IOS ルータ： IPsec および VPN クライアントの ACS に関する Auth-proxy 認証着信

目次

はじめに
前提条件
要件
使用するコンポーネント
表記法
設定
ネットワーク図
設定
VPN Client 4.8 の設定
Cisco Secure ACS を使用して TACACS+ サーバを設定して下さい
フォールバック 機能を設定して下さい
確認
トラブルシューティング
関連情報

概要

ネットワークへのログインへの認証プロキシ 機能割り当てユーザは自動的に TACACS+ か RADIUSサーバから取得され、適用されて特定のアクセス プロファイルが HTTP によってまたはインターネットに、アクセスします。 そのユーザ プロファイルは、認証済みユーザからのアクティブなトラフィックが存在する間だけ有効です。

この設定は始動に 10.1.1.1 の Webブラウザ設計され、10.17.17.17 にそれを向けます。 VPN Client が 10.17.17.x ネットワークに到達することをトンネル エンド ポイント 10.31.1.111 を通過するために設定されるので IPSec トンネルは構築され、（モード設定が実行されたので）PC はプール RTP-POOL から IP アドレスを抜き出します。 認証は Cisco 3640 ルータによってそれから要求されます。 ユーザがユーザ名 および パスワードを（10.14.14.3 で TACACS+ サーバで保存される）入力した後、サーバから渡されるアクセス リストはアクセス リスト 118 に追加されます。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- Cisco VPN Client は Cisco 3640 ルータとの IPSec トンネルを確立するために設定されます。
- TACACS+ サーバは認証プロキシのために設定されます。 詳細については「関連情報」セク

ションを参照して下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS? ソフトウェア リリース 12.4
- Cisco 3640 ルータ
- Windows バージョン 4.8 のための Cisco VPN Client（どの VPN Client でも 4.x および以降ははたらく必要があります）

注: ip auth-proxy コマンドは Cisco IOS ソフトウェア リリース 12.0.5.T.でもたらされました この設定は Cisco IOS ソフトウェア リリース 12.4 とテストされました。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

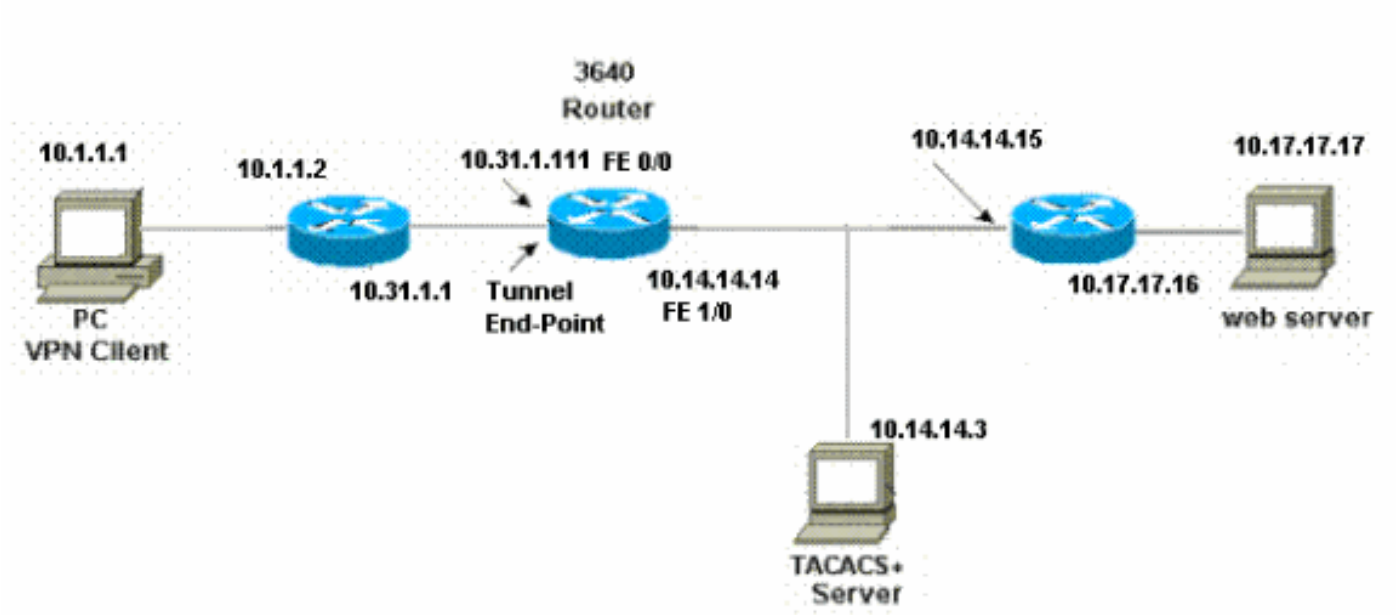
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



設定

3640 ルータ

```
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
!
```

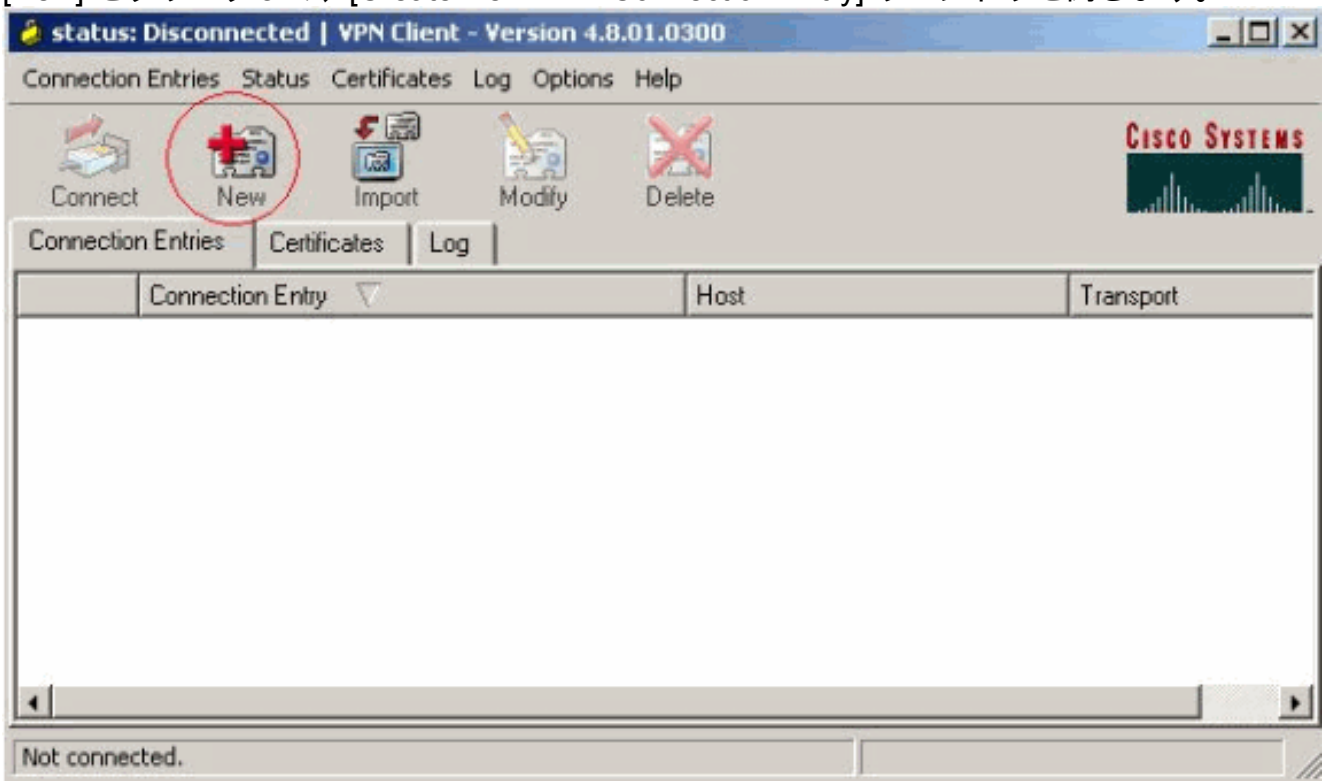
```
!--- Define IPSec transform set and apply it to the
dynamic crypto map. crypto ipsec transform-set RTP-
TRANSFORM esp-des esp-md5-hmac
!
crypto dynamic-map RTP-DYNAMIC 10
 set transform-set RTP-TRANSFORM
!
!--- Define extended authentication (X-Auth) using the
local database. !--- This is to authenticate 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
```

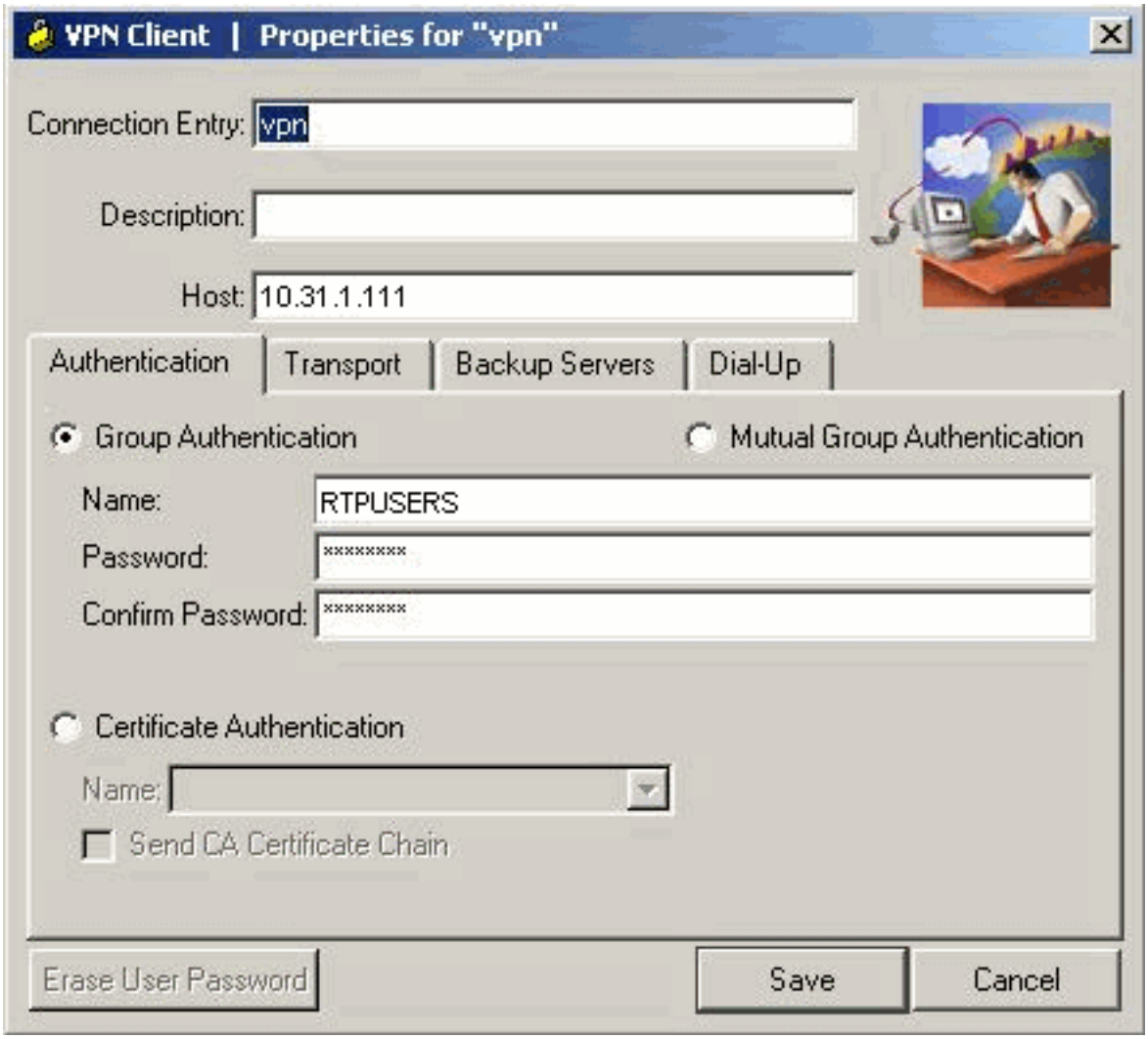
VPN Client 4.8 の設定

VPN Client 4.8 を設定するためにこれらのステップを完了して下さい:

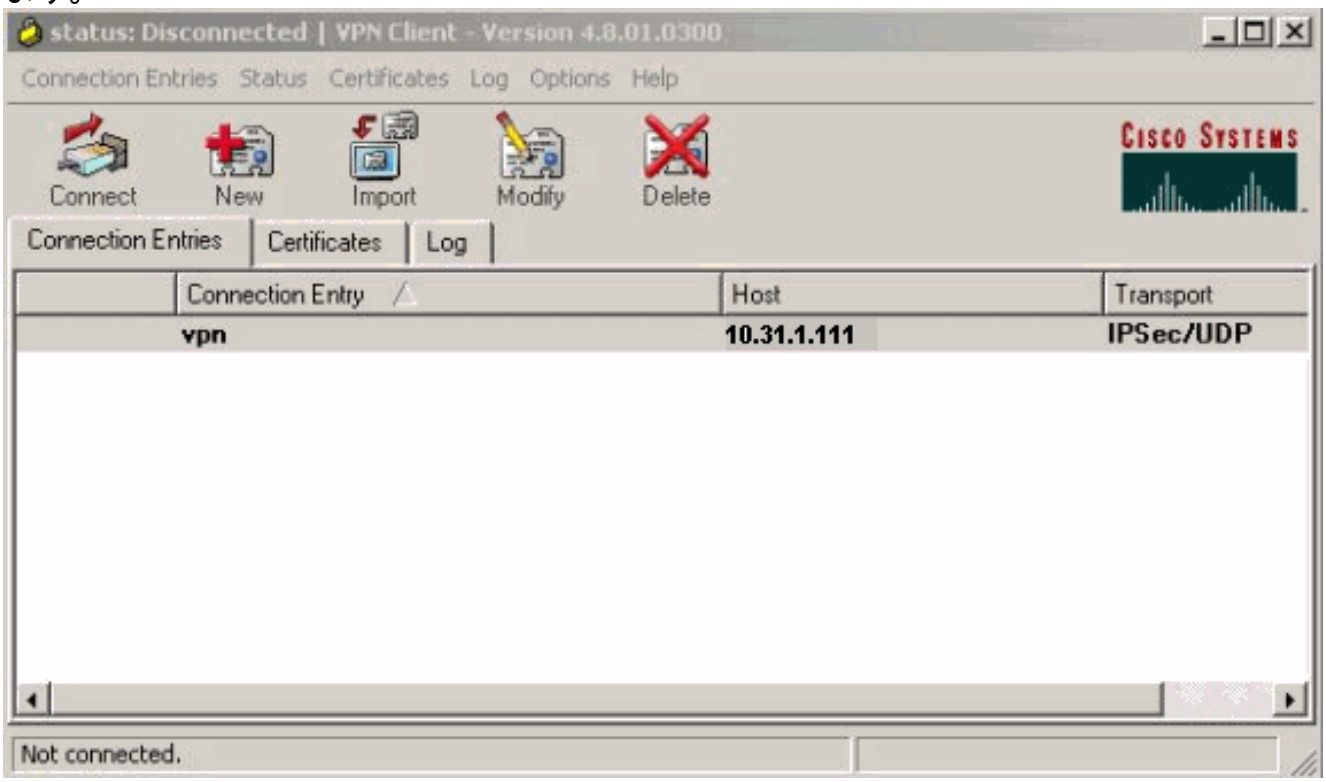
1. [Start] > [Programs] > [Cisco Systems VPN Client] > [VPN Client] の順に選択します。
2. [New] をクリックして、[Create New VPN Connection Entry] ウィンドウを開きます。



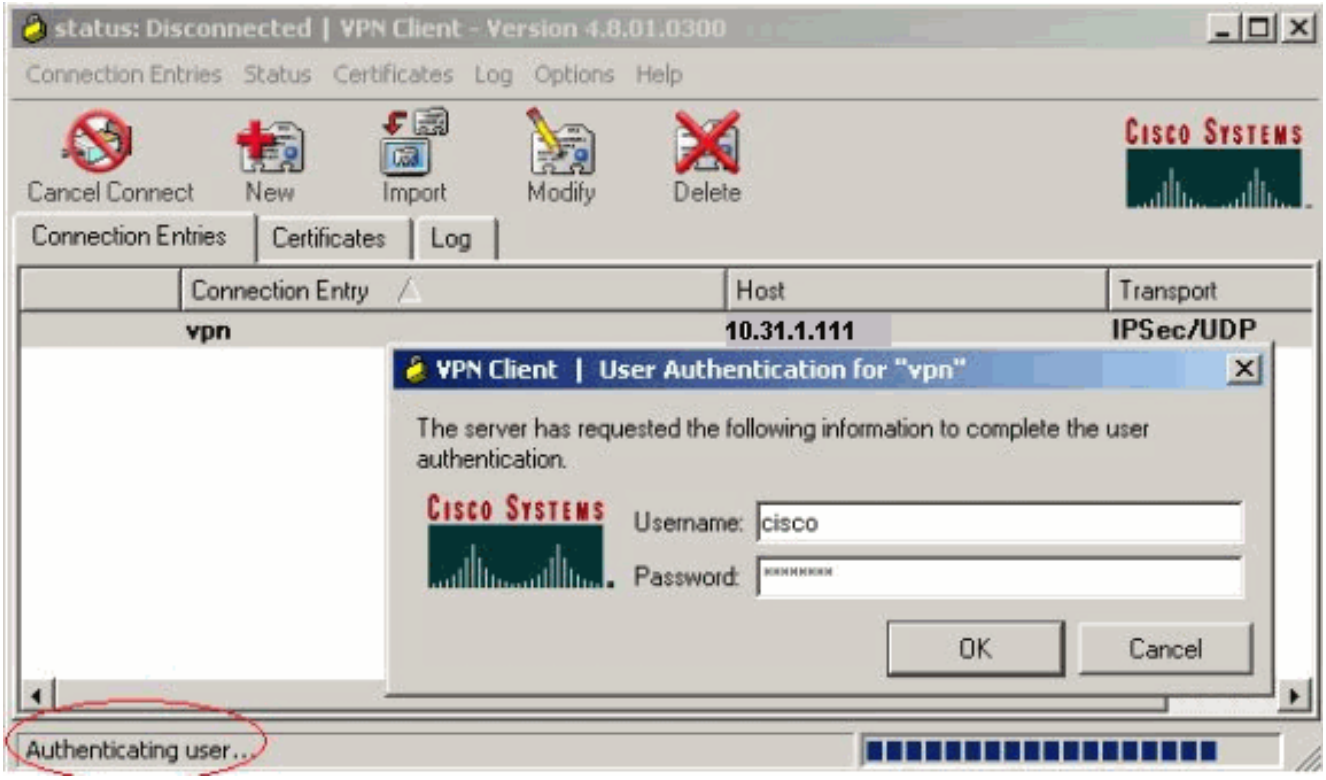
3. 接続エントリの名前と説明を入力します。 ホスト ボックスでルータの外部 IP アドレスを入力して下さい。 それから VPNグループ名およびパスワードを入力し、『SAVE』 をクリック して下さい。



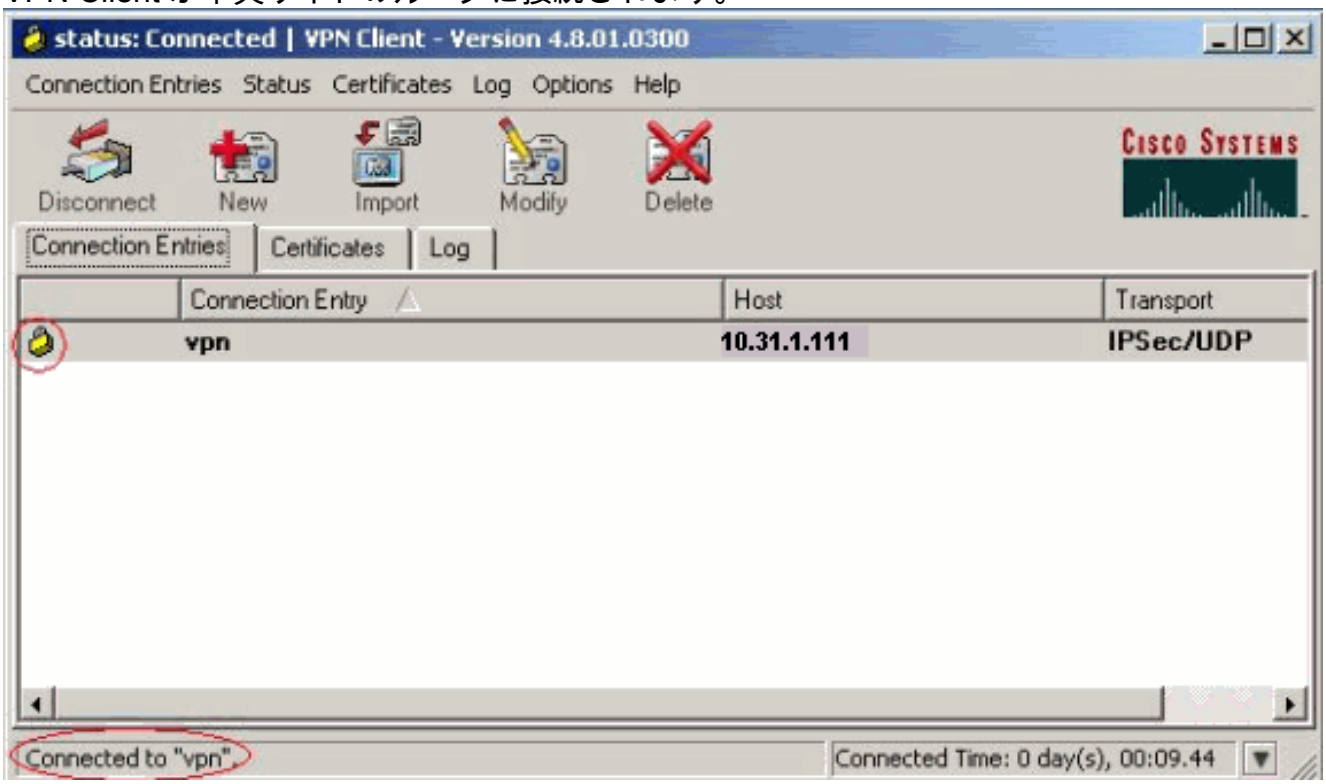
4. 使用する接続をクリックし、VPN Client のメイン ウィンドウから [Connect] をクリックします。



5. プロンプト表示された場合、Xauth のためのユーザ名 および パスワード 情報を入力し、リモートネットワークに接続するために『OK』 をクリック して下さい。



VPN Client が中央サイトのルータに接続されます。



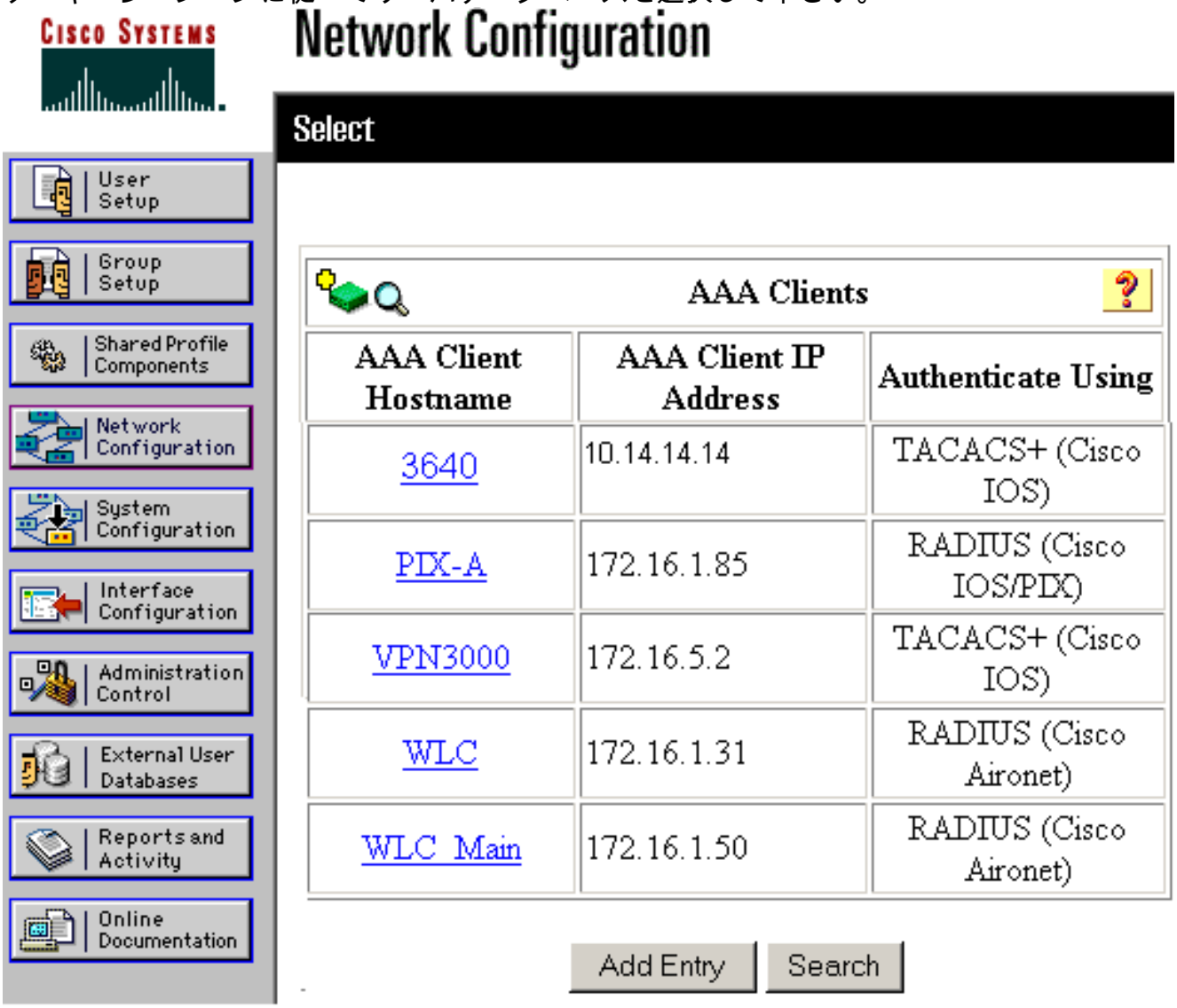
Cisco Secure ACS を使用して TACACS+ サーバを設定して下さい

Cisco Secure ACS の TACACS+ を設定するためにこれらのステップを完了して下さい:

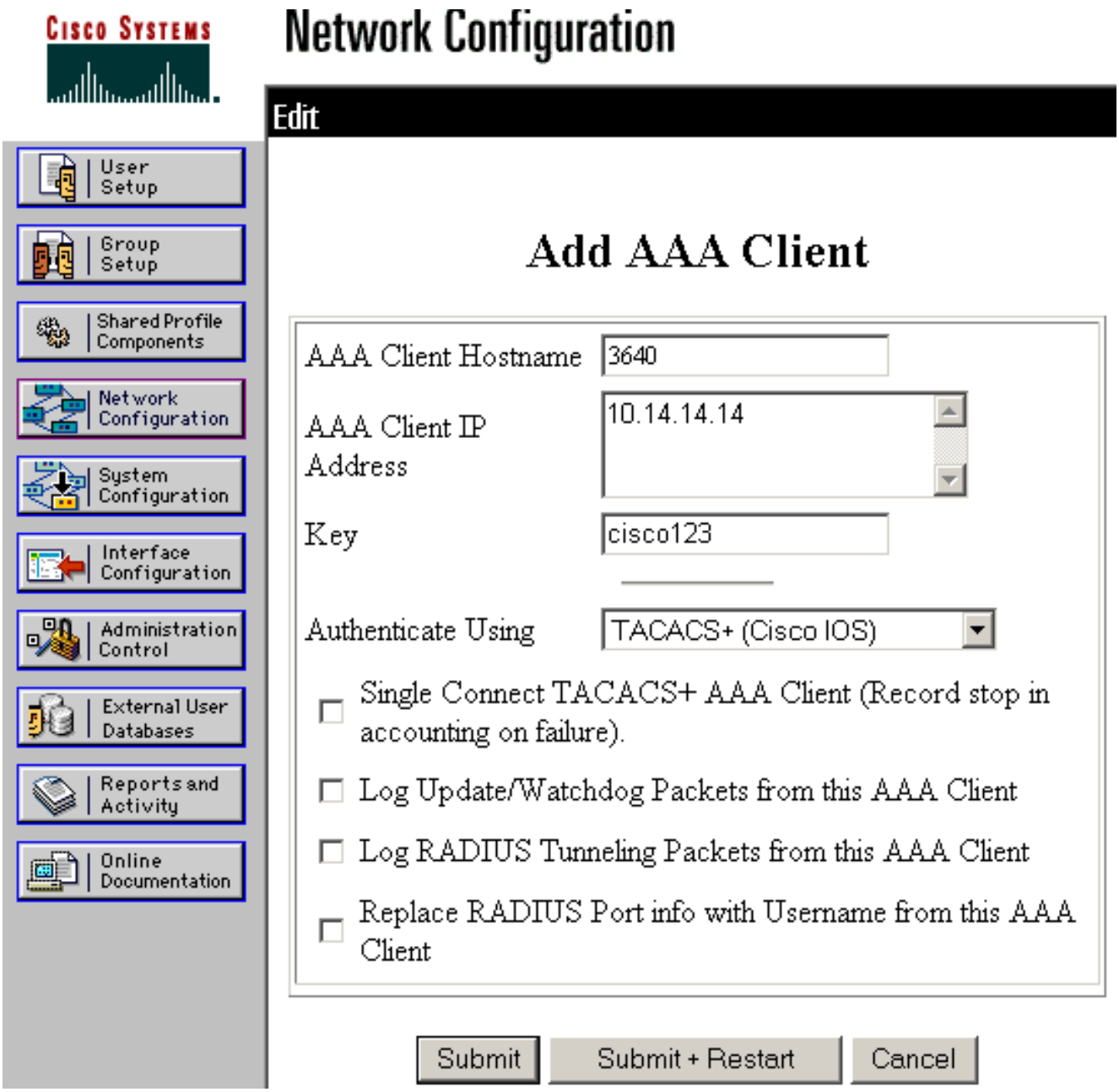
1. ユーザーの資格情報をチェックするために Cisco Secure ACS を見つけるようにルータを設定して下さい。次に、例を示します。

```
3640(config)#
aaa group server tacacs+ RTP
3640(config)#
tacacs-server host 10.14.14.3 key cisco
```

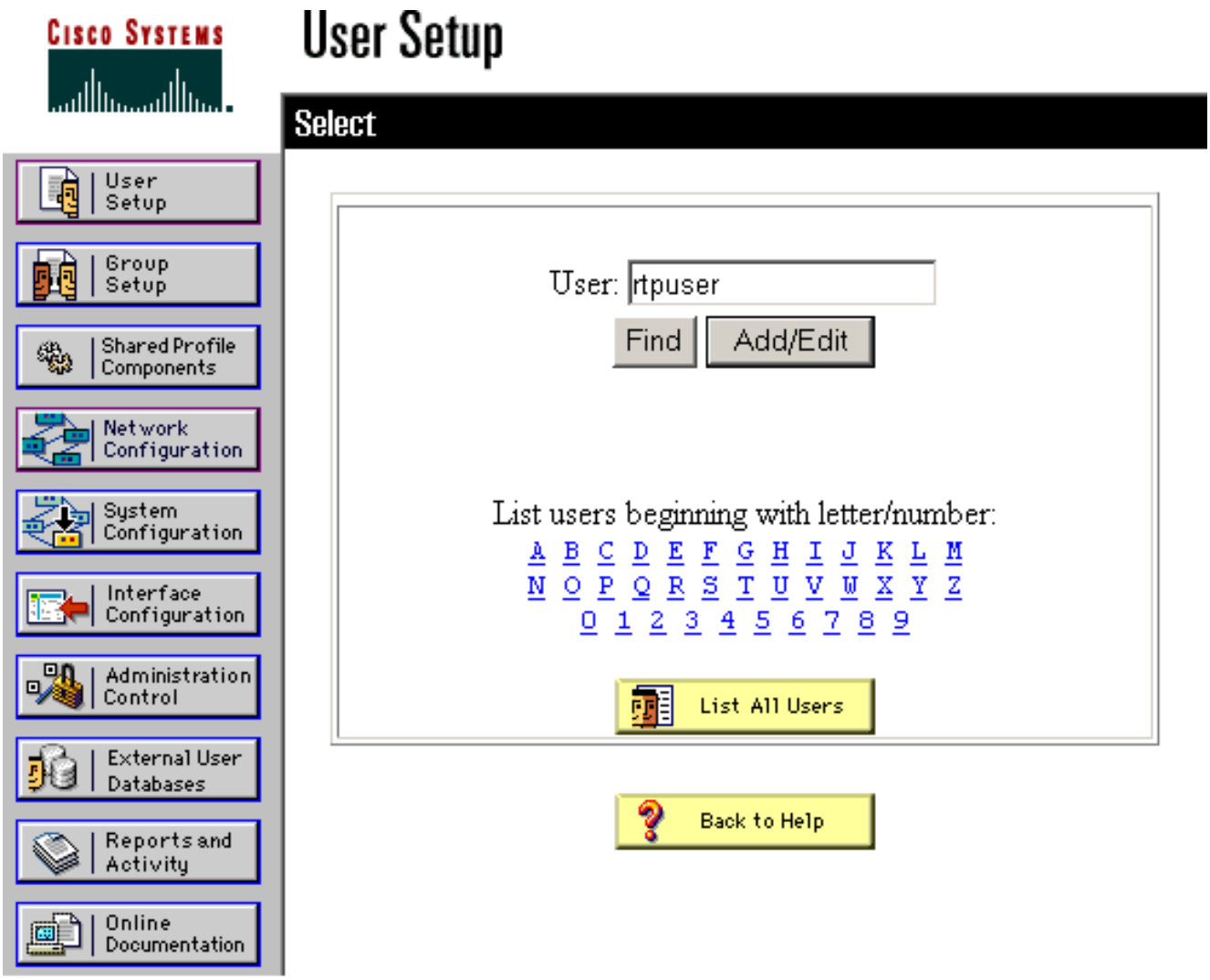
2. 左で『Network Configuration』 を選択 し、どちらかのルータのためのエントリを追加するために TACACS+ サーバデータベース 『Add Entry』 をクリック して下さい。 ルータコンフィギュレーションに従ってサーバデータベースを選択して下さい。



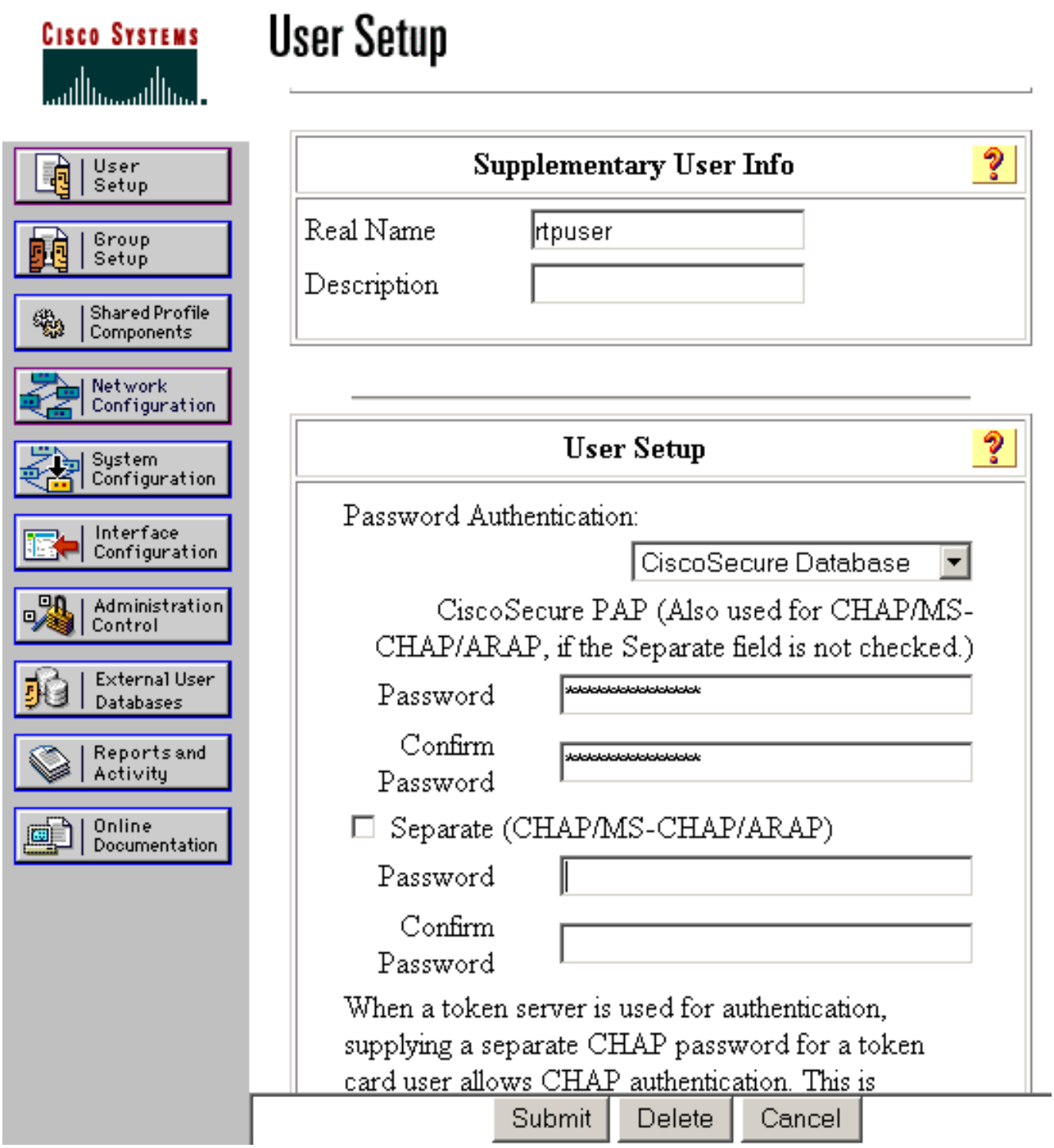
3. キーが 3640 ルータと Cisco Secure ACS サーバの間で認証するのに使用されています。 認証に TACACS+ プロトコルを選択したいと思う場合廃棄メニューを使用して認証するで『TACACS+ （ Cisco IOS ）』 を選択 して下さい。



4. ユーザ名を Cisco Secure データベースの User フィールドで入力し、そして『Add/Edit』 をクリック して下さい。この例では、ユーザー名は rtpuser です。



5. Next ウィンドウでは、rtpuser のためのパスワードを入力して下さい。この例では、パスワードは rtpuserpass です。 希望する場合グループにユーザアカウントをマップできます。終わったら、『SUBMIT』 をクリック して下さい。



フォールバック 機能を設定して下さい

プライマリ RADIUSサーバが利用できなくなるとき、ルータは次のアクティブ バックアップ RADIUSサーバにフェールオーバー。 ルータはプライマリ サーバーが利用できてセカンダリ RADIUSサーバを永久に使用し続けます。 通常、プライマリ サーバはパフォーマンスが高く、優先サーバとなっています。 セカンダリサーバが利用できない場合ローカル データベースは[ローカル RTP が](#)命じる [AAA認証ログイン デフォルト グループ](#)を使用して認証に使用することができます。

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を提供しています。

PC と Cisco 3640 ルータ間の IPSec トンネルを確立して下さい。

PC のブラウザを開き、**http://10.17.17.17** を指して下さい。 Cisco 3640 ルータはこの HTTP トラフィックを、トリガー 認証プロキシ代行受信し、ユーザ名 および パスワードのためにプロンプト表示します。 Cisco 3640 は認証のための TACACS+ サーバに username/password を送信 します。 認証が正常である場合、10.17.17.17 で Webサーバの Webページを見られますはずです。

特定の **show** コマンドは、Output Interpreter Tool (登録ユーザ専用) によってサポートされています。このツールを使用すると、**show** コマンド出力の分析を表示できます。

- **show ip access-lists —** ファイアウォール ルータで設定される標準および拡張 ACL を表示します (ダイナミック ACL エントリが含まれています) 。 ダイナミック ACL エントリは、ユーザが認証されるかどうかに応じて、定期的に追加および削除されます。この出力は auth-proxy が誘発された前に acess リスト 118 を示したものです:

```
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)
```

  この出力は auth-proxy が誘発され、ユーザが認証に成功する後 access-list 118 を示したものです:

```
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)
```

  access-list の最初の 3 つの行はこのユーザ向けに定義され、TACACS+ サーバからダウンロードされるエントリです。
- **ip auth-proxy が cache —** 認証プロキシ エントリか認証プロキシ設定を表示することを示して下さい。 認証プロキシのホスト IP アドレス、送信元ポート番号、タイムアウト値、および認証プロキシを使用する接続のための状態をリストする Cache キーワード。 認証プロキシ状態が確立することである場合ユーザ認証は成功です。

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

トラブルシューティング

verification および debugging コマンドに関しては、他のトラブルシューティング情報と共に、トラブルシューティング 認証プロキシを参照して下さい。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

関連情報

- **認証の構成プロキシ**
- **Cisco IOS の認証プロキシ設定**
- **TACACS+ および RADIUSサーバの認証プロキシの実装**
- **Cisco VPN Client に関するサポート ページ**

- IOS ファイアウォールのサポート ページ
- IPSec に関するサポート ページ
- RADIUS に関するサポート ページ
- Requests for Comments (RFC)
- TACACS/TACACS+ に関するサポートページ
- IOS での TACACS+ に関するドキュメント
- テクニカルサポート - Cisco Systems