# Verrou et clé : Listes d'accès dynamique

## Contenu



## Introduction

L'accès de verrou vous permet d'installer les listes d'accès dynamique qui accordent l'accès par utilisateur à une source/hôte de destination spécifique par un processus d'authentification de l'utilisateur. On permet l'accès client par un Pare-feu de Cisco IOS® dynamiquement, sans n'importe quelle compromission dans les restrictions de Sécurité.

## Conditions préalables

### Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

### Composants utilisés

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Dans ce cas, l'environnement de travaux pratiques s'est composé d'une version de logiciel 12.3(1) courante de Cisco IOS® de 2620 routeurs. 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.

# Charrier des considérations

L'accès de verrou permet à un événement externe pour placer une ouverture dans le Pare-feu Cisco IOS. Après que cette ouverture existe, le routeur est susceptible du détournement de l'adresse source. Afin d'empêcher ceci, fournissez à la prise en charge du chiffrement utilisant le cryptage IP l'authentification ou le cryptage.

La mystification est un problème avec toutes les listes d'accès existantes. L'accès de verrou n'aborde pas ce problème.

Puisque l'accès de verrou introduit une voie potentielle par votre pare-feu réseau, vous devez considérer l'accès dynamique. Un autre hôte, charriant votre adresse authentifiée, accède derrière le Pare-feu. Avec l'accès dynamique, il y a la possibilité qu'un hôte non autorisé, charriant votre adresse authentifiée, accède derrière le Pare-feu. L'accès de verrou ne pose pas le problème de mystification d'adresse. Le problème est seulement identifié ici comme souci à l'utilisateur.

# Représentation

La représentation est affectée dans ces deux situations.

- Chaque liste d'accès dynamique force une reconstruction de liste d'accès sur le système de commutation par silicium (SSE). Ceci fait ralentir le chemin de commutation SSE momentanément.
- Les listes d'accès dynamique exigent l'installation de veille de délai d'attente (même si le délai d'attente est laissé pour se transférer). Par conséquent, les listes d'accès dynamique ne peuvent pas être SSE commuté. Ces entrées sont manipulées dans le chemin de commutation rapide de protocole.

Observez les configurations de routeur de cadre. Les utilisateurs distants créent des entrées de liste d'accès sur le routeur de cadre. La liste d'accès se développe et se rétrécit dynamiquement. Des entrées sont dynamiquement retirées de la liste après que l'inactif-délai d'attente ou la période de maximum-délai d'attente expire. Les grandes Listes d'accès dégradent la représentation de commutation par paquets.

# Quand utiliser le verrou Access

Deux exemples de quand vous utilisez l'accès de verrou sont répertoriés ici :

- Quand vous voulez qu'un serveur distant puisse accéder à un hôte dans votre interréseau par l'Internet. L'accès de verrou limite l'accès au delà de votre Pare-feu sur une base individuelle d'hôte ou de net.
- Quand vous voulez qu'un sous-ensemble d'hôtes sur un réseau accède à un hôte sur un réseau distant protégé par un Pare-feu. Avec l'accès de verrou, vous pouvez permettre seulement à un ensemble désiré d'hôtes d'accéder en les ayant authentifiez par un serveur

TACACS+ ou de RAYON.

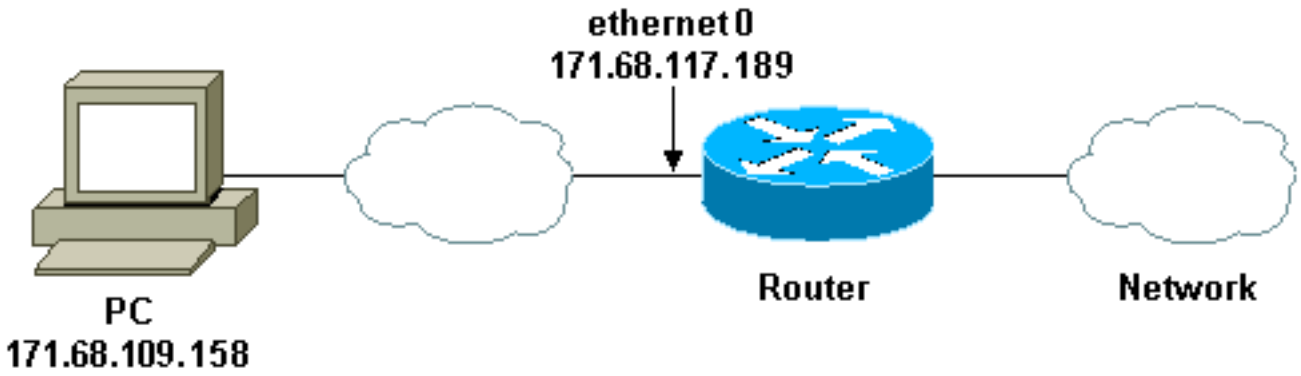
## Exécution d'Access de verrou

Ce processus décrit l'exécution d'accès de verrou.

1. Un utilisateur ouvre une session de telnet à un routeur de cadre configuré pour l'accès de verrou.
2. Le logiciel de Cisco IOS reçoit le paquet de telnet. Il exécute un processus d'authentification de l'utilisateur. L'utilisateur doit passer l'authentification avant qu'on permette l'accès. La procédure d'authentification est faite par le routeur ou un serveur d'accès central tel qu'un serveur TACACS+ ou de RAYON.

## Configuration et dépannage d'échantillon

### Diagramme du réseau




Cisco recommande que vous utilisiez un serveur TACACS+ pour votre processus de requête d'authentification. TACACS+ fournit l'authentification, l'autorisation, et les services de comptabilité. Il fournit également le support de protocole, la spécification de protocole, et une base de données centralisée de Sécurité.

Vous pouvez authentifier l'utilisateur sur le routeur ou avec un serveur TACACS+ ou de RAYON.

**Remarque:** Ces commandes sont globales sauf indication contraire.

Sur le routeur, vous avez besoin d'un **nom d'utilisateur** pour l'utilisateur pour l'authentification locale.

```
username test password test
```

La présence des **gens du pays de procédure de connexion** sur les lignes vty cause ce nom d'utilisateur d'être utilisé.

```
line vty 0 4
login local
```

Si vous ne faites pas confiance à l'utilisateur pour émettre la commande d'**access-enable**, vous pouvez faire une de deux choses :

- Associez le délai d'attente avec l'utilisateur sur une base par utilisateur.
  ```
  username test autocommand access-enable host
  timeout 10
  ```
  ou
- Forcez tous les utilisateurs ce telnet dedans pour avoir le même délai d'attente.
  ```
  line vty 0 4
  login local
  autocommand access-enable host timeout 10
  ```

Remarque: Les 10 dans la syntaxe est le délai d'attente *de veille de la* liste d'accès. Il est ignoré par la temporisation absolue dans la liste d'accès dynamique.

Définissez une liste d'accès étendue qui est appliquée quand un utilisateur (tout utilisateur) se connecte dans le routeur et la commande d'access-enable est émis. Le moment absolu maximum pour ce « trou » dans le filtre est placé à 15 minutes. Après 15 minutes, le trou se ferme si n'importe qui l'utilise. Le testlist de nom doit exister mais être non significatif. Limitez les réseaux auxquels l'utilisateur a accès en configurant l'adresse source ou de destination (ici, l'utilisateur n'est pas limité).

```
access-list 120 dynamic testlist timeout 15 permit ip any any
```

Définissez la liste d'accès requise pour bloquer tout à moins que la capacité au telnet dans le routeur (afin d'ouvrir un trou, le telnet des besoins de l'utilisateur au routeur). L'adresse IP ici est l'adresse IP d'Ethernets du routeur.

```
access-list 120 permit tcp any host 171.68.117.189 eq telnet
```

Il y a un implicite refusent tous à l'extrémité (non entrée ici).

Appliquez cette liste d'accès à l'interface sur dans laquelle les utilisateurs sont livré.

```
interface ethernet1
       ip access-group 120 in
```

Vous êtes fait.

C'est ce qui ressemble au filtre sur le routeur en ce moment :

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Les utilisateurs qui obtiennent l'accès à votre réseau interne ne peuvent pas voir n'importe quoi jusqu'à eux telnet au routeur.

Remarque: Les 10 voici le délai d'attente *de veille de la* liste d'accès. Il est ignoré par la temporisation absolue dans la liste d'accès dynamique.

```
%telnet 2514A
Trying 171.68.117.189 ...
Connected to 2514A.network.com.
Escape character is '^]'.

User Access Verification

Username: test
Password: test
```

```
Connection closed by foreign host.
```

Le filtre ressemble à ceci.

```
Router#show access-lists
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.158 any log (time left 394)
    20 permit tcp any host 171.68.117.189 eq telnet (68 matches)
```

Il y a un trou dans le filtre pour cet un utilisateur basé sur l'adresse IP source. Quand quelqu'un d'autre fait ceci, vous voyez *deux trous*.

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

Ces utilisateurs peuvent avoir accès complet IP à n'importe quelle adresse IP de destination de leur *adresse IP source*.

## Utilisant TACACS+

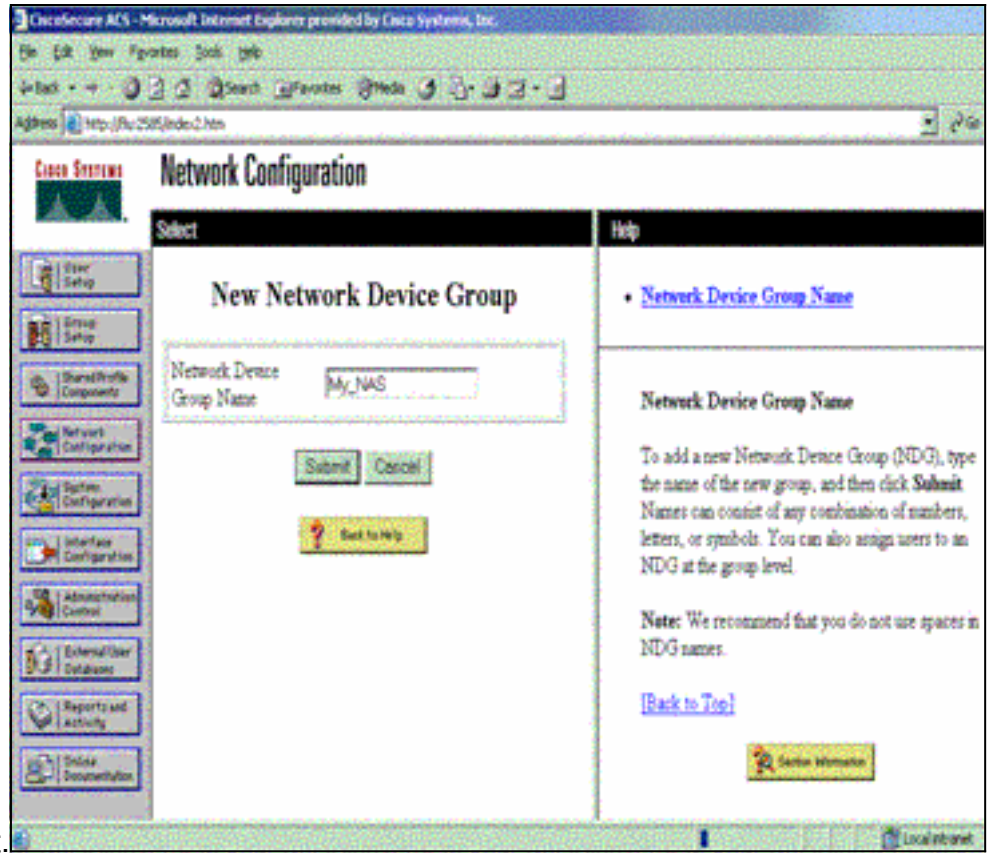
### Configurez TACACS+

Configurez un serveur TACACS+ pour forcer l'authentification et l'autorisation d'être fait sur le serveur TACACS+ afin d'utiliser TACACS+, comme cette sortie affiche :

```
Router#show ip access-lists 120
Extended IP access list 120
    10 Dynamic testlist permit ip any any log
       permit ip host 171.68.109.64 any log
       permit ip host 171.68.109.158 any log
    20 permit tcp any host 171.68.117.189 eq telnet (288 matches)
```

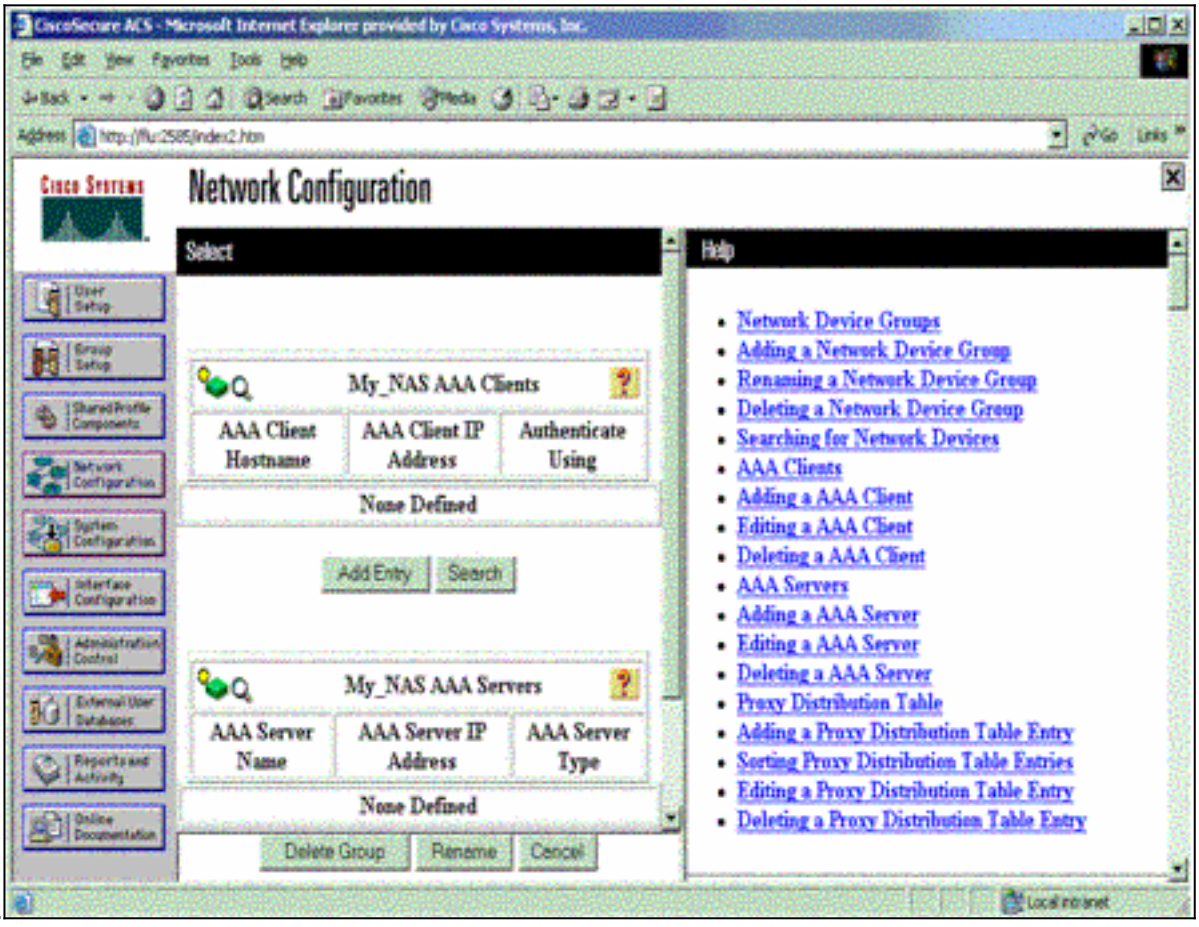
Terminez-vous ces étapes pour configurer TACACS+ sur le Cisco Secure ACS pour Windows :

1. Ouvrez un navigateur Web. Introduisez l'adresse de votre serveur ACS, qui est sous forme de *<IP_address de* http:// *ou de DNS_name>:2002*. (Cet exemple utilise un port par défaut de 2002.) Procédure de connexion comme admin.
2. Cliquez sur Network Configuration. Cliquez sur Add l'**entrée** pour créer un groupe de périphériques réseau qui contient les serveurs d'accès à distance (NAS). Écrivez un nom pour le groupe et cliquez sur



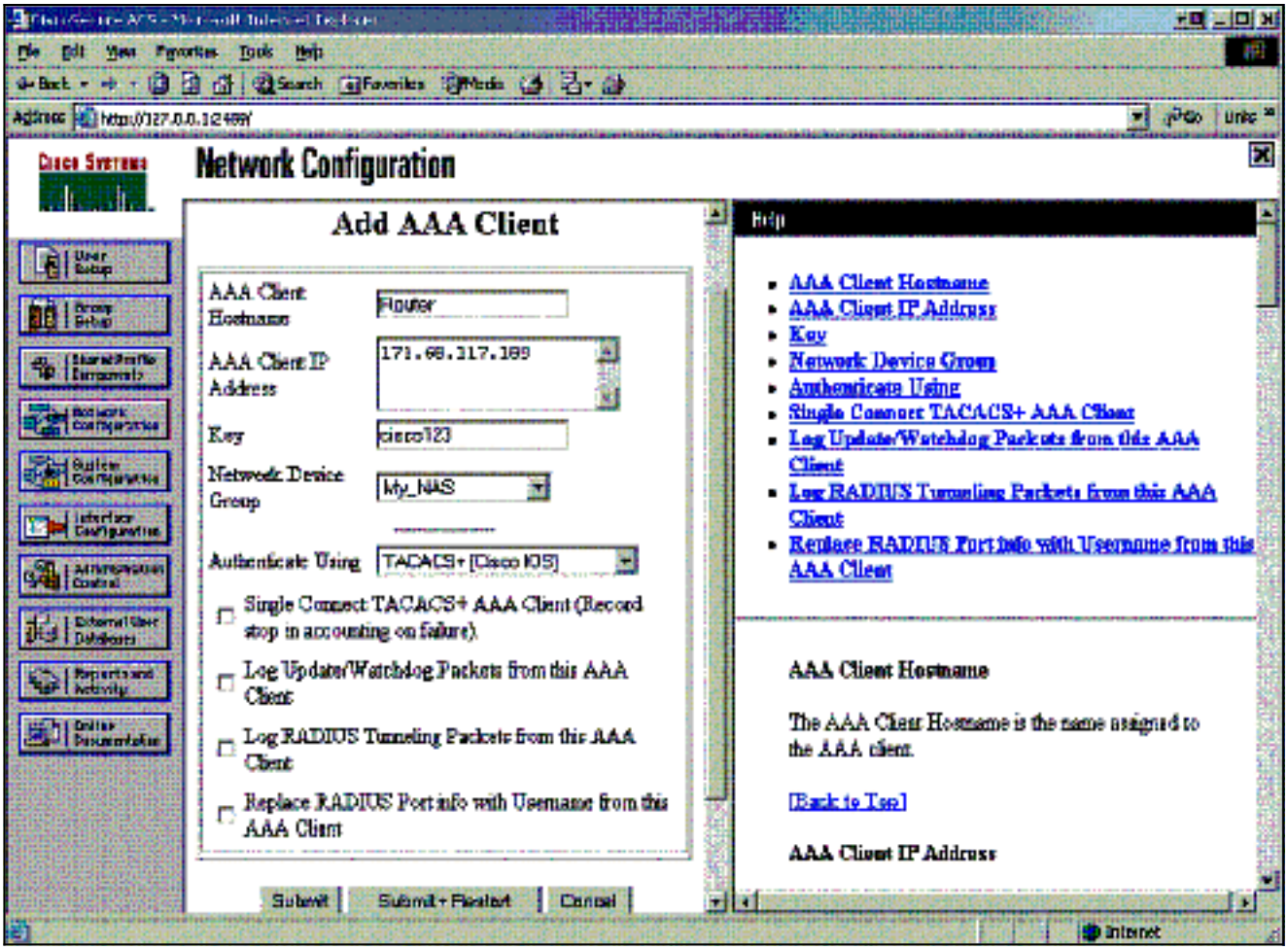

Submit.

3. Cliquez sur Add l'**entrée** pour ajouter un client d'Authentification, autorisation et comptabilité (AAA)

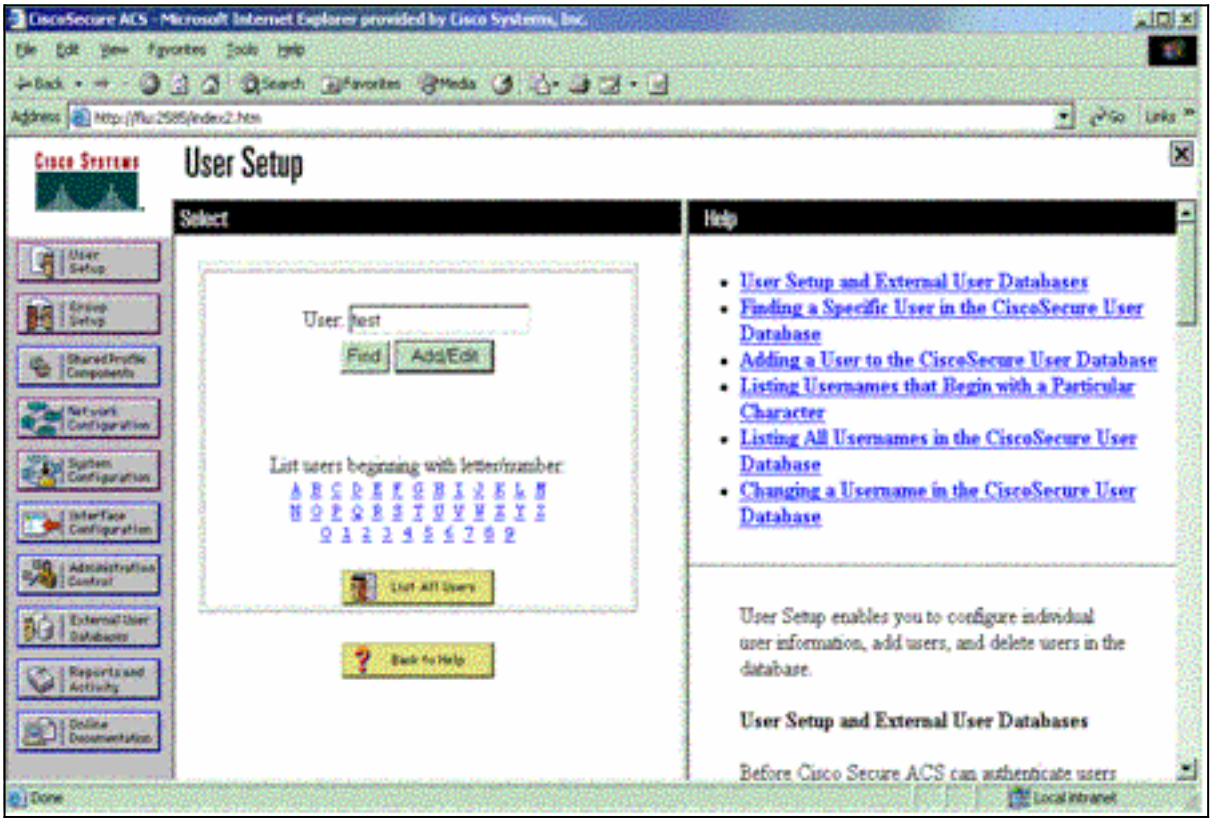



(NAS).

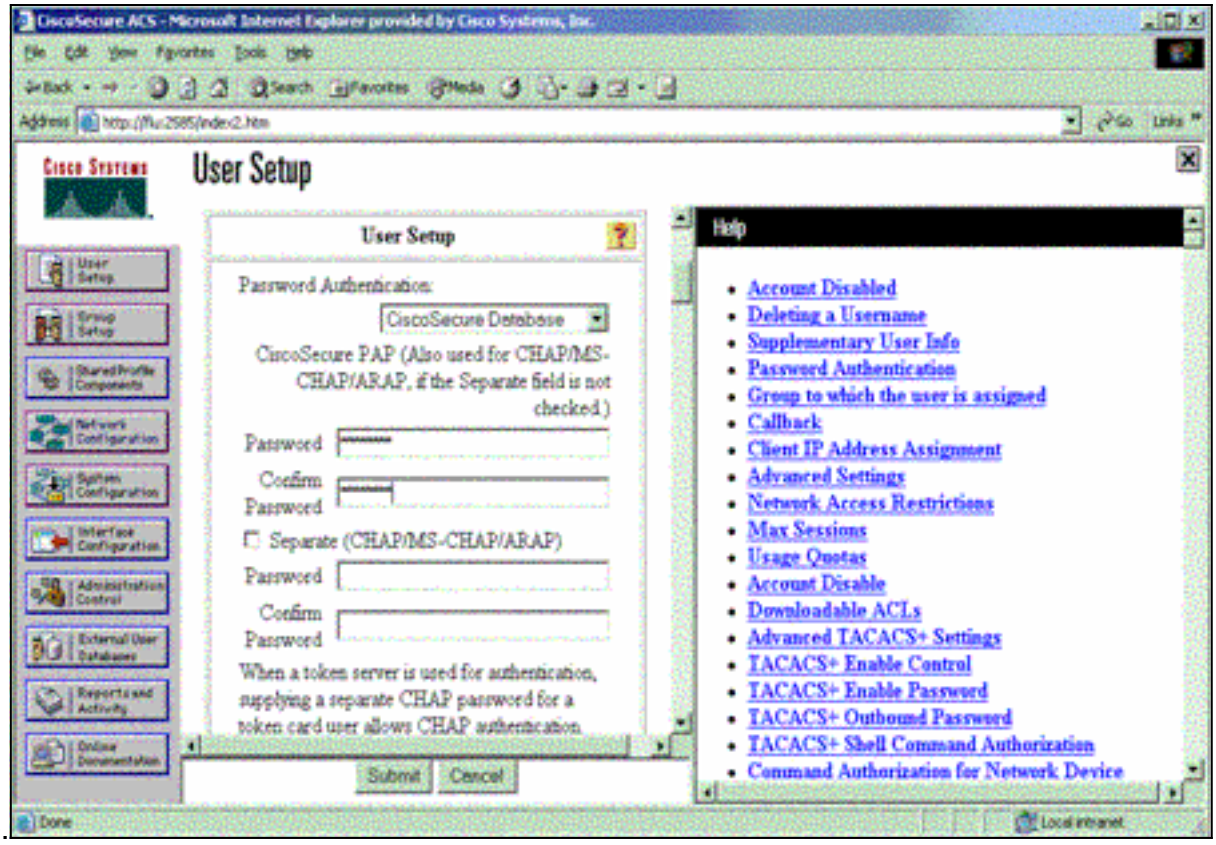
4. Introduisez le nom d'hôte, l'adresse IP, et la clé utilisée pour chiffrer la transmission entre le serveur d'AAA et le NAS. **TACACS+** choisi **(Cisco IOS)** comme méthode d'authentification. Quand vous êtes de finition, cliquez sur Submit **+Restart** pour appliquer les modifications.




5. Cliquez sur User Setup, écrivez un user-id, et cliquez sur Add/l'éditez.

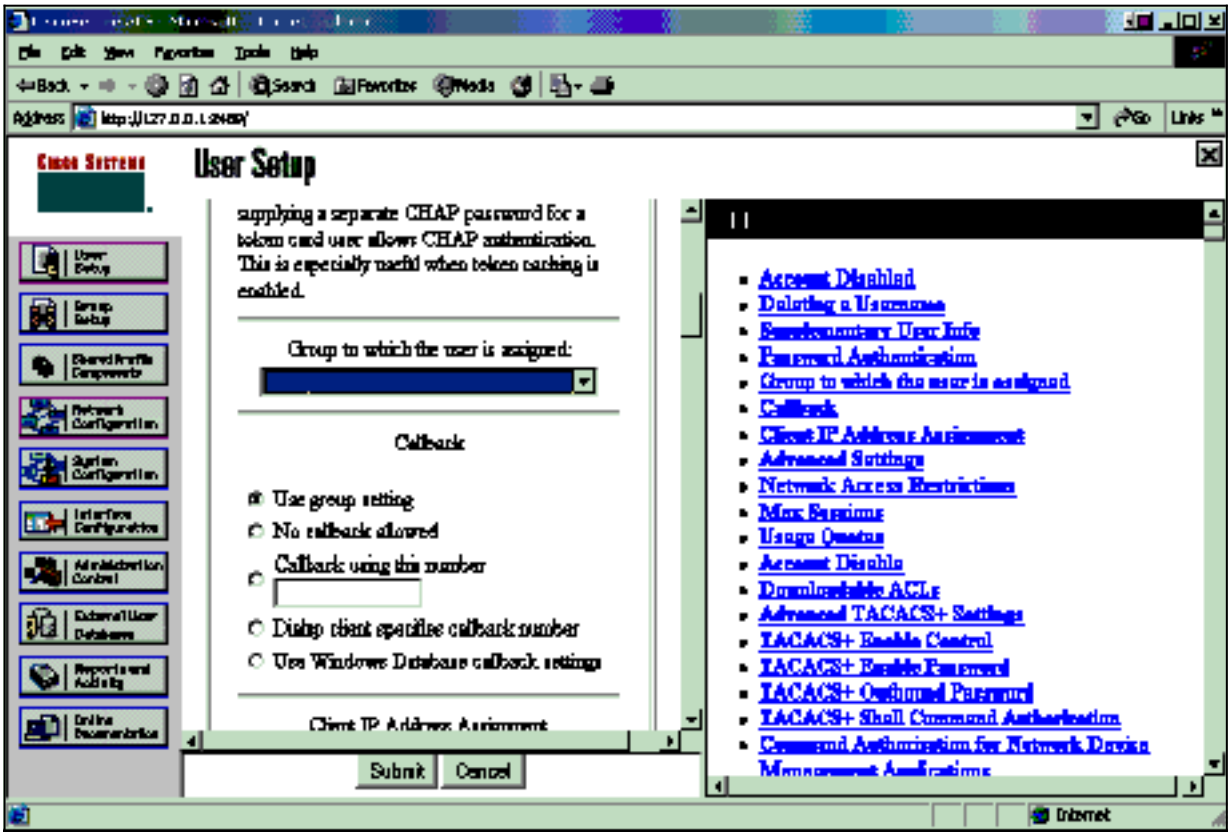



6. Choisissez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur, et confirmez le mot de

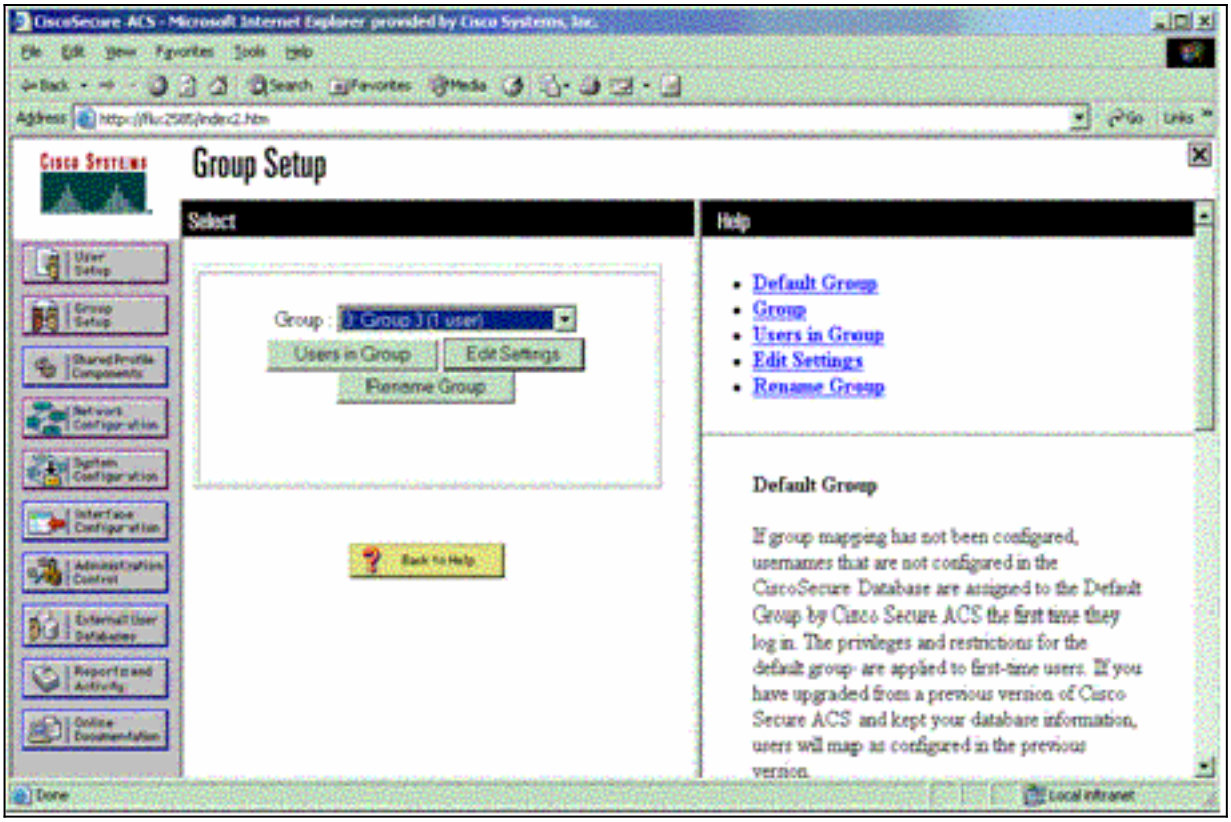



passe.

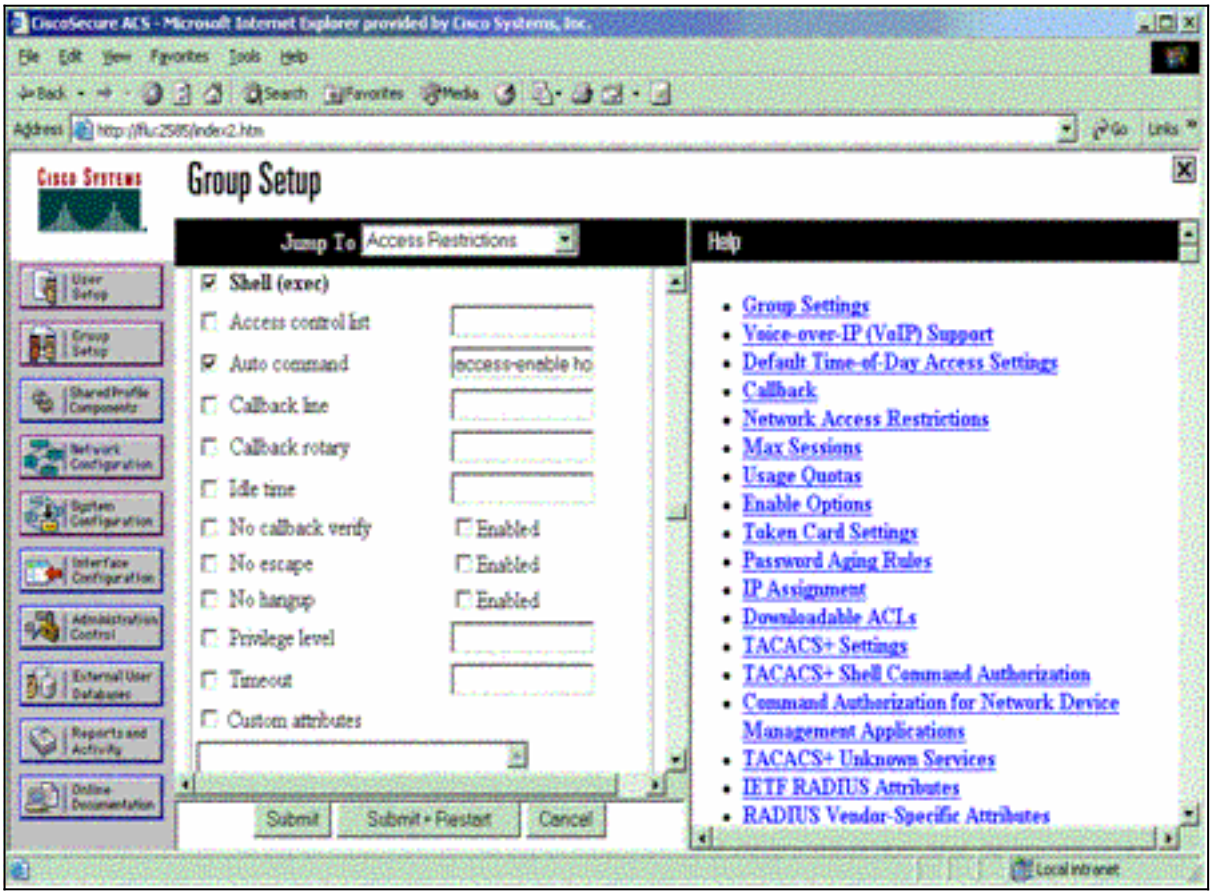
7. Choisissez le groupe auquel l'utilisateur est assigné et vérifiez la **configuration de groupe d'utilisation**. Cliquez sur **Submit**.




8. **Group Setup de** clic. Sélectionnez le groupe auquel l'utilisateur a été assigné dans l'étape 7. cliquent sur Edit des **configurations**.




9. Faites descendre l'écran à la section de configurations TACACS+. Cochez la case pour l'**exécutif de shell**. Cochez la case pour la **commande auto**. Sélectionnez la commande d'être exécuté sur l'autorisation réussie de l'utilisateur. (Cet exemple utilise la commande du **délai d'attente 10 d'hôte d'access-enable**.) Clic **Submit+Restart**.




[Dépannez TACACS+]

Utilisez ces commandes de **débogage** sur le NAS de dépanner des problèmes TACACS+.

**Remarque:** Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **authentification de debug tacacs** — Affiche des informations sur la procédure d'authentification TACACS+. Seulement disponible dans quelques versions de logiciel. S'indisponible, utilisez le **debug tacacs** seulement.
- **autorisation de debug tacacs** — Affiche des informations sur le processus d'autorisation TACACS+. Seulement disponible dans quelques versions de logiciel. S'indisponible, utilisez le **debug tacacs** seulement.
- **événements de debug tacacs** — Affiche des informations du processus d'aide TACACS+. Seulement disponible dans quelques versions de logiciel. S'indisponible, utilisez le **debug tacacs** seulement.

Utilisez ces commandes de dépanner des problèmes d'AAA :

- **debug aaa authentication** — Affiche des informations sur l'authentification AAA/TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie de débogage ici affiche une authentification et un processus réussis d'autorisation sur le serveur ACS TACACS+.

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
 TPLUS: Authentication start packet created for 9()
 TPLUS: Using server 10.48.66.53
 TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
 TPLUS(00000009)/0/82A2E088: Processing the reply packet
 TPLUS: Received authen response status GET_USER (7)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 16 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 28 bytes response
```

```
 TPLUS(00000009)/0/8347F3FC: Processing the reply packet
 TPLUS: Received authen response status GET_PASSWORD (8)
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication continue request id 9
 TPLUS: Authentication continue packet generated for 9
 TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
 TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 6 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 18 bytes response
 TPLUS(00000009)/0/8347EE4C: Processing the reply packet
 TPLUS: Received authen response status PASS (2)
 AAA/AUTHOR (0x9): Pick method list 'default'
 TPLUS: Queuing AAA Authorization request 9 for processing
 TPLUS: processing authorization request id 9
 TPLUS: Protocol set to None .....Skipping
 TPLUS: Sending AV service=shell
 TPLUS: Sending AV cmd
 TPLUS: Authorization request created for 9(tne-1)
 TPLUS: using previously set server 10.48.66.53
   from group tacacs+
 TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
 TPLUS(00000009)/0/NB_WAIT: socket event 2
 TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: Would block while reading
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 12 header bytes
   (expect 44 bytes data)
 TPLUS(00000009)/0/READ: socket event 1
 TPLUS(00000009)/0/READ: read entire 56 bytes response
 TPLUS(00000009)/0/8347F508: Processing the reply packet
 TPLUS: Processed AV autocmd=access-enable host timeout 10
 TPLUS: received authorization response for 9: PASS
 AAA/AUTHOR/EXEC(00000009): processing AV cmd=
 AAA/AUTHOR/EXEC(00000009): processing AV
   autocmd=access-enable host timeout 10
 AAA/AUTHOR/EXEC(00000009): Authorization successful
```

## Utilisant le RAYON

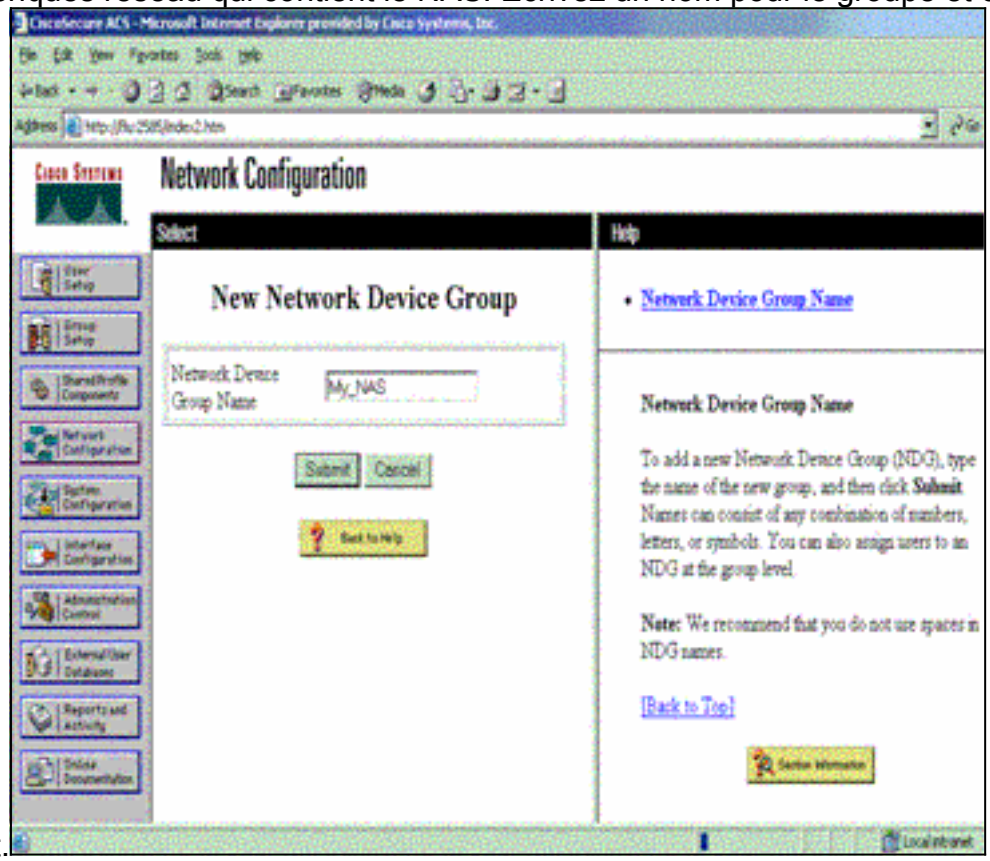
### Configurez le RAYON

Afin d'utiliser le RAYON, configurez un serveur de RAYON pour forcer l'authentification à faire sur le serveur de RAYON avec des paramètres d'autorisation (l'autocommand) à envoyer vers le bas dans l'attribut 26 de constructeur-particularité, comme affiché ici :

```
Router#show debug
General OS:
  TACACS+ events debugging is on
  TACACS+ authentication debugging is on
  TACACS+ authorization debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
======================================================
Router#
 AAA/BIND(00000009): Bind i/f
 AAA/AUTHEN/LOGIN (00000009): Pick method list 'default'
 TPLUS: Queuing AAA Authentication request 9 for processing
 TPLUS: processing authentication start request id 9
```

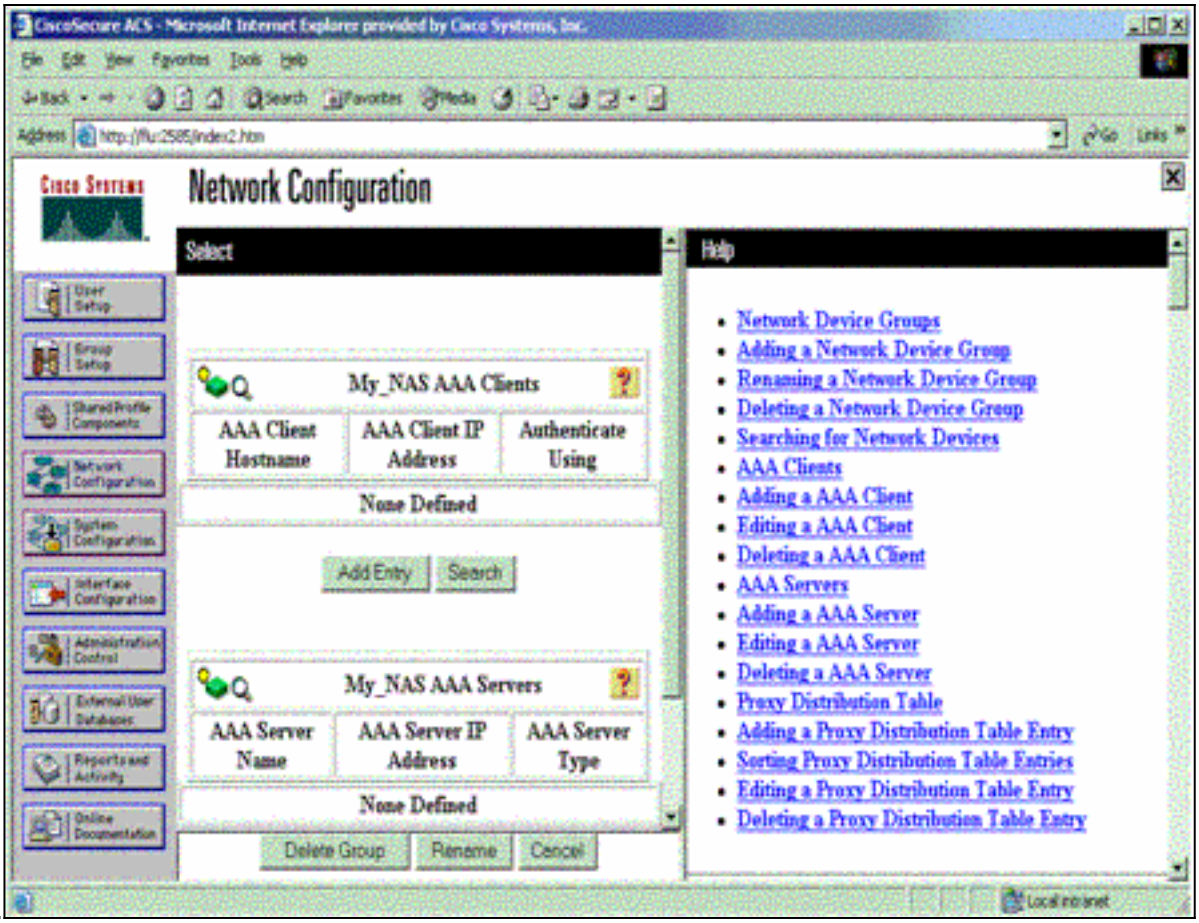
```
TPLUS: Authentication start packet created for 9()
TPLUS: Using server 10.48.66.53
TPLUS(00000009)/0/NB_WAIT/82A2E088: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 36 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/82A2E088: Processing the reply packet
TPLUS: Received authen response status GET_USER (7)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347F3FC: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 22 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 16 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 28 bytes response
TPLUS(00000009)/0/8347F3FC: Processing the reply packet
TPLUS: Received authen response status GET_PASSWORD (8)
TPLUS: Queuing AAA Authentication request 9 for processing
TPLUS: processing authentication continue request id 9
TPLUS: Authentication continue packet generated for 9
TPLUS(00000009)/0/WRITE/8347EE4C: Started 5 sec timeout
TPLUS(00000009)/0/WRITE: wrote entire 25 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 6 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 18 bytes response
TPLUS(00000009)/0/8347EE4C: Processing the reply packet
TPLUS: Received authen response status PASS (2)
AAA/AUTHOR (0x9): Pick method list 'default'
TPLUS: Queuing AAA Authorization request 9 for processing
TPLUS: processing authorization request id 9
TPLUS: Protocol set to None .....Skipping
TPLUS: Sending AV service=shell
TPLUS: Sending AV cmd
TPLUS: Authorization request created for 9(tne-1)
TPLUS: using previously set server 10.48.66.53
  from group tacacs+
TPLUS(00000009)/0/NB_WAIT/8347F508: Started 5 sec timeout
TPLUS(00000009)/0/NB_WAIT: socket event 2
TPLUS(00000009)/0/NB_WAIT: wrote entire 60 bytes request
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: Would block while reading
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 12 header bytes
  (expect 44 bytes data)
TPLUS(00000009)/0/READ: socket event 1
TPLUS(00000009)/0/READ: read entire 56 bytes response
TPLUS(00000009)/0/8347F508: Processing the reply packet
TPLUS: Processed AV autocmd=access-enable host timeout 10
TPLUS: received authorization response for 9: PASS
AAA/AUTHOR/EXEC(00000009): processing AV cmd=
AAA/AUTHOR/EXEC(00000009): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000009): Authorization successful
```

Terminez-vous ces étapes pour configurer le RAYON sur le Cisco Secure ACS pour Windows :

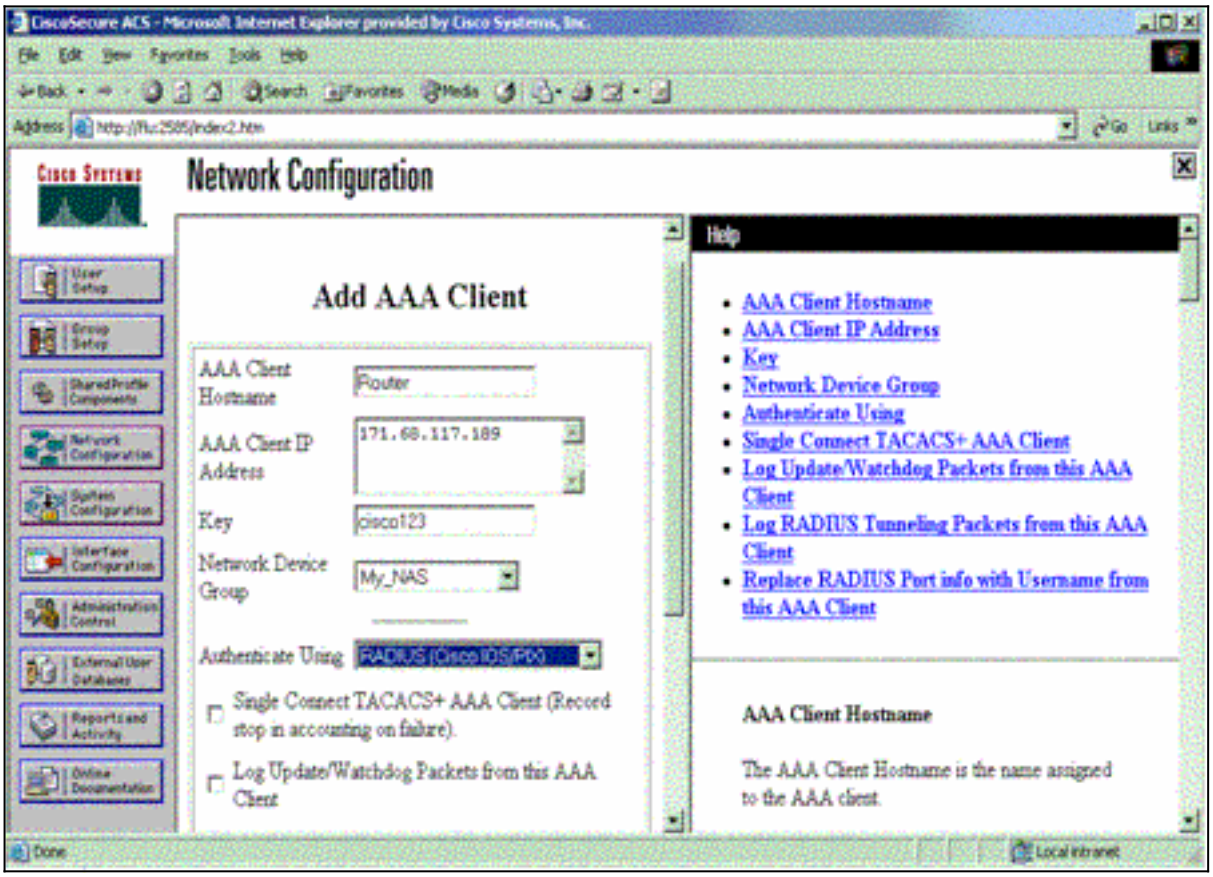
1. Ouvrez un navigateur Web et introduisez l'adresse de votre serveur ACS, qui est sous forme de *<IP_address de* http:// *ou de DNS_name>:2002*. (Cet exemple utilise un port par défaut de 2002.) Procédure de connexion comme admin.
2. Cliquez sur Network Configuration. Cliquez sur Add l'entrée pour créer un groupe de périphériques réseau qui contient le NAS. Écrivez un nom pour le groupe et cliquez sur Submit. 

3. Cliquez sur Add l'entrée pour ajouter un client d'AAA

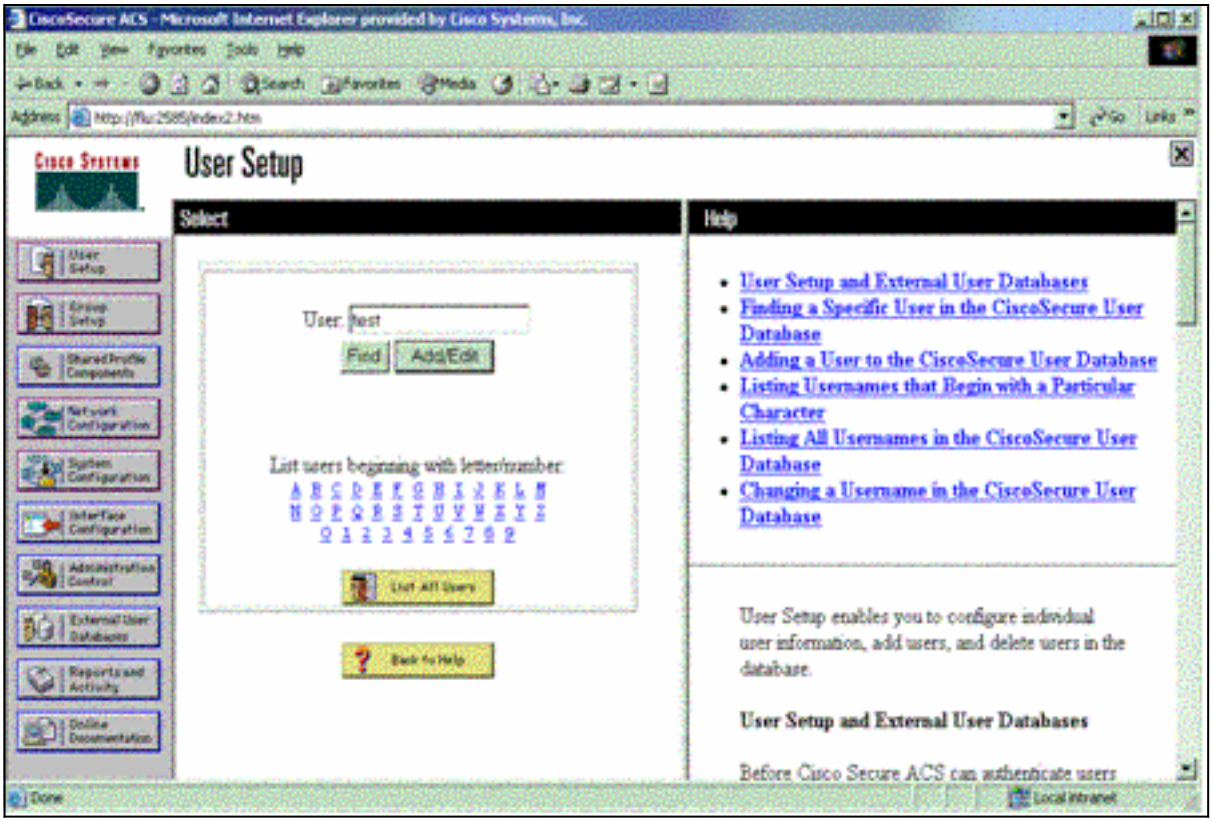
(NAS).



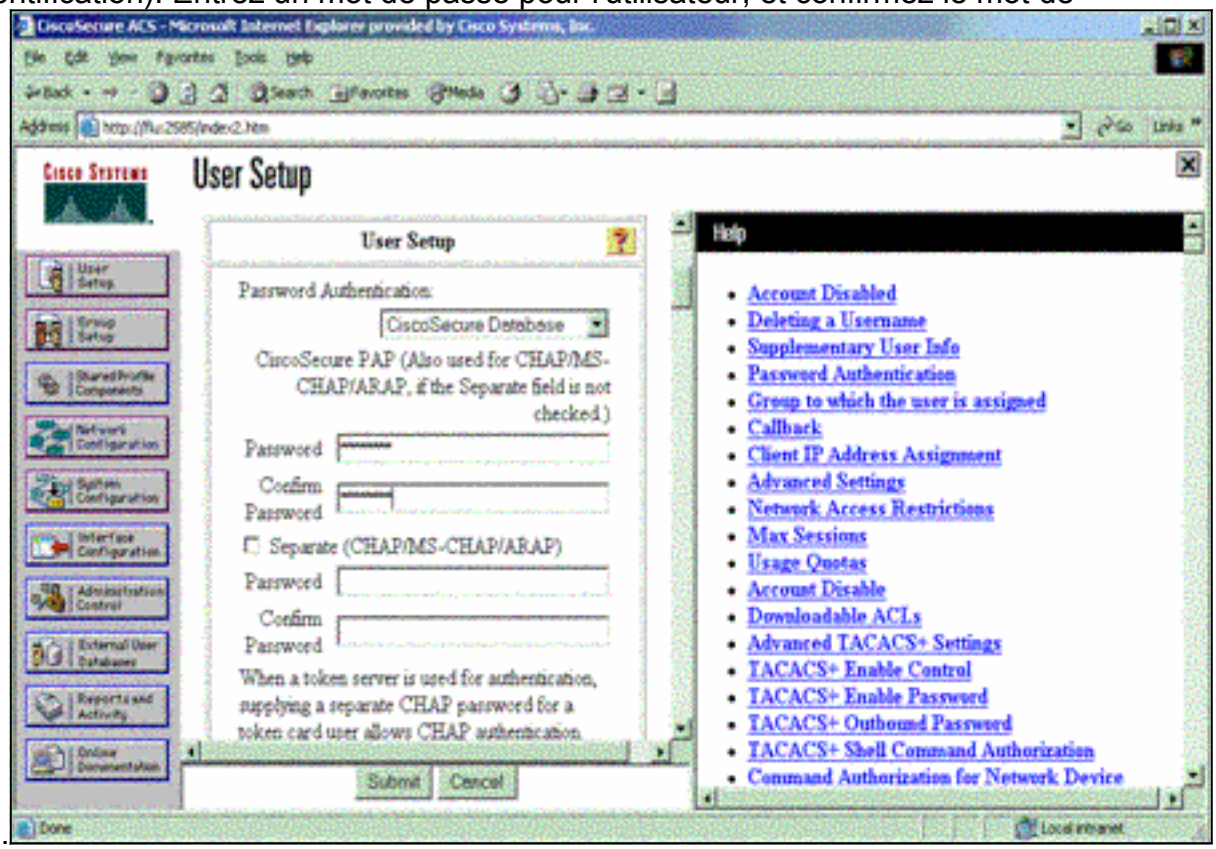

4. Introduisez le nom d'hôte, l'adresse IP, et la clé utilisée pour chiffrer la transmission entre le serveur d'AAA et le NAS. **RAYON** choisi **(Cisco IOS/PIX)** comme méthode d'authentification. Quand vous êtes de finition, cliquez sur Submit **+Restart** pour appliquer les modifications.



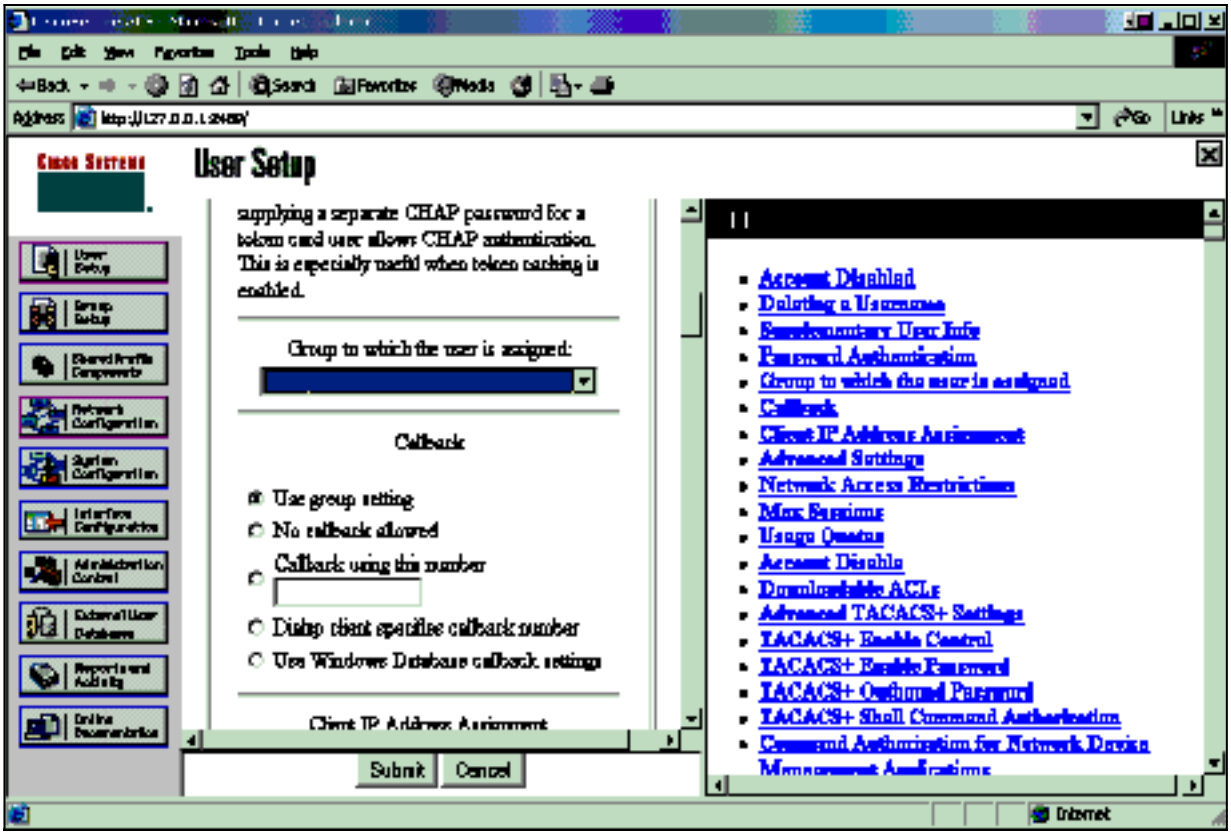

5. Cliquez sur User Setup, écrivez un user-id, et cliquez sur Add/**l'éditez**.



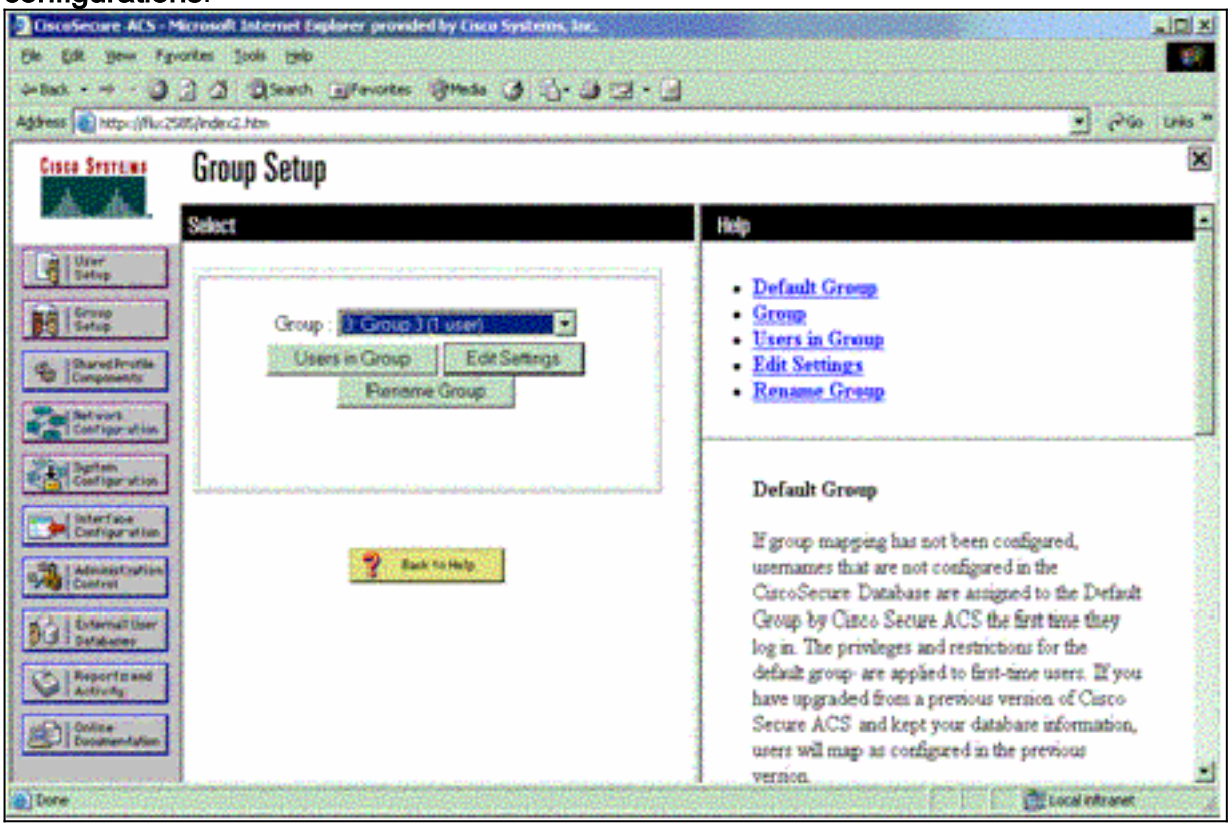

6. Choisissez une base de données pour authentifier l'utilisateur. (Dans cet exemple, l'utilisateur est « test » et la base de données interne de l'ACS est utilisée pour l'authentification). Entrez un mot de passe pour l'utilisateur, et confirmez le mot de passe.



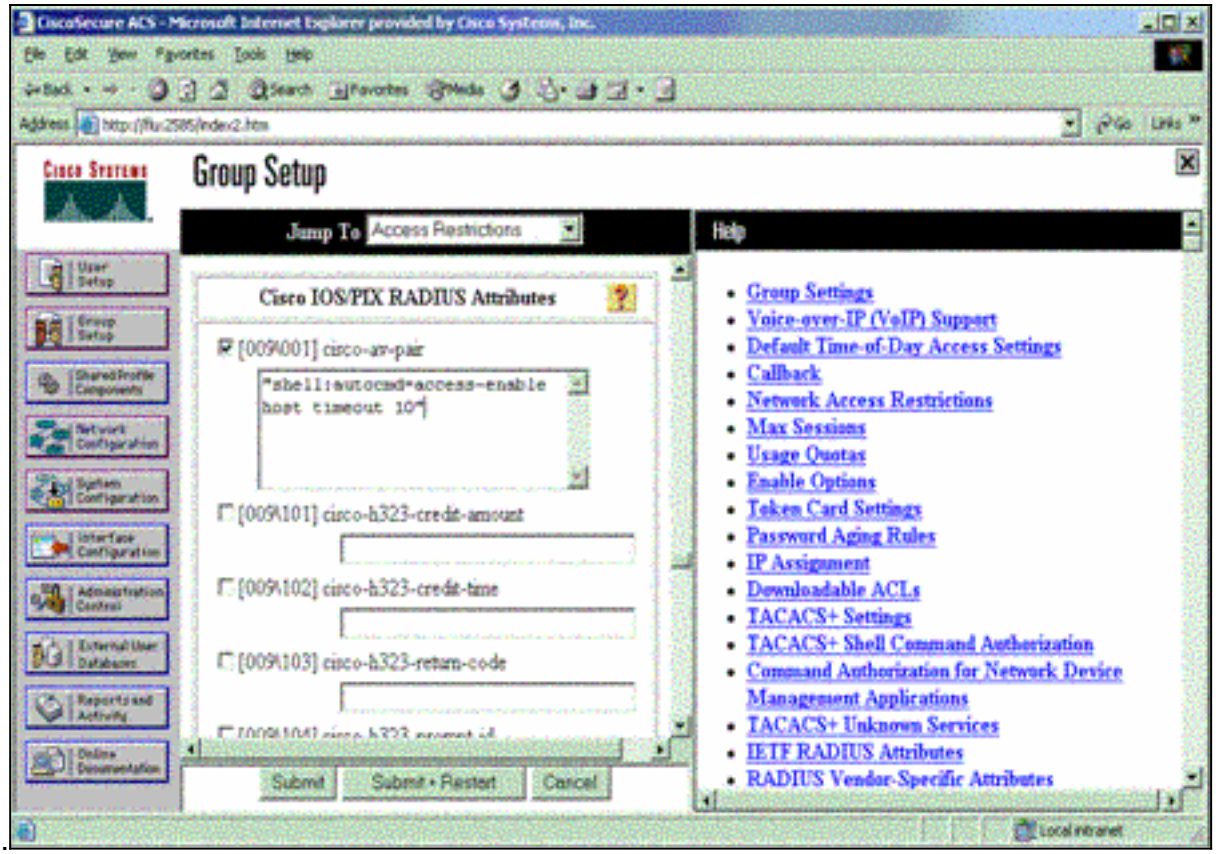

7. Choisissez le groupe auquel l'utilisateur est assigné et vérifiez la **configuration de groupe d'utilisation**. Cliquez sur **Submit**.




8. Cliquez sur le **Group Setup** et sélectionnez le groupe auquel l'utilisateur a été assigné dans l'étape précédente. Cliquez sur Edit les **configurations**.




9. Faites descendre l'écran à la section d'attributs RADIUS de Cisco IOS/PIX. Cochez la case pour des Cisco-poids du commerce-**paires**. Sélectionnez la **commande shell** d'être exécuté sur l'autorisation réussie de l'utilisateur. (Cet exemple utilise le **shell :** clic **autocmd=access-enable Submit+Restart du délai d'attente 10.**

d'hôte). 


## Dépannez le RAYON

Utilisez ces commandes de **débogage** sur le NAS de dépanner des problèmes de RAYON.

**Remarque:** Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug radius** — Affiche des informations associée avec le RAYON.

Utilisez ces commandes de dépanner des problèmes d'AAA :

- **debug aaa authentication** — Affiche des informations sur l'authentification AAA/TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.

L'exemple de sortie de débogage ici affiche une authentification et un processus réussis d'autorisation sur l'ACS configuré pour le RAYON.

```
Router#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on

Radius protocol debugging is on
Radius packet protocol debugging is on
=======================================================
Router#
 AAA/BIND(00000003): Bind i/f
 AAA/AUTHEN/LOGIN (00000003): Pick method list 'default'
 RADIUS/ENCODE(00000003): ask "Username: "
 RADIUS/ENCODE(00000003): send packet; GET_USER
 RADIUS/ENCODE(00000003): ask "Password: "
 RADIUS/ENCODE(00000003): send packet; GET_PASSWORD
 RADIUS:  AAA Unsupported     [152] 5
 RADIUS:   74 74 79                        [tty]
```

```
RADIUS(00000003): Storing nasport 66 in rad_db
RADIUS/ENCODE(00000003): dropping service type,
  "radius-server attribute 6 on-for-login-auth" is off
RADIUS(00000003): Config NAS IP: 0.0.0.0
RADIUS/ENCODE(00000003): acct_session_id: 1
RADIUS(00000003): sending
RADIUS/ENCODE: Best Local IP-Address 172.18.124.1
  for Radius-Server 10.48.66.53
RADIUS(00000003): Send Access-Request to 10.48.66.53:1645
  id 21645/1, len 77
RADIUS:  authenticator 5A 95 1F EA A7 94 99 E5 -
  BE B5 07 BD E9 05 5B 5D
RADIUS:  User-Name           [1]   7   "test"
RADIUS:  User-Password       [2]   18  *
RADIUS:  NAS-Port            [5]   6   66
RADIUS:  NAS-Port-Type       [61]  6   Virtual     [5]
RADIUS:  Calling-Station-Id  [31]  14  "171.68.109.158"
RADIUS:  NAS-IP-Address      [4]   6   171.68.117.189
RADIUS: Received from id 21645/1 10.48.66.53:1645,
  Access-Accept, len 93
RADIUS:  authenticator 7C 14 7D CB 33 19 97 19 -
  68 4B C3 FC 25 21 47 CD
RADIUS:  Vendor, Cisco       [26]  51
RADIUS:   Cisco AVpair       [1]   45
  "shell:autocmd=access-enable host timeout 10"
RADIUS:  Class               [25]  22
RADIUS:   43 49 53 43 4F 41 43 53 3A 61 63 31 32 37 63 30
  [CISCOACS:ac127c0]
RADIUS:   31 2F 36 36                [1/66]
RADIUS(00000003): Received from id 21645/1
AAA/AUTHOR/EXEC(00000003): processing AV
  autocmd=access-enable host timeout 10
AAA/AUTHOR/EXEC(00000003): Authorization successful
```

# Informations connexes

- Sécurité de verrou de Cisco IOS
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems