Routeur IOS : Configuration de l'authentification des utilisateurs entrants par proxy d'authentification avec ACS pour IPSec et VPN Client

Contenu

Introduction

La fonction de proxy d'authentification permet aux utilisateurs de se connecter à un réseau ou d'accéder à Internet via HTTP, avec leurs profils d'accès spécifiques automatiquement récupérés et appliqués à partir d'un serveur TACACS+ ou RADIUS. Les profils utilisateur sont actifs uniquement lorsqu'il y a du trafic actif en provenance des utilisateurs authentifiés.

Cette configuration est conçue pour activer le navigateur Web sur 10.1.1.1 et l'orienter vers 10.17.17.17. Comme le client VPN est configuré pour passer par le point d'extrémité du tunnel 10.31.1.111 pour accéder au réseau 10.17.17.x, le tunnel IPSec est construit et le PC obtient l'adresse IP du pool RTP-POOL (puisque la configuration en mode est effectuée). L'authentification est ensuite demandée par le routeur Cisco 3640. Une fois que l'utilisateur a entré un nom d'utilisateur et un mot de passe (stockés sur le serveur TACACS+ à l'adresse 10.14.14.3), la liste d'accès transmise depuis le serveur est ajoutée à la liste d'accès 118.

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, assurez-vous de respecter les conditions suivantes :

- Le client VPN Cisco est configuré pour établir un tunnel IPSec avec le routeur Cisco 3640.
- Le serveur TACACS+ est configuré pour le proxy d'authentification. Voir la section « Informations connexes » pour plus d'informations.

Components Used

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

- Cisco IOS Version logicielle 12.4
- Routeur Cisco 3640
- Client VPN Cisco pour Windows version 4.8 (tout client VPN 4.x et ultérieur doit fonctionner)

Remarque : La commande **ip auth-proxy** a été introduite dans le logiciel Cisco IOS Version 12.0.5.T. Cette configuration a été testée avec le logiciel Cisco IOS Version 12.4.

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

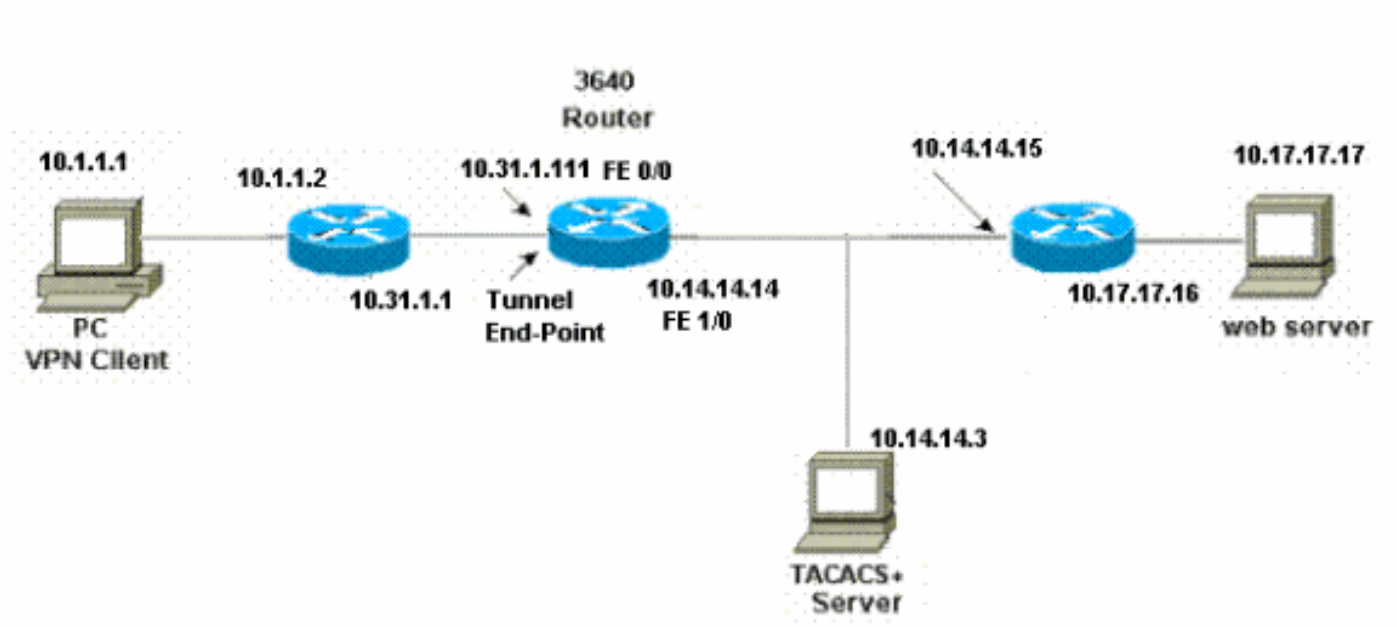
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configuration

Routeur 3640

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 3640
!
!--- The username and password is used during local
authentication. username rtpuser password 0 rtpuserpass

!--- Enable AAA. aaa new-model

!--- Define server-group and servers for TACACS+. aaa
group server tacacs+ RTP
 server 10.14.14.3
!

!--- In order to set authentication, authorization, and
accounting (AAA) authentication at login, use the aaa
authentication login command in global configuration
mode

aaa authentication login default group RTP local
aaa authentication login userauth local
aaa authorization exec default group RTP none
aaa authorization network groupauth local
aaa authorization auth-proxy default group RTP
enable secret 5 $1$CQHC$R/07uQ44E2JgVuCsOUWdG1
enable password ww
!
ip subnet-zero
!
!--- Define auth-proxy banner, timeout, and rules. ip
auth-proxy auth-proxy-banner http ^C
Please Enter Your Username and Password:
```

```
^C
ip auth-proxy auth-cache-time 10
ip auth-proxy name list_a http
ip audit notify log
ip audit po max-events 100
cns event-service server
!
!--- Define ISAKMP policy. crypto isakmp policy 10
 hash md5
 authentication pre-share
 group 2

!--- These commands define the group policy that !--- is
enforced for the users in the group RTPUSERS. !--- This
group name and the key should match what !--- is
configured on the VPN Client. The users from this !---
group are assigned IP addresses from the pool RTP-POOL.
crypto isakmp client configuration group RTPUSERS
 key cisco123
 pool RTP-POOL
!
!--- Define IPSec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
!
crypto dynamic-map RTP-DYNAMIC 10
 set transform-set RTP-TRANSFORM
!
!--- Define extended authentication (X-Auth) using the
local database. !--- This is to authenticate the users
before they can !--- use the IPSec tunnel to access the
resources. crypto map RTPCLIENT client authentication
list userauth

!--- Define authorization using the local database. !---
This is required to push the 'mode configurations' to
the VPN Client. crypto map RTPCLIENT isakmp
authorization list groupauth
crypto map RTPCLIENT client configuration address
initiate
crypto map RTPCLIENT client configuration address
respond
crypto map RTPCLIENT 10 ipsec-isakmp dynamic RTP-DYNAMIC
!
interface FastEthernet0/0
 ip address 10.31.1.111 255.255.255.0
 ip access-group 118 in
 no ip directed-broadcast

!--- Apply the authentication-proxy rule to the
interface. ip auth-proxy list_a
 no ip route-cache
 no ip mroute-cache
 speed auto
 half-duplex

!--- Apply the crypto-map to the interface. crypto map
RTPCLIENT
!
interface FastEthernet1/0
 ip address 10.14.14.14 255.255.255.0
 no ip directed-broadcast
 speed auto
 half-duplex
```

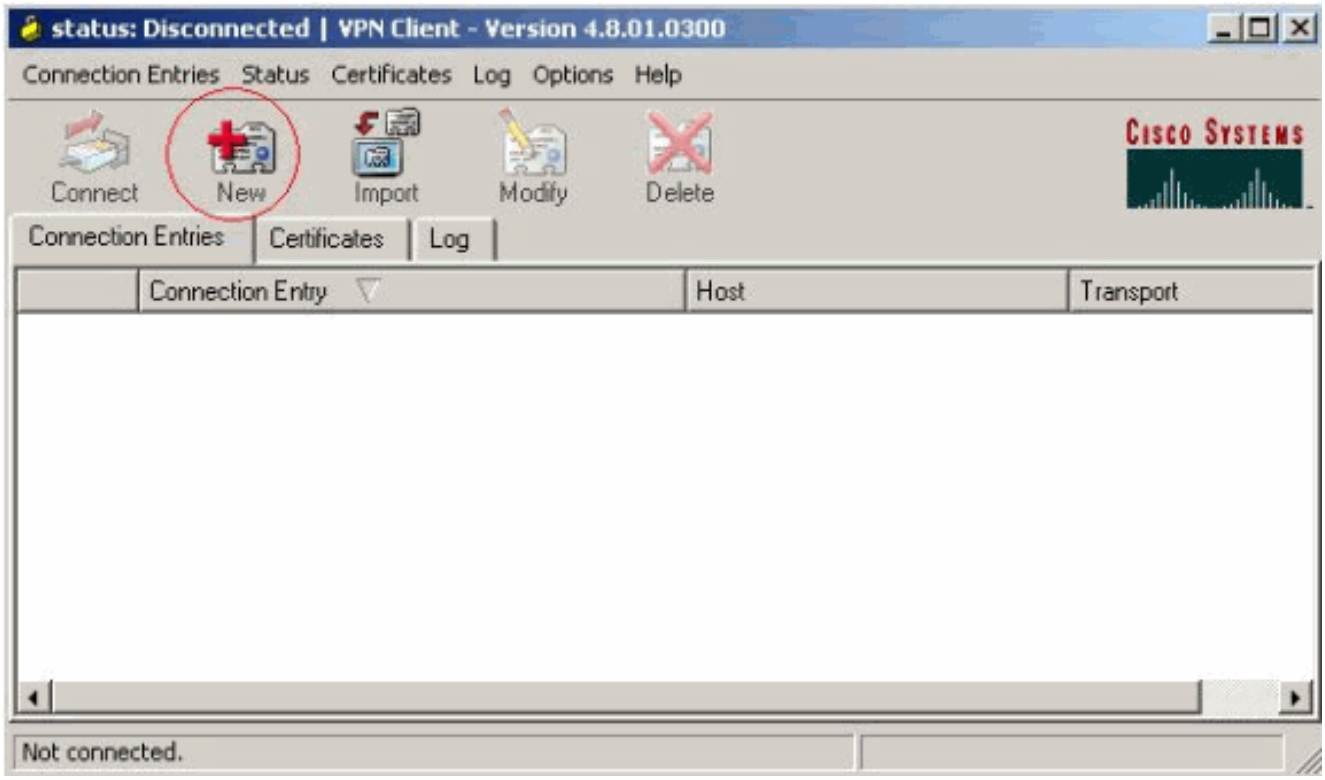
```
!
!--- Define the range of addresses in the pool. !--- VPN
Clients will have thier 'internal addresses' assigned !-
-- from this pool. ip local pool RTP-POOL 10.20.20.25
10.20.20.50
ip classless
ip route 0.0.0.0 0.0.0.0 10.14.14.15
ip route 10.1.1.0 255.255.255.0 10.31.1.1

!--- Turn on the HTTP server and authentication. !---
This is required for http auth-proxy to work. ip http
server
ip http authentication aaa
!
!--- The access-list 118 permits ISAKMP and IPSec
packets !--- to enable the Cisco VPN Client to establish
the IPSec tunnel. !--- The last line of the access-list
118 permits communication !--- between the TACACS+
server and the 3640 router to enable !--- authentication
and authorization. All other traffic is denied. access-
list 118 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111
access-list 118 permit udp 10.1.1.0 0.0.0.255 host
10.31.1.111 eq isakmp
access-list 118 permit tcp host 10.14.14.3 host
10.31.1.111
!
!--- Define the IP address and the key for the TACACS+
server. tacacs-server host 10.14.14.3 key cisco
!
line con 0
 transport input none
line aux 0
line vty 0 4
 password ww
!
end
```

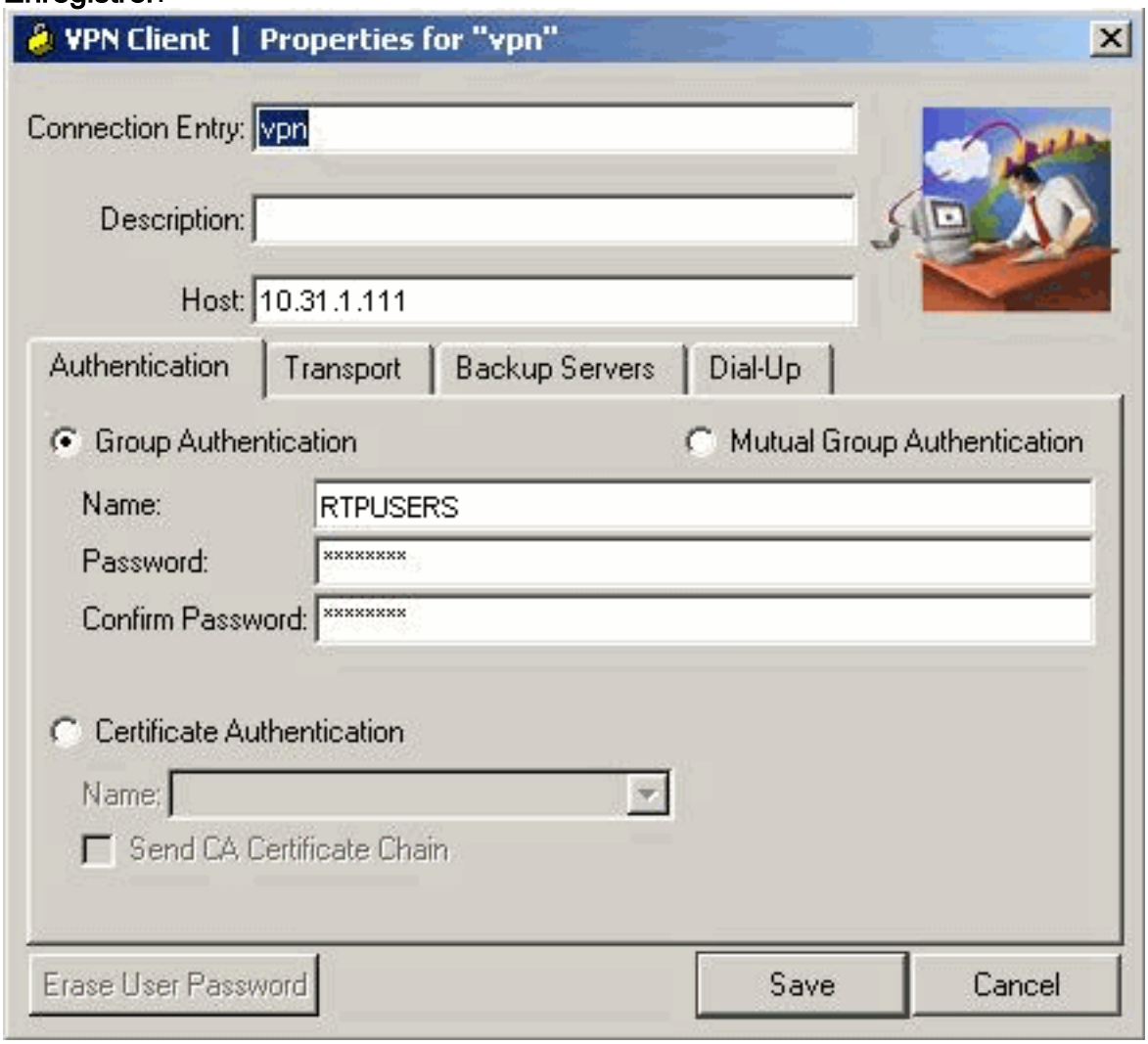
Configuration VPN Client 4.8

Suivez la procédure suivante pour configurer Cisco VPN Client 4.8:

1. Sélectionnez **Start > Programs > Cisco Systems VPN Client > VPN Client** (démarrer > programmes > client VPN Cisco Systems > client VPN).
2. Cliquez **New pour ouvrir la fenêtre Create New VPN Connection Entry.**

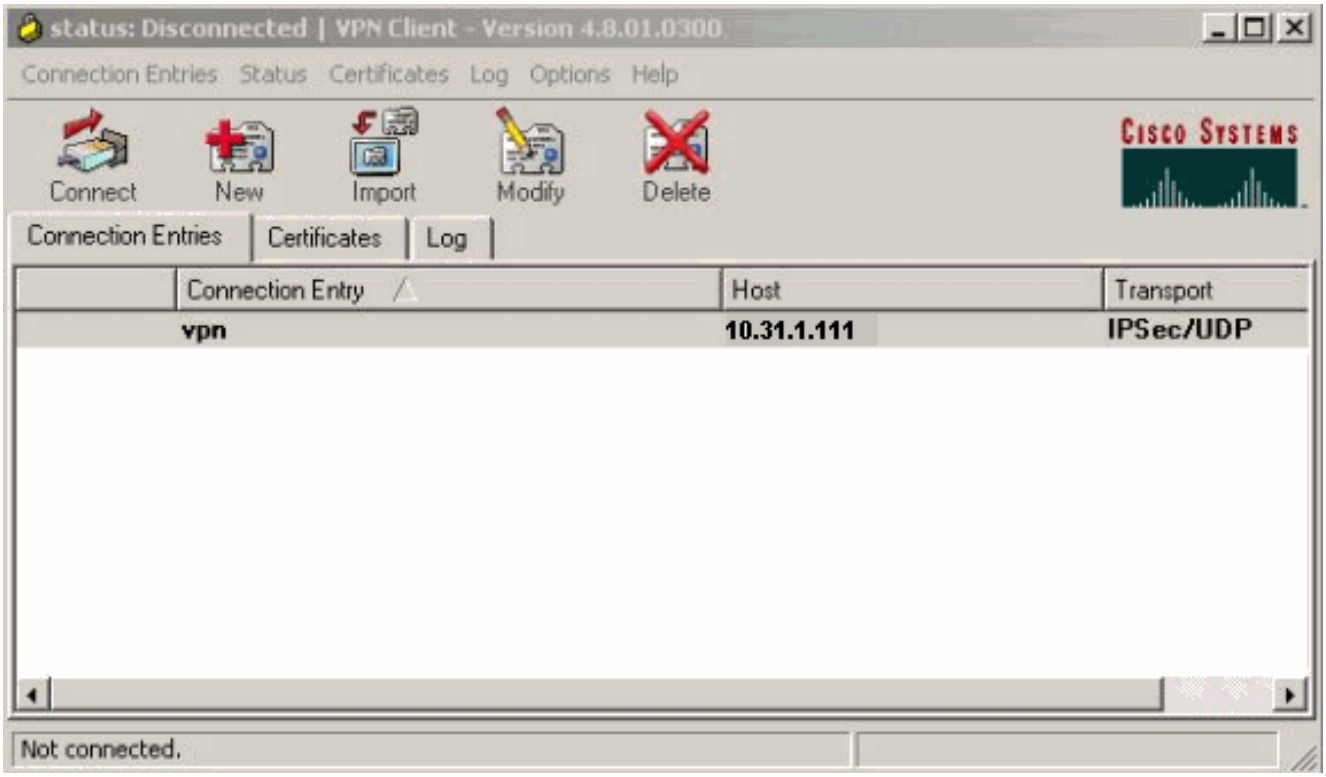


3. Entrez le nom de l'entrée de connexion avec une description. Saisissez l'adresse IP externe du routeur dans la zone Host. Entrez ensuite le nom et le mot de passe du groupe VPN, puis cliquez sur
Enregistrer.

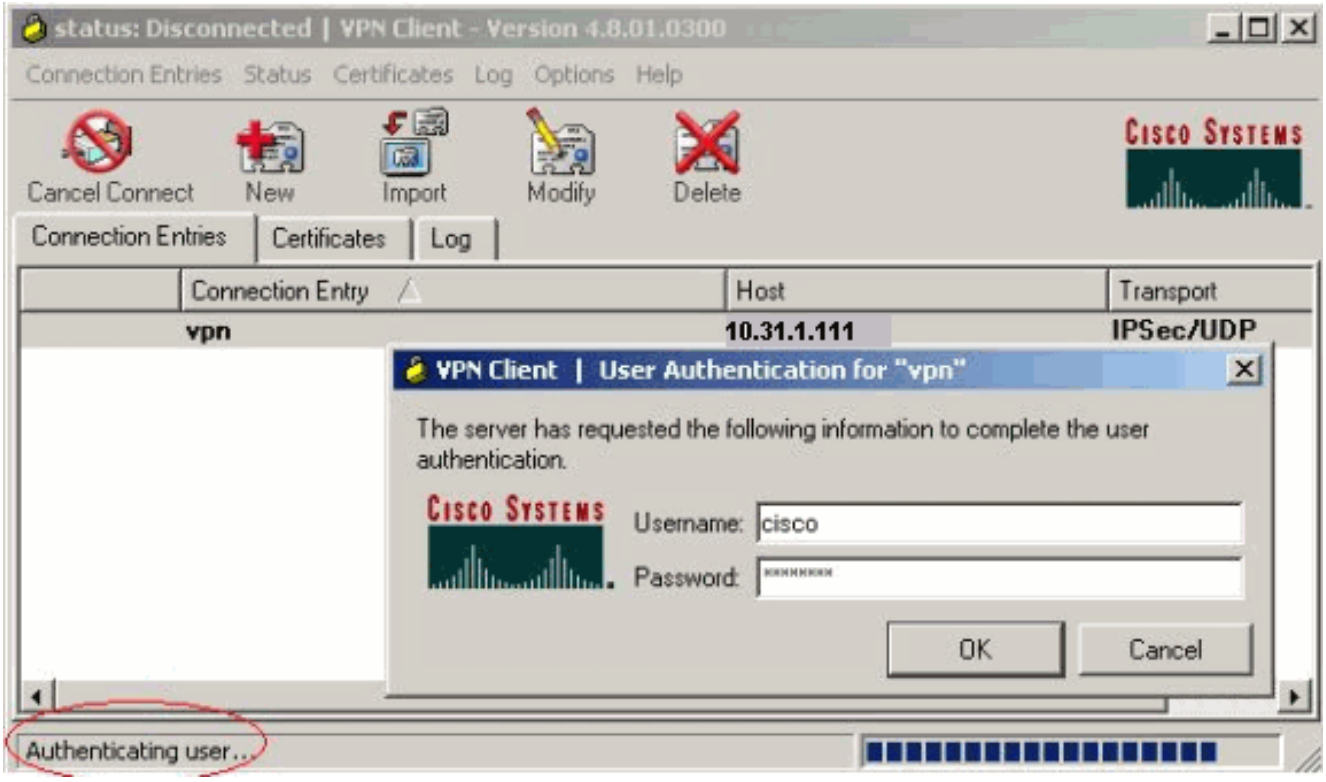


4. Cliquez sur la connexion que vous souhaitez utiliser et cliquez sur **Connect dans la fenêtre**

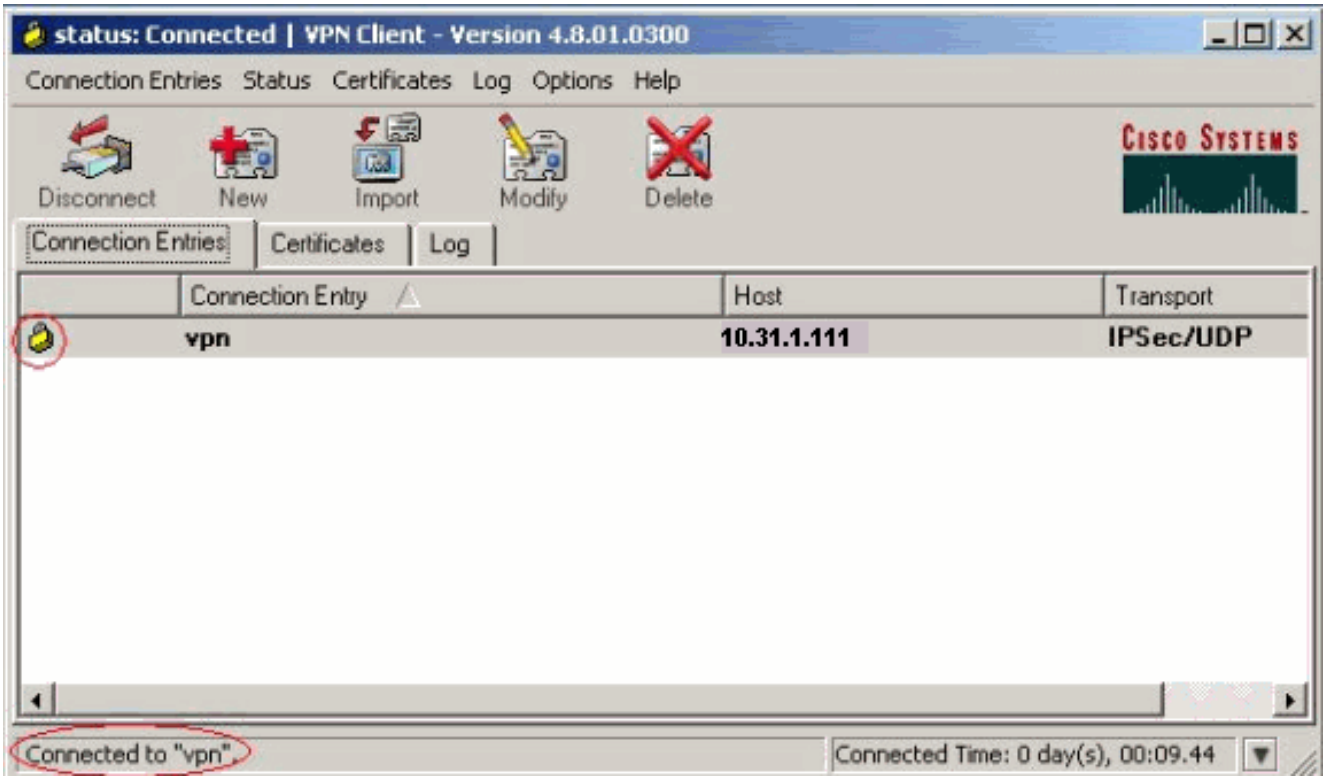
principale du Client
VPN.



5. Lorsque vous y êtes invité, saisissez le nom d'utilisateur et le mot de passe pour Xauth et cliquez sur **OK pour vous connecter au réseau distant.**



Le client VPN se connecte au routeur sur le site central.

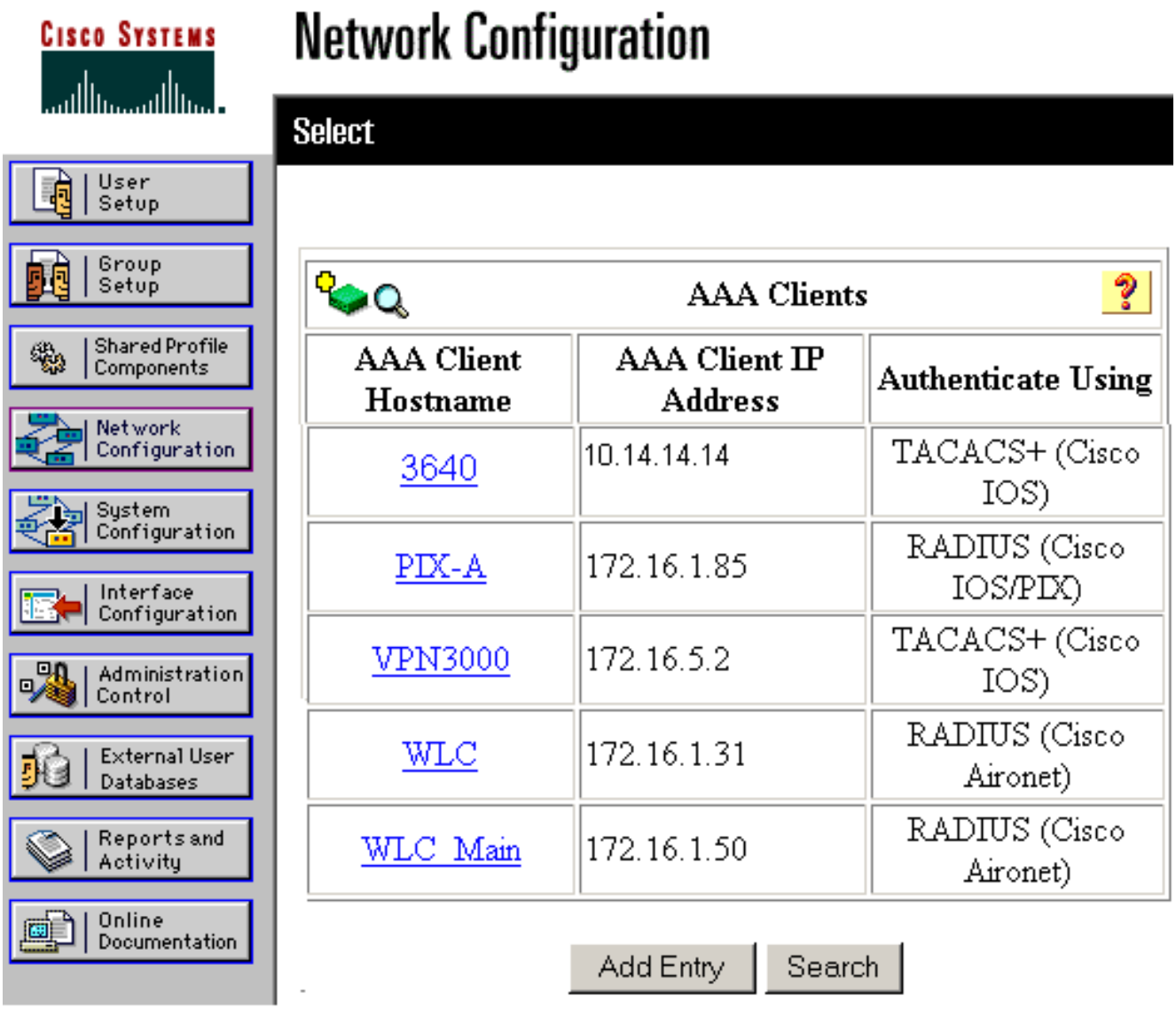


Configurer le serveur TACACS+ à l'aide de Cisco Secure ACS

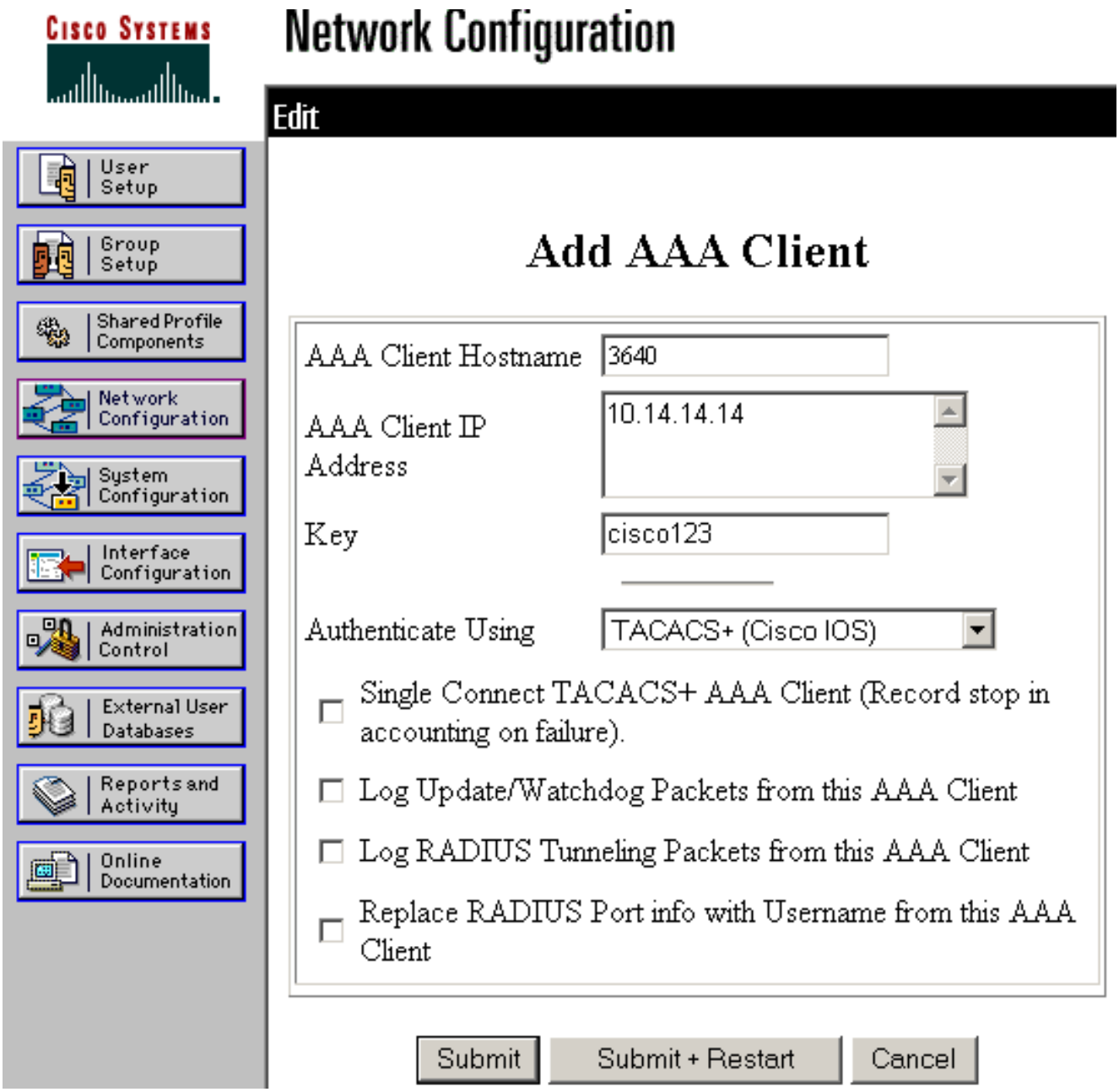
Complétez ces étapes afin de configurer TACACS+ dans un Cisco Secure ACS :

1. Vous devez configurer le routeur pour localiser Cisco Secure ACS afin de vérifier les informations d'identification de l'utilisateur.Exemple :
   ```
   3640(config)#
   aaa group server tacacs+ RTP
   3640(config)#
   tacacs-server host 10.14.14.3 key cisco
   ```

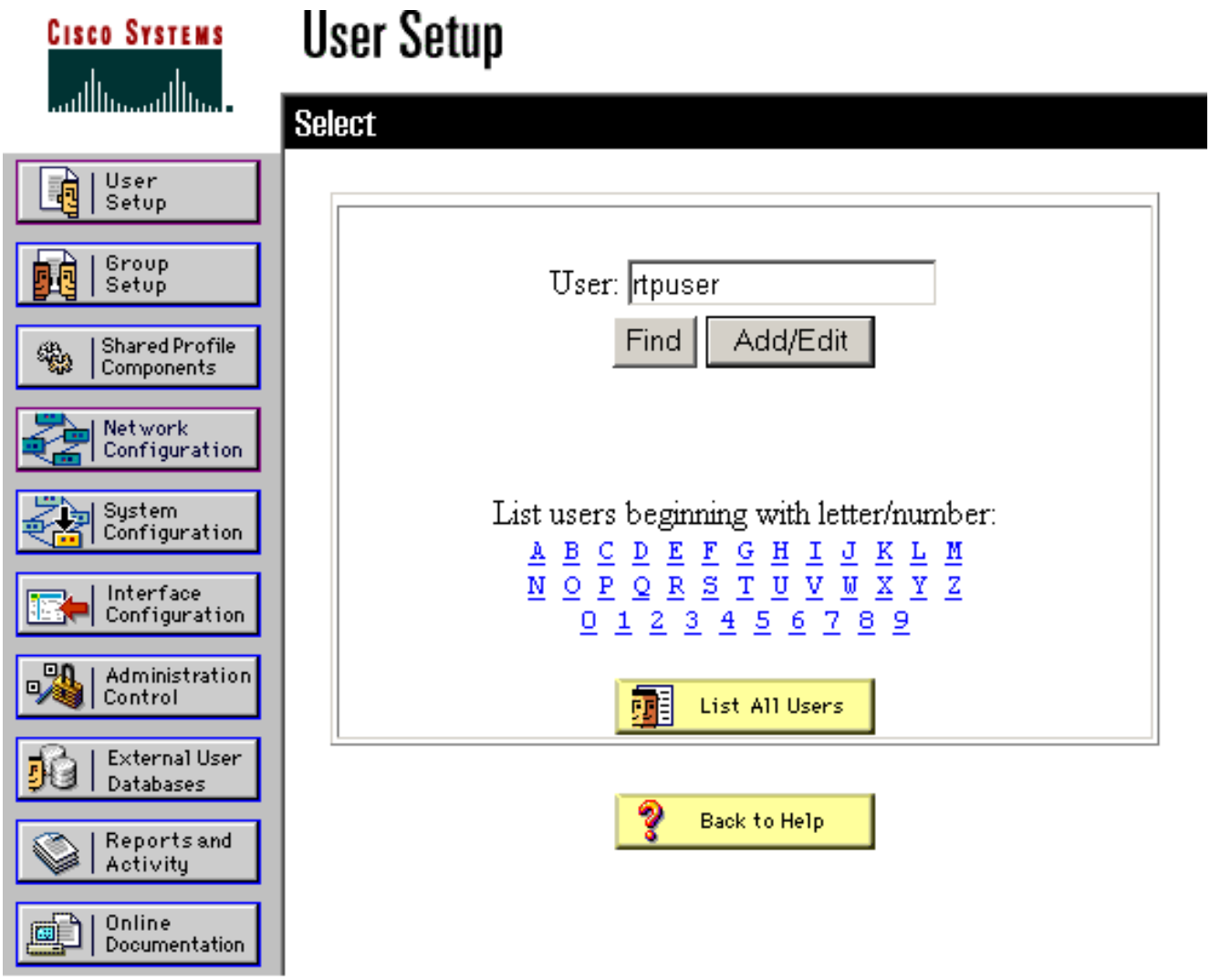
2. Choisissez **Network Configuration** à gauche et cliquez sur **Add Entry** pour ajouter une entrée pour le routeur dans la base de données du serveur TACACS+. Choisissez la base de données du serveur en fonction de la configuration du routeur.



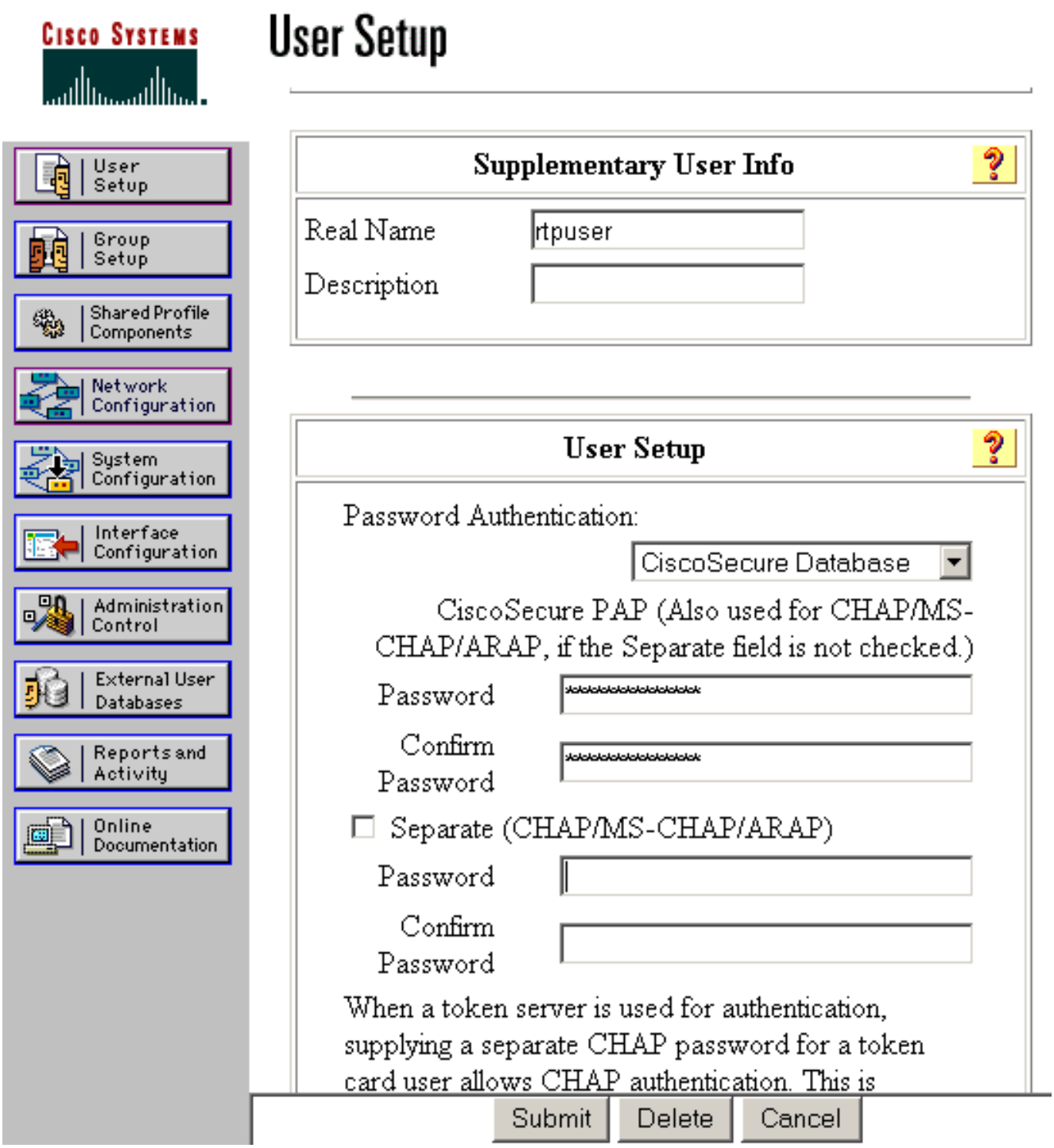
3. La clé est utilisée pour l'authentification entre le routeur 3640 et le serveur Cisco Secure ACS. Si vous souhaitez sélectionner le protocole TACACS+ pour l'authentification, sélectionnez **TACACS+ (Cisco IOS)** dans le menu déroulant Authentifier à l'aide.



4. Entrez le nom d'utilisateur dans le champ User de la base de données Cisco Secure, puis cliquez sur **Add/Edit**.Dans cet exemple, le nom d'utilisateur est rtpuser.



5. Dans la fenêtre suivante, saisissez le mot de passe de rtpuser.Dans cet exemple, le mot de passe est rtpuserpass. Vous pouvez mapper le compte utilisateur à un groupe si vous le souhaitez. Lorsque vous avez terminé, cliquez sur **Soumettre**.



Configuration de la fonction de secours

Lorsque le serveur RADIUS principal devient indisponible, le routeur bascule vers le serveur RADIUS de sauvegarde actif suivant. Le routeur continuera à utiliser le serveur RADIUS secondaire pour toujours, même si le serveur principal est disponible. Généralement, le serveur principal est hautes performances et le serveur préféré. Si le serveur secondaire n'est pas disponible, la base de données locale peut être utilisée pour l'authentification à l'aide de la commande aaa authentication login default group RTP local.

Vérification

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

Établissez un tunnel IPSec entre le PC et le routeur Cisco 3640.

Ouvrez un navigateur sur le PC et pointez-le sur **http://10.17.17.17**. Le routeur Cisco 3640 intercepte ce trafic HTTP, déclenche le proxy d'authentification et vous invite à saisir un nom d'utilisateur et un mot de passe. Le Cisco 3640 envoie le nom d'utilisateur/mot de passe au serveur TACACS+ pour authentification. Si l'authentification réussit, vous devriez voir les pages Web sur le serveur Web à l'adresse 10.17.17.17.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- show ip access-lists : affiche les listes de contrôle d'accès standard et étendues configurées sur le routeur de pare-feu (y compris les entrées de liste de contrôle d'accès dynamique). Les entrées de la liste de contrôle d'accès dynamique sont ajoutées et supprimées périodiquement selon que l'utilisateur s'authentifie ou non.Cette sortie montre la liste de contrôle d'accès 118 avant le déclenchement du proxy auth :

```
3640#show ip access-lists 118
   Extended IP access list 118
   10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (321 matches)
   20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (276 matches)
   30 permit tcp host 10.14.14.3 host 10.31.1.111 (174 matches)
```

  Cette sortie montre access-list 118 après le déclenchement du proxy d'authentification et l'authentification réussie de l'utilisateur :

```
3640#show ip access-lists 118
   Extended IP access list 118
   permit tcp host 10.20.20.26 any (7 matches)
   permit udp host 10.20.20.26 any (14 matches)
   permit icmp host 10.20.20.26 any
   10 permit esp 10.1.1.0 0.0.0.255 host 10.31.1.111 (379 matches)
   20 permit udp 10.1.1.0 0.0.0.255 host 10.31.1.111 eq isakmp (316 matches)
   30 permit tcp host 10.14.14.3 host 10.31.1.111 (234 matches)
```

  Les trois premières lignes de la liste d'accès sont les entrées définies pour cet utilisateur et téléchargées à partir du serveur TACACS+.
- show ip auth-proxy cache : affiche les entrées du proxy d'authentification ou la configuration du proxy d'authentification en cours. Mot clé cache permettant de répertorier l'adresse IP de l'hôte, le numéro de port source, la valeur de délai d'attente du proxy d'authentification et l'état des connexions qui utilisent le proxy d'authentification. Si l'état du proxy d'authentification est ESTAB, l'authentification de l'utilisateur est une réussite.

```
3640#show ip auth-proxy cache
   Authentication Proxy Cache
   Client IP 10.20.20.26 Port 1705, timeout 5, state ESTAB
```

Dépannage

Pour les commandes de vérification et de débogage, ainsi que d'autres informations de dépannage, référez-vous à Dépannage du proxy d'authentification.

Remarque : avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

Informations connexes

- Configuration du proxy d'authentification
- Configurations du proxy d'authentification dans Cisco IOS
- Implémentation du proxy d'authentification dans les serveurs TACACS+ et RADIUS
- Cisco VPN Client Support Page
- Page de support pour le pare-feu d'IOS
- Page d'assistance IPsec
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Page de support TACACS/TACACS+
- TACACS+ dans la documentation d'IOS
- Support technique - Cisco Systems