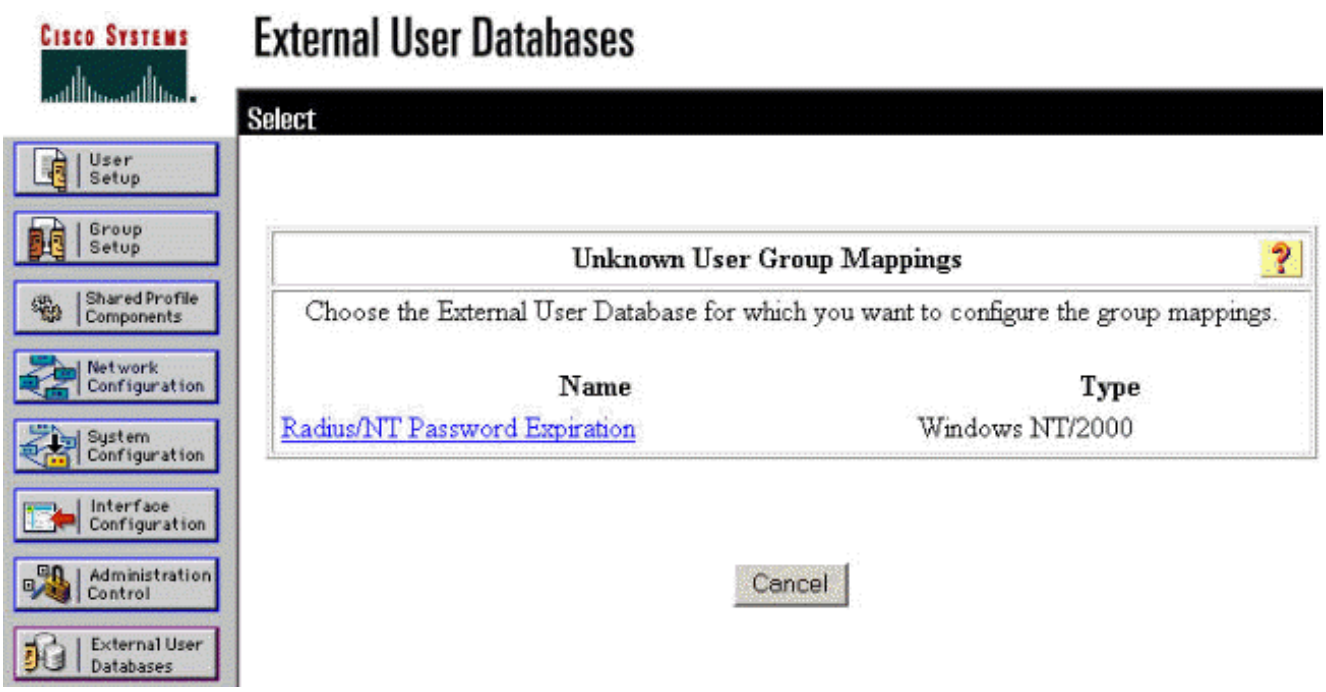
5. Cliquez sur **Configurer** pour configurer le nom de domaine pour l'authentification utilisateur.



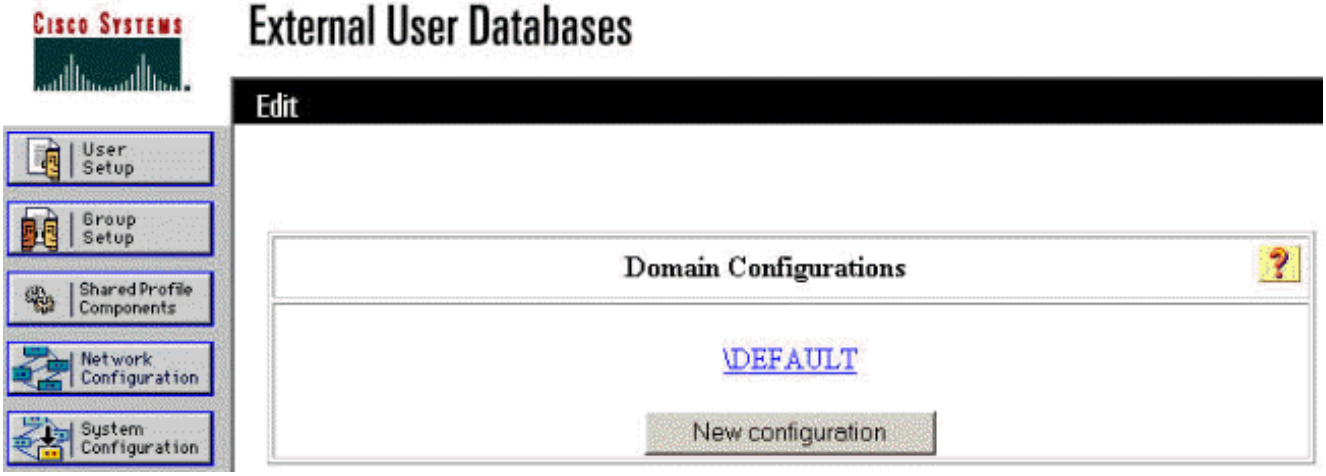
6. Sélectionnez votre domaine NT dans la zone « Domaines disponibles », puis cliquez sur la flèche droite pour l'ajouter à la liste de domaines. Sous « Paramètres MS-CHAP », assurez-vous que les options **Permit password change en utilisant MS-CHAP version 1** et **version 2** sont sélectionnées. Cliquez sur **Submit lorsque vous avez terminé.**



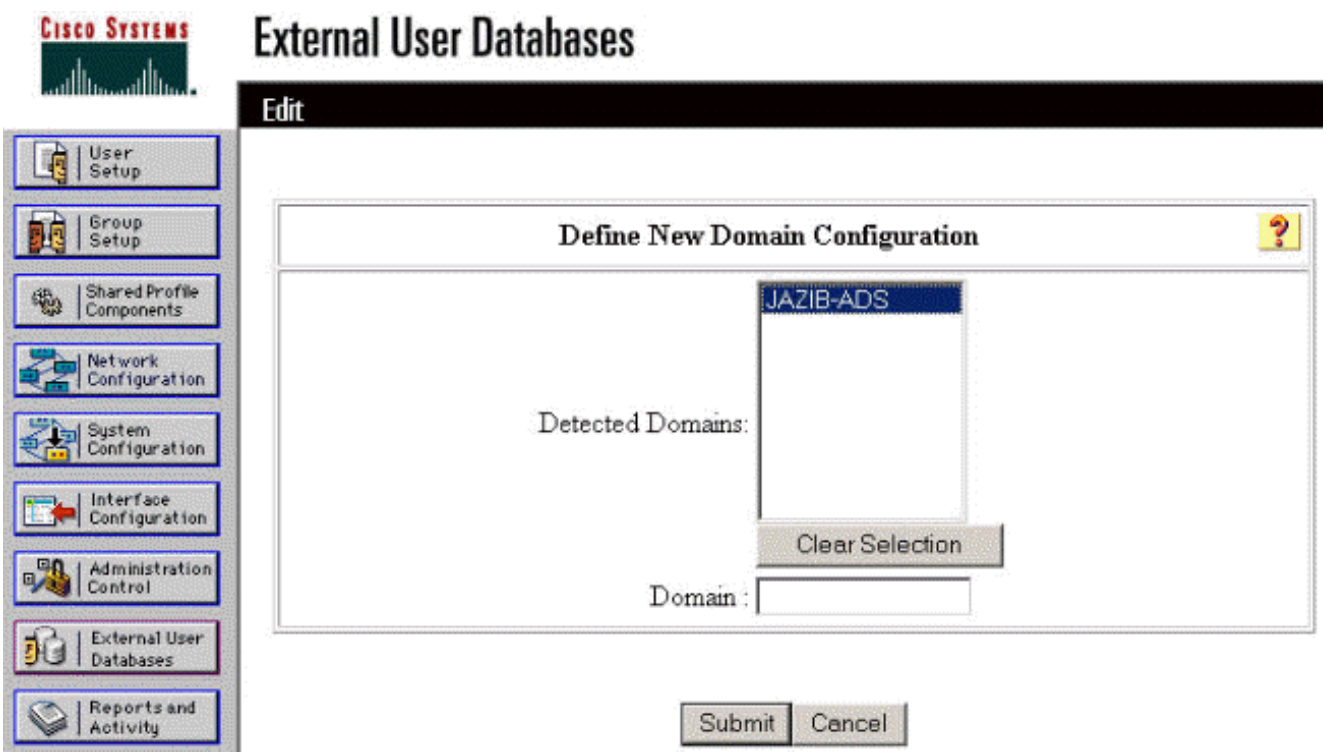
7. Cliquez sur **Base de données d'utilisateurs externes** dans le panneau de gauche, puis cliquez sur le lien correspondant aux **mappages de groupes de bases de données** (comme dans cet exemple). Vous devriez voir une entrée pour votre base de données externe précédemment configurée. L'exemple ci-dessous montre une entrée pour « Radius/NT Password Expiration », la base de données que nous venons de configurer.



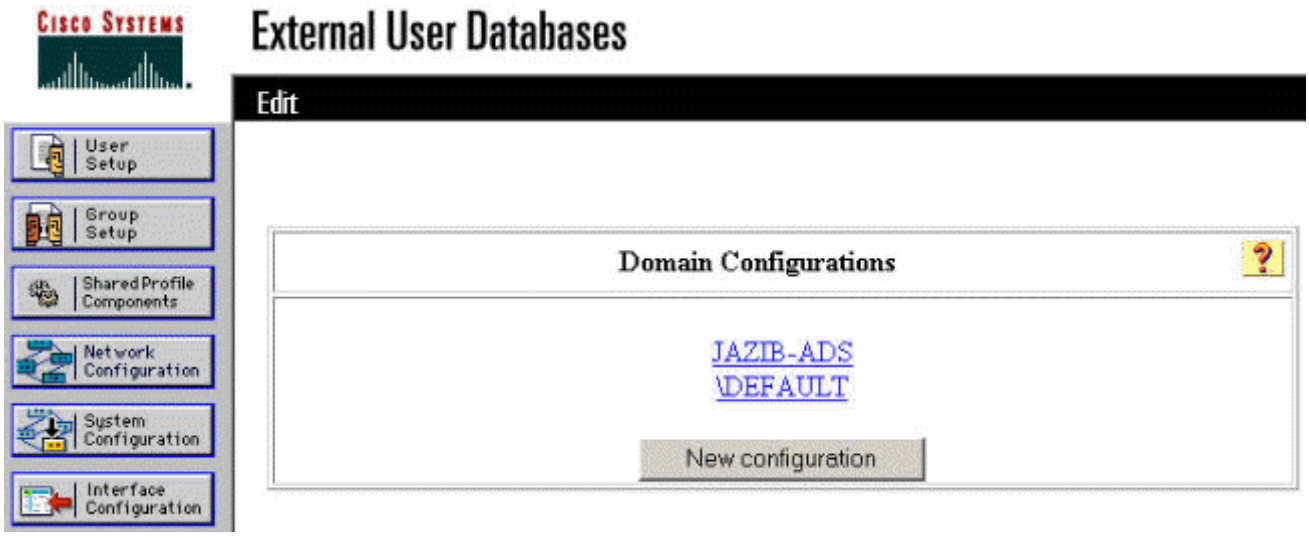
8. Dans l'écran « Configurations de domaine », cliquez sur **Nouvelle configuration** pour ajouter les configurations de
domaine.



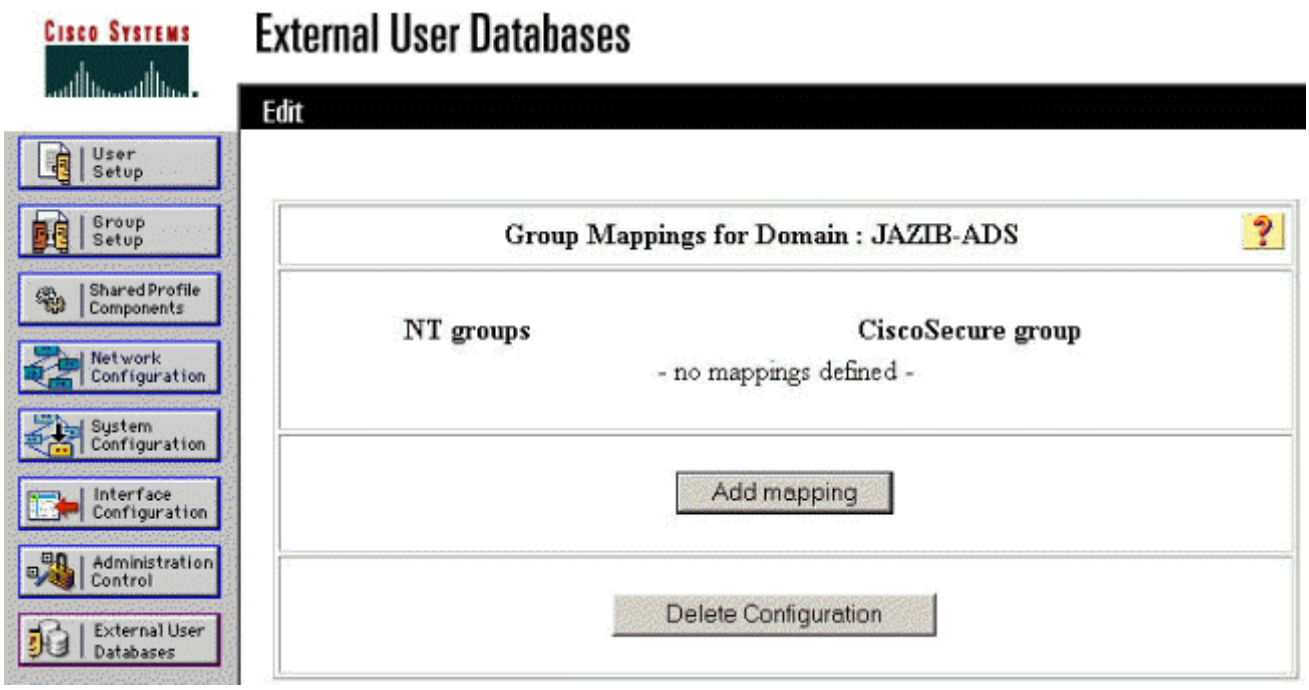
9. Sélectionnez votre domaine dans la liste des domaines détectés et cliquez sur **Soumettre**. L'exemple ci-dessous montre un domaine nommé « JAZIB-ADS.
»



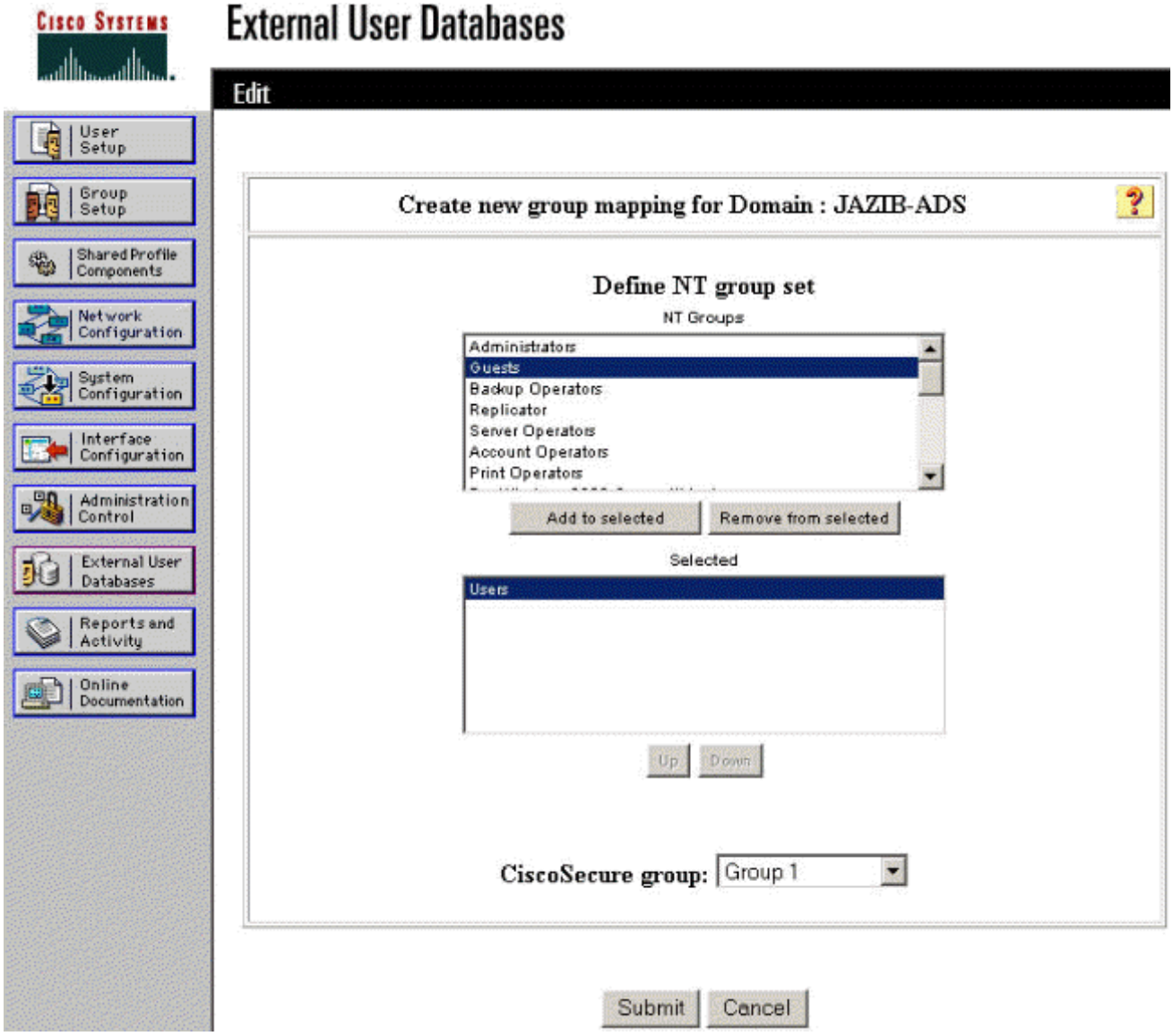
10. Cliquez sur votre nom de domaine pour configurer les mappages de groupe. Cet exemple montre le domaine « JAZIB-ADS.
    »



11. Cliquez sur **Ajouter un mappage** pour définir les mappages de groupe.

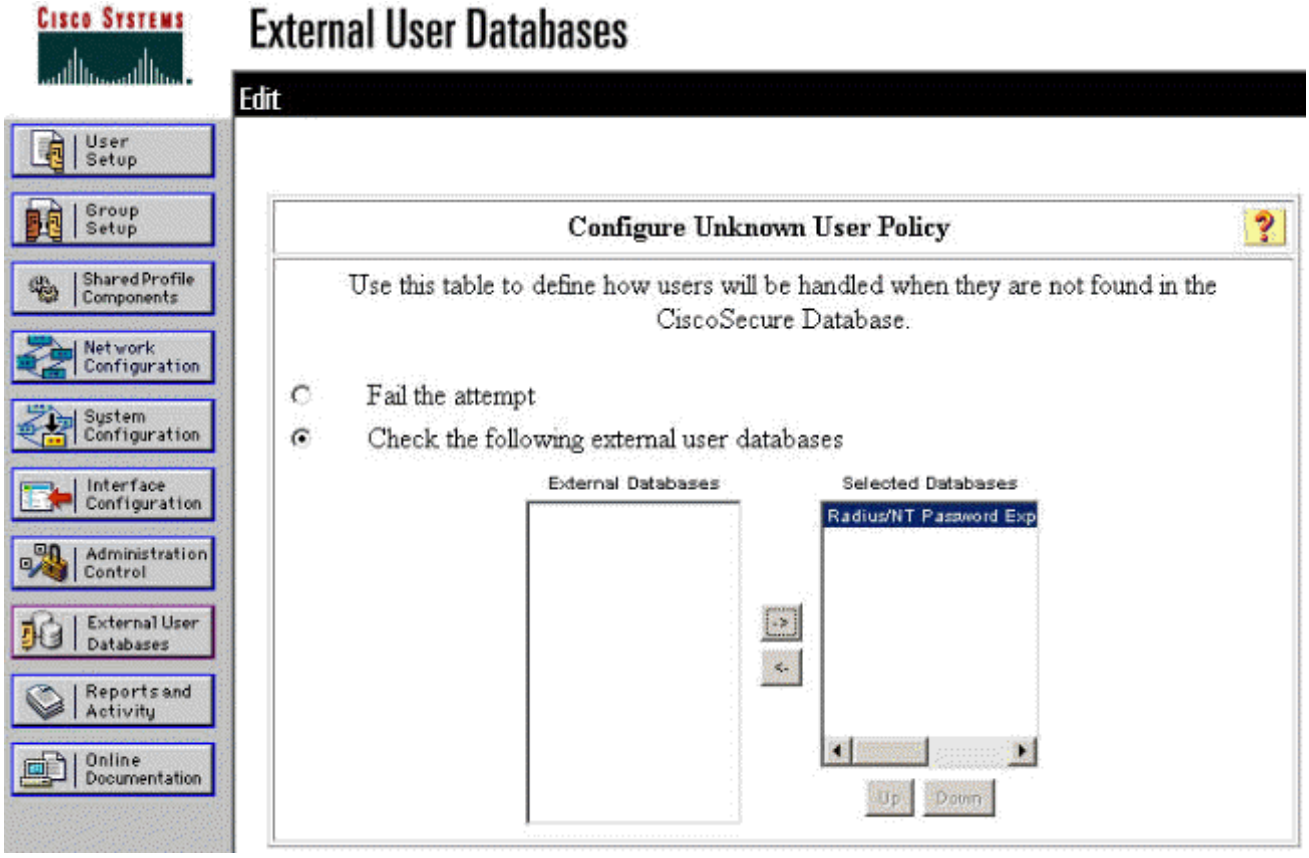


12. Dans l'écran « Créer un nouveau mappage de groupe », mappez le groupe sur le domaine NT à un groupe sur le serveur RADIUS CSNT, puis cliquez sur **Soumettre**. L'exemple ci-dessous mappe le groupe NT « Users » au groupe RADIUS « Group 1 ».



13. Cliquez sur **Base de données utilisateur externe** dans le panneau de gauche, puis cliquez

sur le lien **Stratégie utilisateur inconnu** (comme dans cet exemple). Assurez-vous que l'option **Vérifier les bases de données utilisateur externes suivantes** est sélectionnée. Cliquez sur la flèche droite pour déplacer la base de données externe précédemment configurée de la liste des « bases de données externes » vers la liste des « bases de données sélectionnées
».

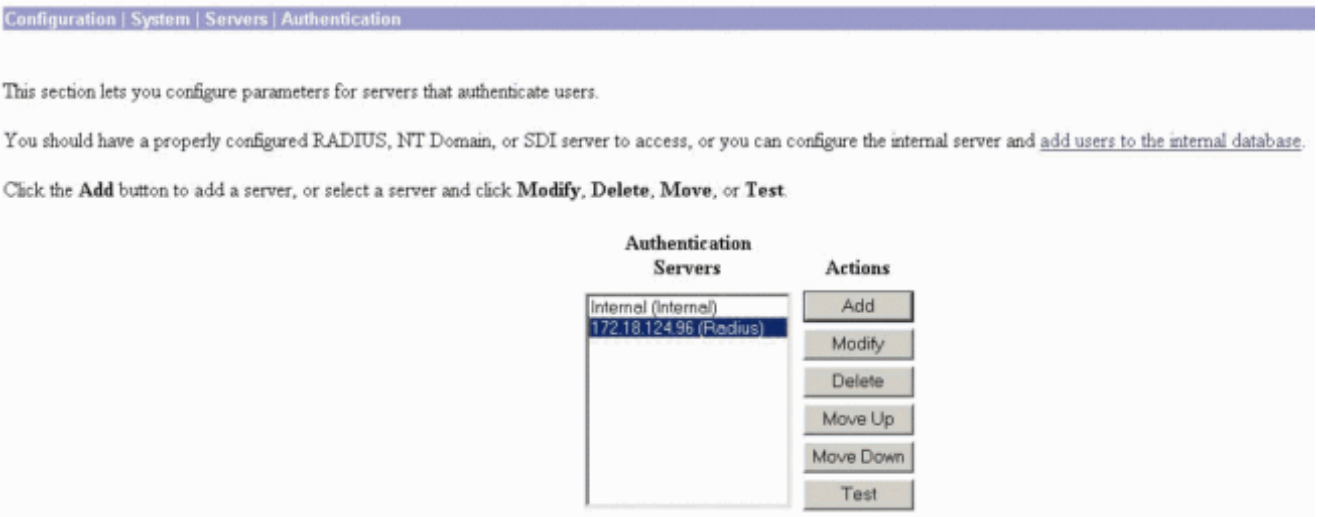


Test de la fonction d'expiration du mot de passe NT/RADIUS

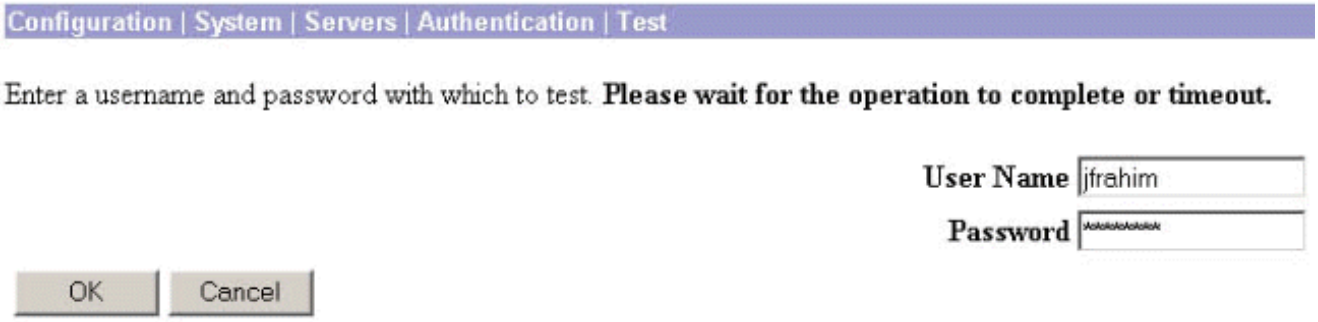
Le concentrateur offre une fonction pour tester l'authentification RADIUS. Pour tester correctement cette fonctionnalité, veillez à suivre attentivement ces étapes.

Test de l'authentification RADIUS

1. Accédez à **Configuration > System > Servers > Authentication**. Sélectionnez votre serveur RADIUS et cliquez sur
Test.



2. Lorsque vous y êtes invité, tapez votre nom d'utilisateur et votre mot de passe de domaine NT, puis cliquez sur **OK**. L'exemple ci-dessous montre le nom d'utilisateur « jfrahim » configuré sur le serveur de domaine NT avec « cisco123 » comme mot de passe.



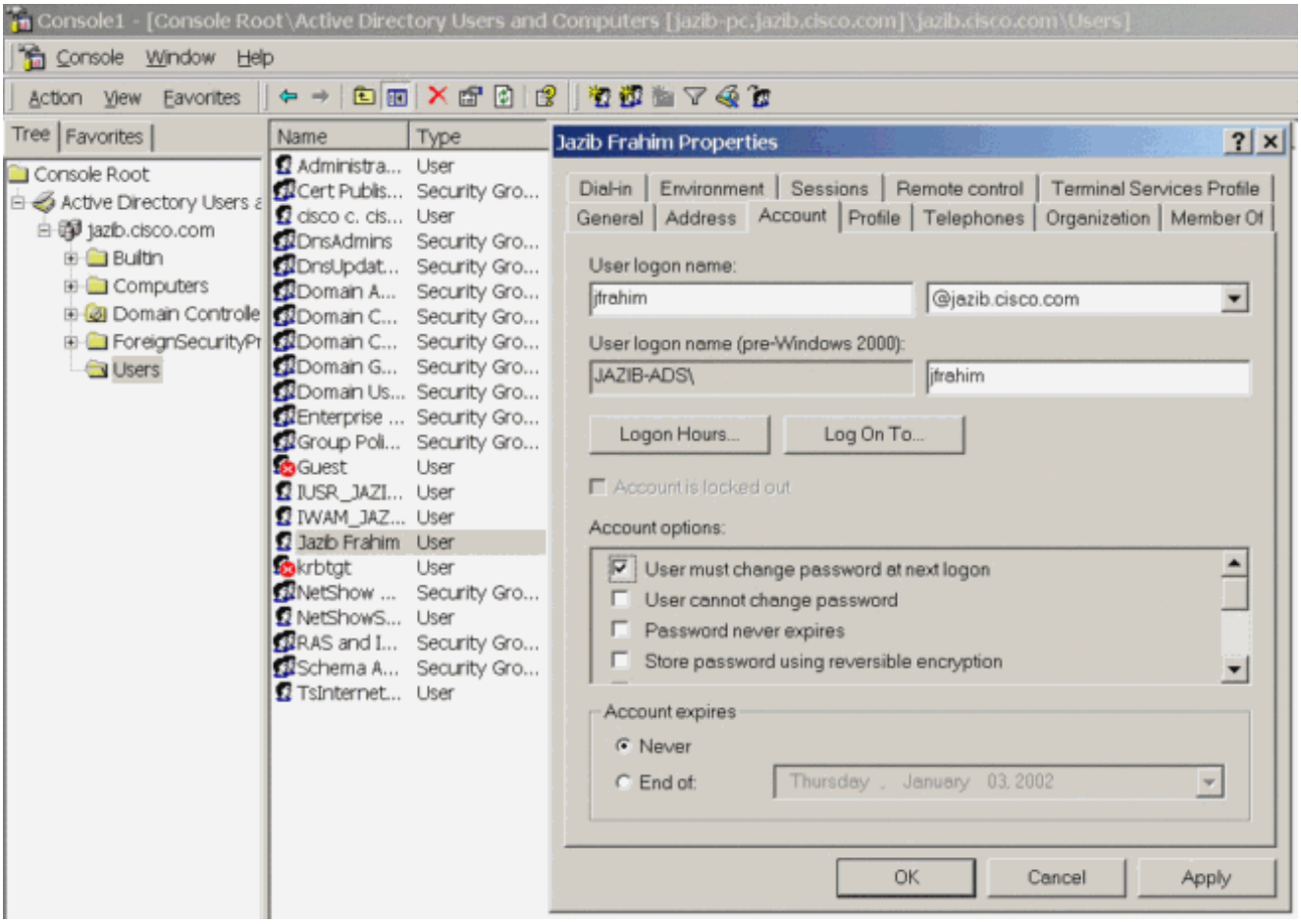
3. Si votre authentification est configurée correctement, vous devez recevoir un message indiquant « Authentication Success

». Si vous recevez un message autre que celui présenté ci-dessus, il y a un problème de configuration ou de connexion. Répétez les étapes de configuration et de test décrites dans ce document pour vous assurer que tous les paramètres ont été correctement définis. Vérifiez également la connectivité IP entre vos périphériques.

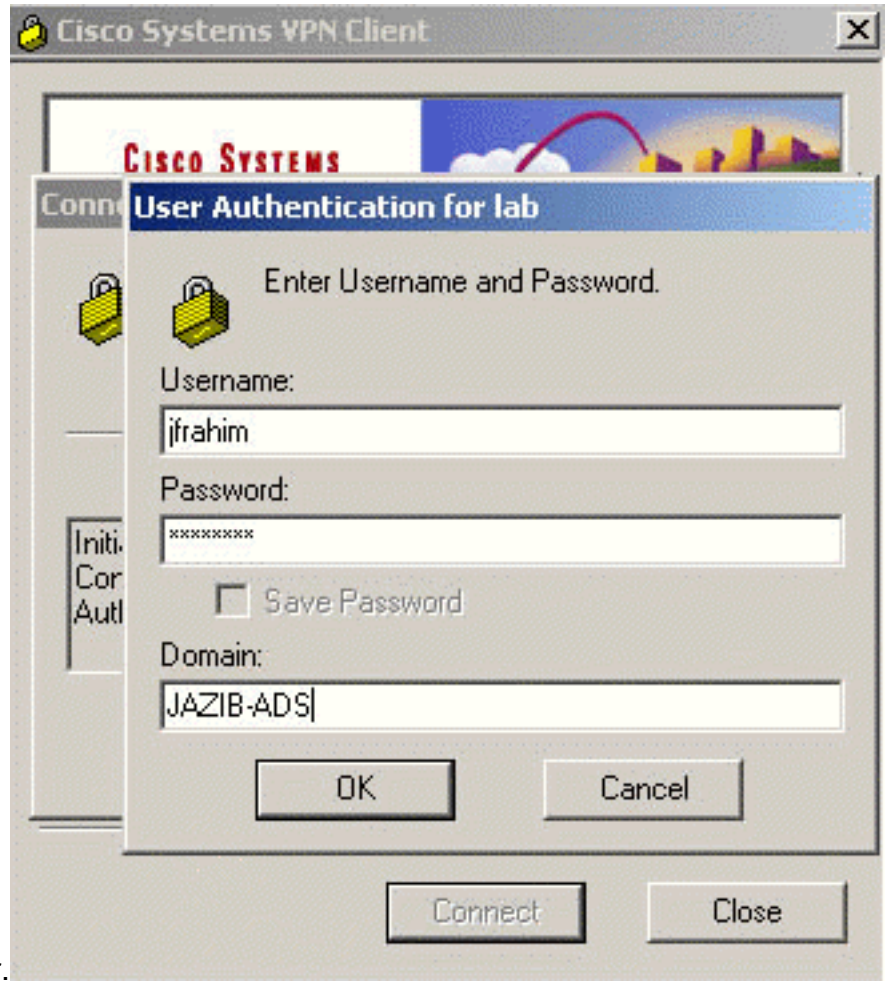
Authentification de domaine NT réelle à l'aide du proxy RADIUS pour tester la fonction d'expiration du mot de passe

1. Si l'utilisateur est déjà défini sur le serveur de domaine, modifiez les propriétés afin que l'utilisateur soit invité à modifier le mot de passe lors de la prochaine connexion. Accédez à l'onglet « Compte » de la boîte de dialogue des propriétés de l'utilisateur, sélectionnez

l'option pour **l'utilisateur doit changer de mot de passe lors de la prochaine ouverture de session**, puis cliquez sur
OK.



2. Lancez le client VPN, puis essayez d'établir le tunnel vers le

concentrateur. 

3. Lors de l'authentification de l'utilisateur, vous devez être invité à modifier le mot de passe. 

Informations connexes

- Concentrateur de la gamme Cisco VPN 3000
- IPsec
- Cisco Secure Access Control Server pour Windows
- RADIUS
- Demandes de commentaires (RFC)