ロック アンド キー： ダイナミック アクセス リスト

目次

概要

ロック アンド キー アクセスを使用すると、ユーザ認証プロセスを使用して特定の発信元/送信先ホストへのアクセスをユーザ単位で許可する、ダイナミック アクセス リストを設定できます。ユーザアクセスはセキュリティ制限の侵害なしで Cisco IOS ® ファイアウォールによって、動的に許可されます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、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。 この場合、ラボ 環境は Cisco IOS® ソフトウェア リリース 12.3(1)を実行する 2620 ルータで構成されていました。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十

分に理解しておく必要があります。

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。

スプーフィングについて

ロック および キー アクセスは外部イベントが Cisco IOS ファイアウォールに開始を置くようにします。 この穴が開いてしまうと、ルータは発信元アドレスのスプーフィングを受ける可能性があります。 これを防ぐために、認証か暗号化を IP 暗号化を使用して暗号化サポートに与えて下さい。

スプーフィングの問題はすべての既存のアクセス リストに存在します。 ロック アンド キー アクセスではこの問題に対処できません。

ロック アンド キー アクセスでは、ネットワーク ファイアウォールに潜在的な通路が作成されるため、ダイナミック アクセスを検討する必要があります。 認証 された アドレスをスプーフィングする別のホストはファイアウォールの後ろでアクセス権を得ます。 ダイナミックアクセスによって、認証 された アドレスをスプーフィングする不正 ホストがファイアウォールの後ろでアクセス権を得るという可能性があります。 ロック アンド キー アクセスでは、アドレス スプーフィングの問題は発生しません。 この文書では、この問題はユーザが懸念すべき問題として認識されるにとどまります。

パフォーマンス

パフォーマンスはこれら二つの状況で影響を及ぼされます。

- それぞれのダイナミック アクセス リストによって、Silicon Switching Engine (SSE; シリコン スイッチング エンジン) では強制的にアクセス リストが再作成されます。 これが原因で、SSE スイッチング パスの速度が一瞬低下します。
- ダイナミック アクセス リストは (タイムアウトがディフォルトするために残っていても) アイドルタイムアウト ファシリティを必要とします。 従って、ダイナミック アクセス リストは切り替えられる SSE である場合もありません。 これらのエントリはプロトコル ファスト スイッチング パスで処理されます。

ボーダールータ コンフィギュレーションを視聴して下さい。 リモート ユーザは、境界ルータにアクセス リストのエントリを作成します。 アクセス リストは動的に育ち、縮まります。 idle-timeout または max-timeout の期間が経過すると、エントリがリストから動的に削除されます。 アクセス リストが大きくなると、パケット交換のパフォーマンスが低下します。

ロック アンド キー アクセスを使用する状況

ロック および キー アクセスを使用するとき 2 つの例はのここにリストされています:

- リモートホストにインターネットを通してインターネットワークのホストにアクセスできてほしい時。 ロック および キー アクセスは個々のホストまたはネット基礎のファイアウォールを越えるアクセスを制限します。
- ネットワーク上の一部のホストが、ファイアウォールで保護されたリモート ネットワーク上

のホストにアクセスできるようにする場合。 ロック アンド キー アクセスを使用すると、TACACS+ または RADIUS サーバによる認証を行うことで、希望するホスト群のみにアクセスを許可できます。

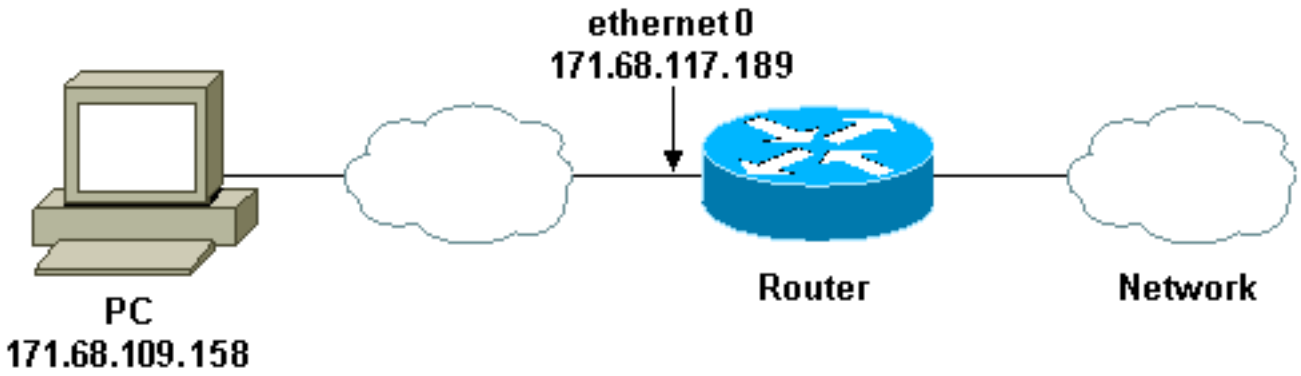
ロック アンド キー アクセスの動作

このプロセスはロック および キーアクセス オペレーションを記述します。

1. ユーザが、ロック アンド キー アクセス用に設定された境界ルータへの Telnet セッションを開きます。
2. Cisco IOSソフトウェアは Telnet パケットを受信します。 それはユーザ認証プロセスを行います。 ユーザは認証をパスしない限り、アクセスを許可されません。 認証プロセスは TACACS+ または RADIUSサーバのようなルータかセントラルアクセスサーバによって実行されます。

設定例とトラブルシューティング

ネットワーク図



Cisco は認証クエリ プロセスのために TACACS+ サーバを使用することを推奨します。 TACACS+ では、認証、許可、および会計サービスが提供されます。 また、プロトコル サポート、プロトコル仕様、および中央集中型セキュリティ データベースも提供されます。

ユーザの認証は、ルータで行うことも、TACACS+ または RADIUS サーバを使用することもできます。

注: これらのコマンドは特に明記しない限りグローバルです。

ルータで、ローカル認証のユーザ向けの**ユーザ名を**必要とします。

```
username test password test
```

VTY 行の **login local** の存在はこのユーザ名を使用します。

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

access-enable コマンドを発行するためにユーザを信頼しない場合 2 つの事柄の 1 つをすることができます:

- ユーザー単位のユーザとタイムアウトを関連付けて下さい。
  username test autocommand access-enable host timeout 10 または
- 同じタイムアウトがあるために Telnet で接続するすべてのユーザを強制して下さい。
  line vty 0 4 login local autocommand access-enable host timeout 10

注: 構文の **10 は**アクセス リストの*アイドルタイムアウト*です。 それはダイナミック アクセス リストの絶対タイムアウトによって無効になります。

ユーザ（あらゆるユーザ）がルータおよび **access-enable コマンドに**発行される**ログイン** するとき適用する拡張アクセスリストを定義して下さい。 フィルタのこの「ホール」の最大絶対時間は 15 分に設定 されます。 15 分後に、ホールはだれでもそれを使用するかどうか閉じます。 testlist という名前は存在している必要がありますが、重要ではありません。 ユーザは送信元または宛先アドレスの設定によってアクセスできるネットワークを制限して下さい（ここに、ユーザは限られていません）。

access-list 120 dynamic testlist timeout 15 permit ip any any
すべてをブロックするのに必要とされるアクセス リストを以外ルータに Telnet で接続する機能定義して下さい（ホールを開くため、ルータに Telnet で接続することをユーザーのニーズ）。 ここの IP アドレスはルータのイーサネット IPアドレスです。

access-list 120 permit tcp any host 171.68.117.189 eq telnet
端に暗黙の deny が**すべて**あります（ここに入らない）。

ユーザが入って来インターフェイスにこのアクセス リストを追加して下さい。

interface ethernet1 ip access-group 120 in
終了します。

これはフィルタがルータでのように見える今はものにです:

```
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)
```

内部ネットワークにアクセスを得るユーザはルータに Telnet で接続するまで何でも見られません。

注: 10 はここにアクセス リストの*アイドルタイムアウト*です。 それはダイナミック アクセス リストの絶対タイムアウトによって無効になります。

```
%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.
```

このようにフィルタな。

```
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)
```

ソース IP アドレスに基づいてこの 1 人のユーザ向けのフィルタにホールがあります。 誰か他の人がこれをするとき、*2 人のホール*に会います。

```
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)
```

これらのユーザは*ソース IP アドレス*からのあらゆる宛先 IP アドレスに完全な IPアクセスを持てます。

TACACS+ の使用

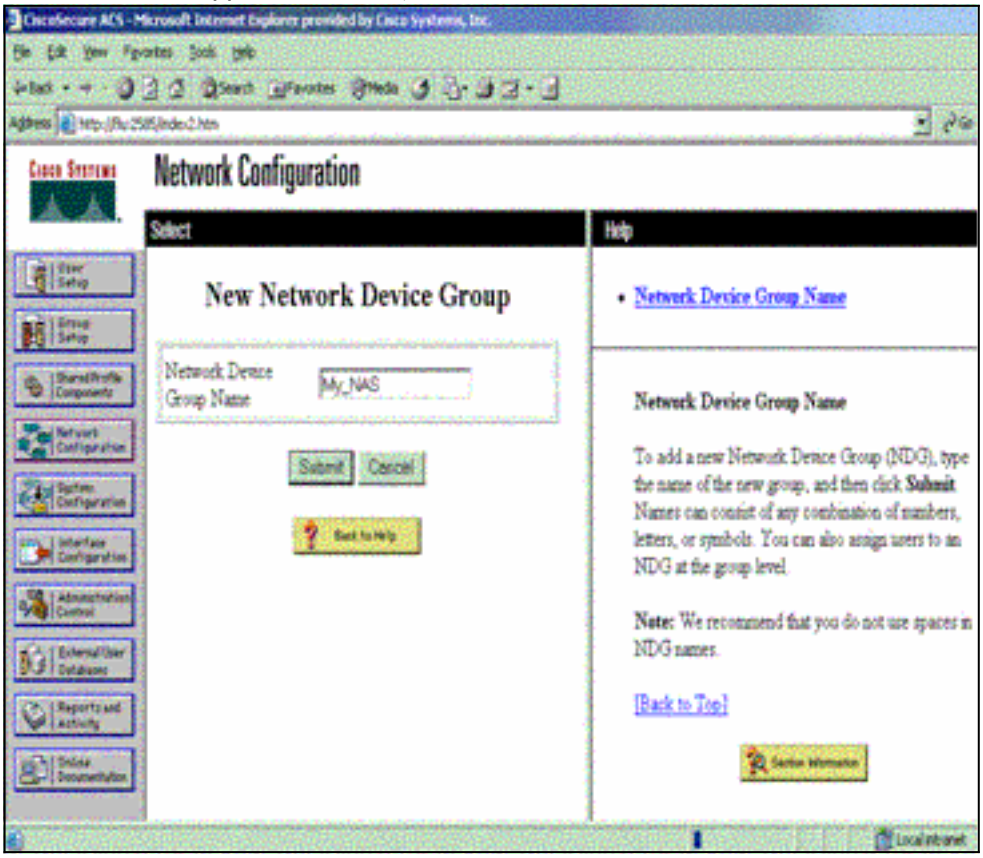
設定 TACACS+

この出力が示すように認証 および 権限を TACACS+ サーバで TACACS+ を使用するためにされるように強制するように TACACS+ サーバを設定して下さい:

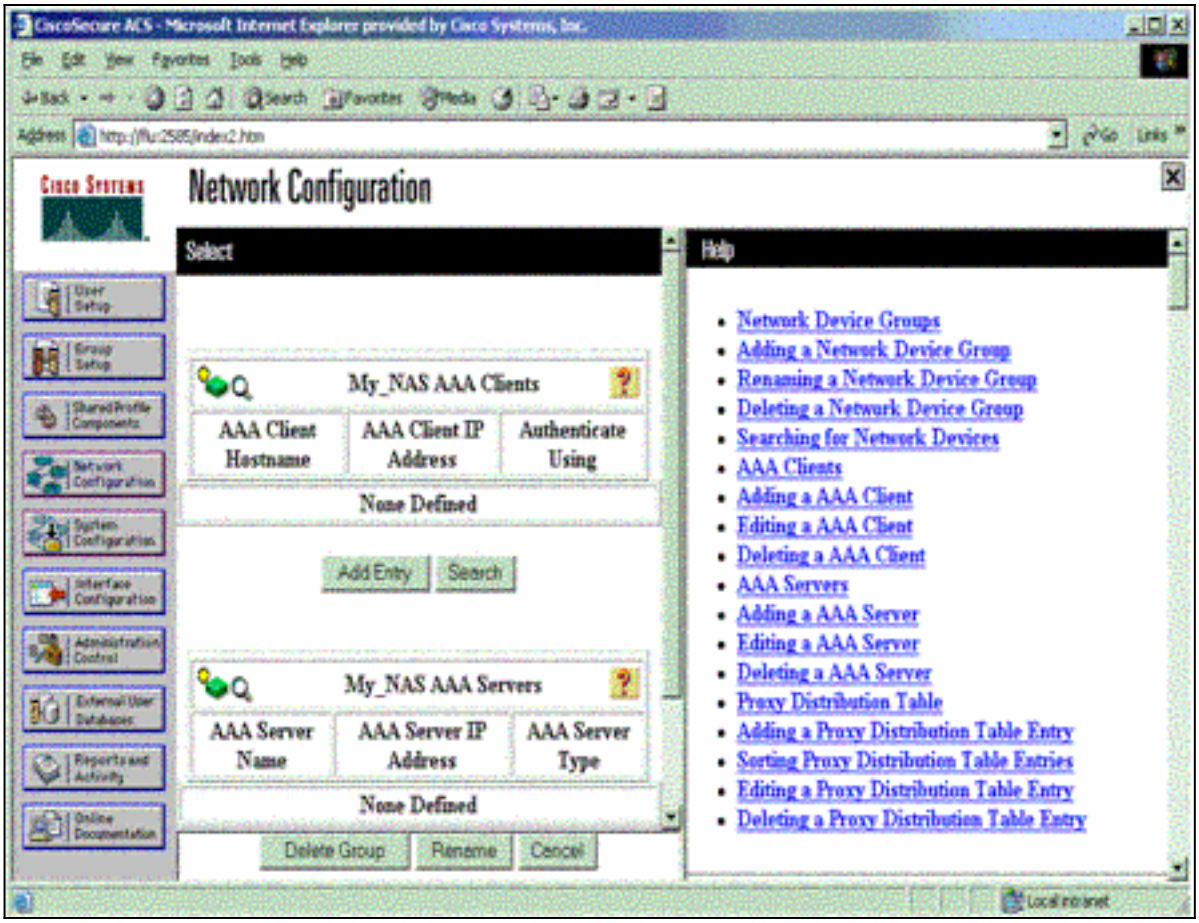
```
aaa new-model
!
!
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+
tacacs-server host 10.48.66.53 key cisco123
```

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

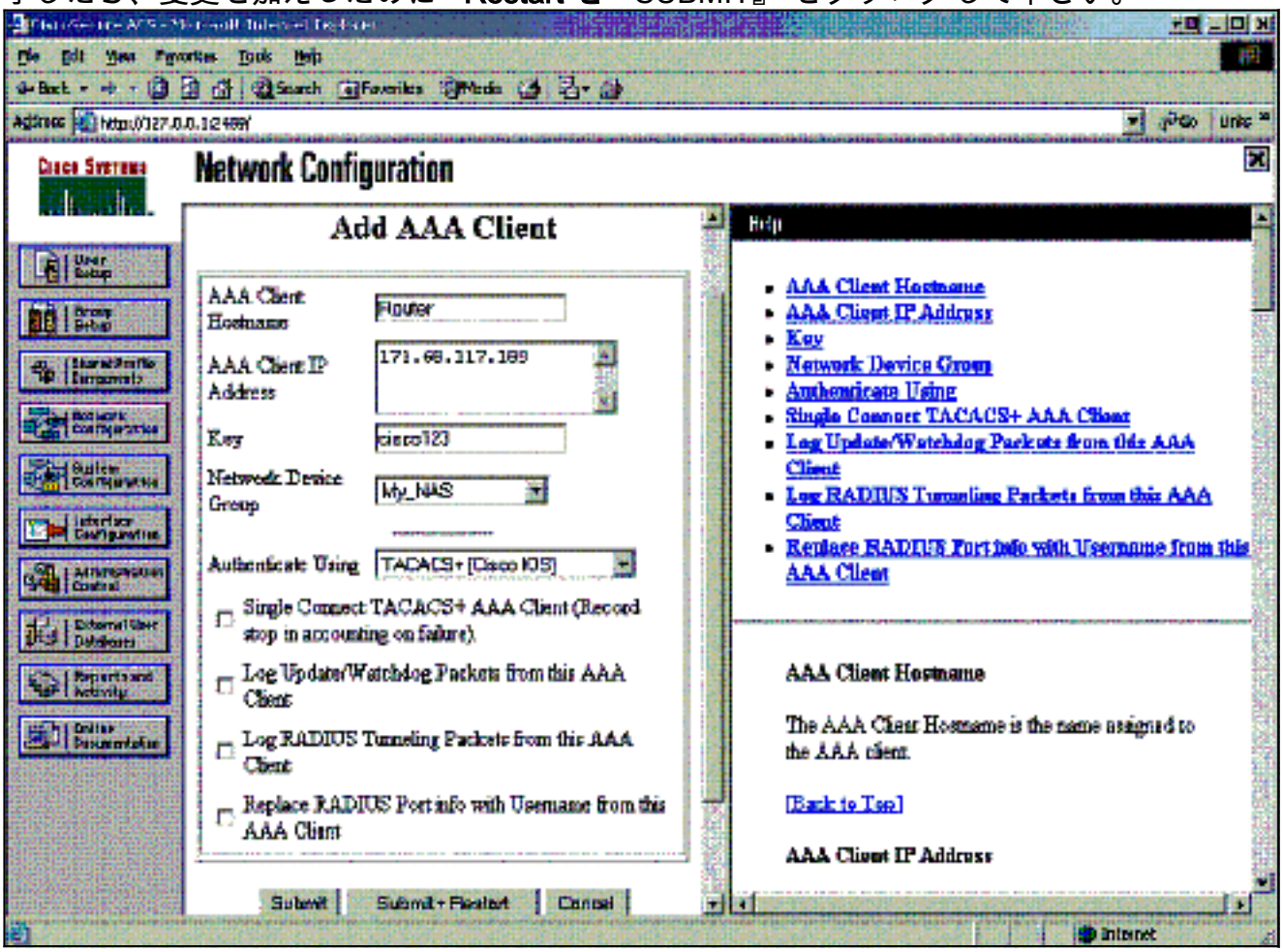
1. Web ブラウザを開きます。 ACS サーバのアドレスを入力して下さい、**http:// *<IP_address か DNS_name>:2002*** の形にある。 （ この例は 2002 年のデフォルトポートを使用します。 ）admin として口グイン。
2. [Network Configuration] をクリックします。 network access servers （ NAS ）が含まれているネットワーク デバイス グループを作成するために『Add Entry』 をクリック して下さい。 グループの名前を入力し、『SUBMIT』 をクリック して下さい。



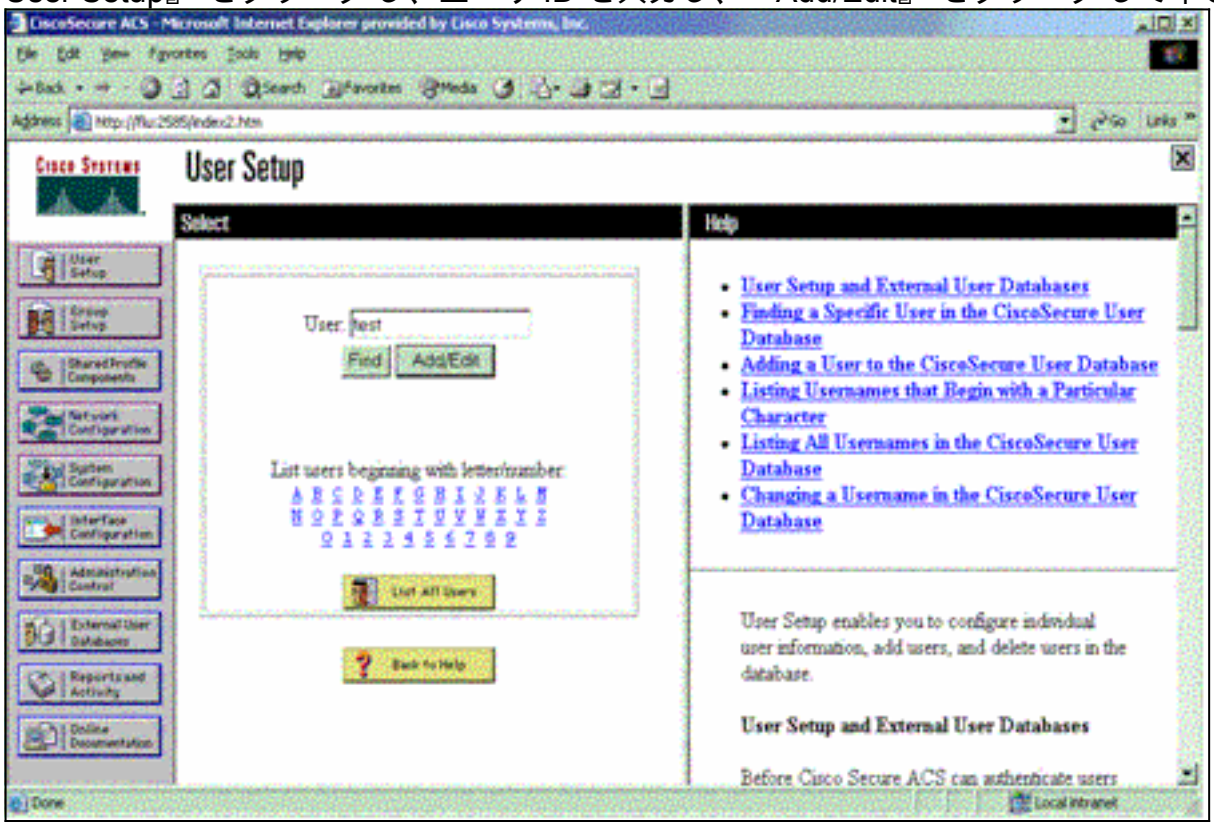
3. 認証、許可、アカウンティング（ AAA ） クライアント（ NAS ）を追加するために『Add Entry』 をクリック して下さい。



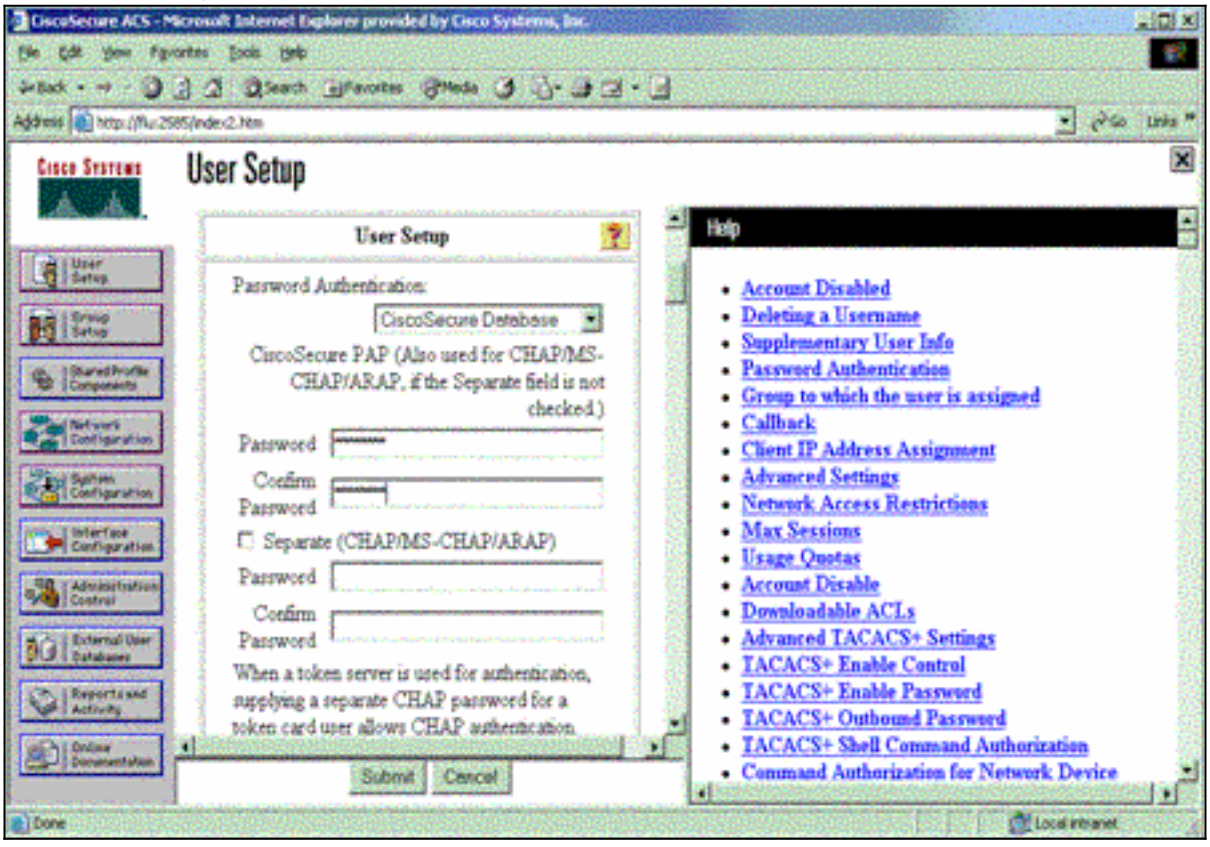
4. ホスト名、IP アドレスおよび AAAサーバと NAS 間の通信を暗号化するのに使用されるキーを入力して下さい。 認証方式として『TACACS+（Cisco IOS）』 を選択 して下さい。 終了したら、変更を加えるために **+Restart を**『SUBMIT』 をクリック して下さい。



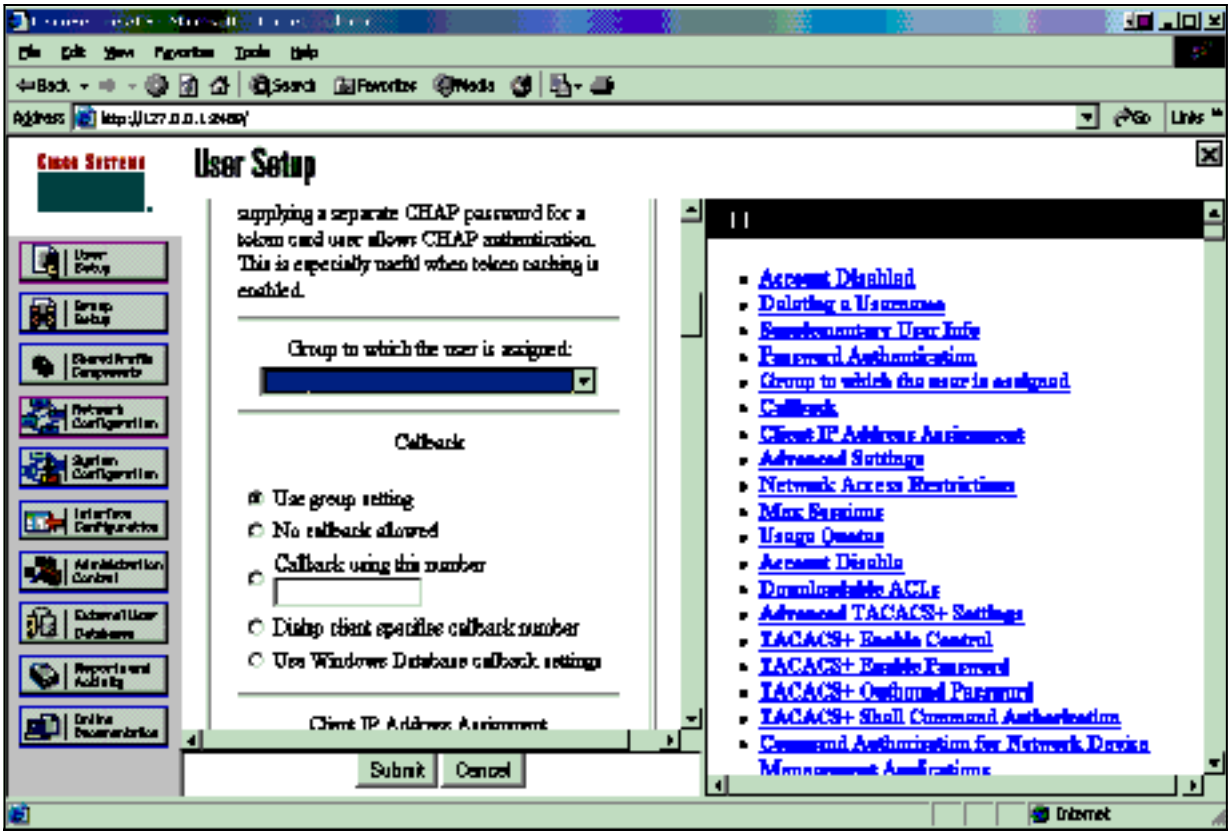
5. 『User Setup』 をクリック し、ユーザ ID を入力し、『Add/Edit』 をクリック して下さい。



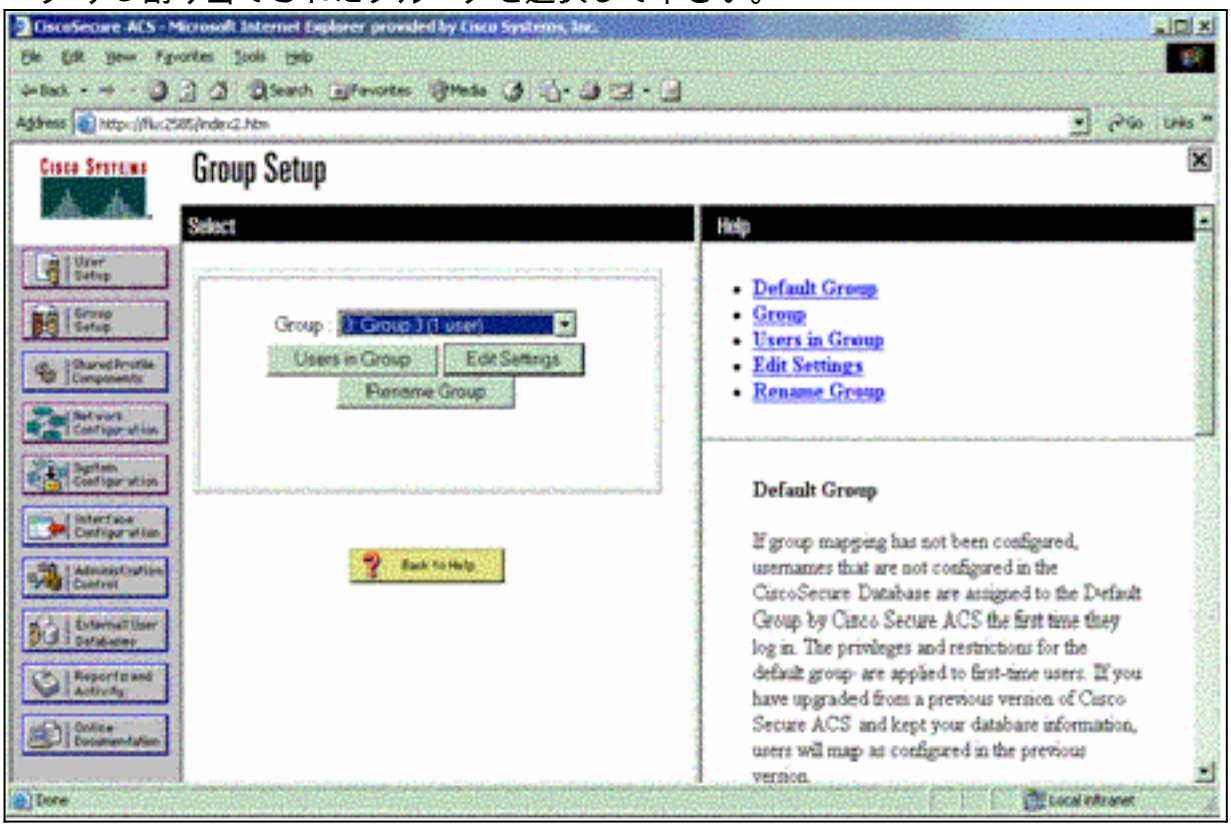
6. ユーザを認証するためにデータベースを選択して下さい。（この例で、ユーザは「テスト」であり、ACS の内部データベースは認証のために使用されます）。 ユーザ向けのパスワードを入力し、パスワードを確認して下さい。



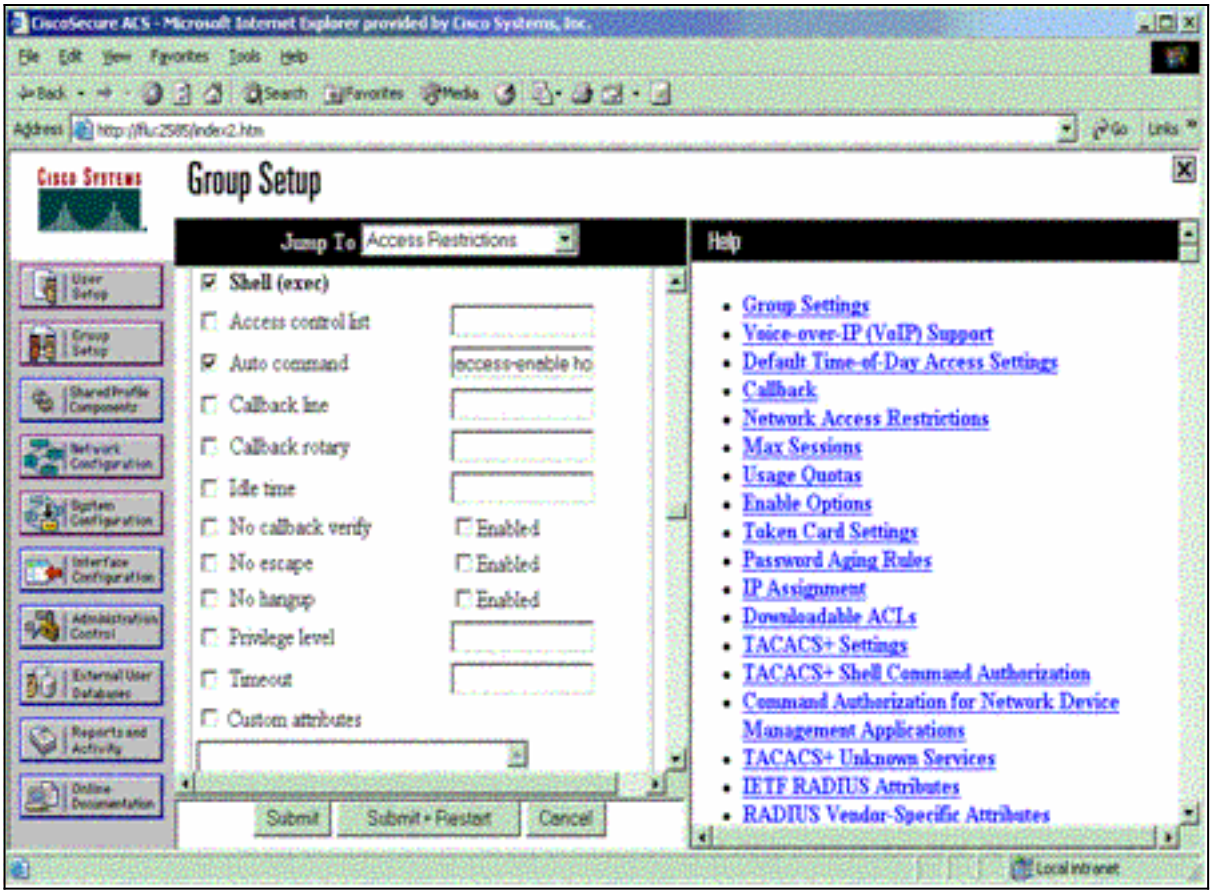
7. ユーザが割り当てられる選択し、**使用 グループ設定を**チェックして下さいグループを。[Submit] をクリックします。



8. 『Group Setup』 をクリック して下さい。 ユーザがステップ 7.で『Edit Settings』 をクリック する割り当てられたグループを選択して下さい。



9. TACACS+ 設定セクションにスクロールして下さい。 **シェル exec が**あるようにボックスを確認して下さい。 **オートコマンドが**あるようにボックスを確認して下さい。 ユーザの認証の成功に実行されたべき autocommand を入力して下さい。 （ この例は **access-enable host timeout 10 コマンドを**使用します。 ）[Submit + Restart] をクリックします。



TACACS+ を解決して下さい

TACACS+ 問題を解決する NAS のこれらの **debug コマンドを**使用して下さい。

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。

- **debug tacacs authentication** — TACACS+ 認証 プロセスの情報を表示する。 いくつかのソフトウェアのバージョンだけで利用可能。 利用できなかったら、**debug tacacs だけを**使用して下さい。
- **debug tacacs authorization** — TACACS+ 許可 プロセスの情報を表示する。 いくつかのソフトウェアのバージョンだけで利用可能。 利用できなかったら、**debug tacacs だけを**使用して下さい。
- **debug tacacs events** — TACACS+ 助手プロセスからの情報を表示する。 いくつかのソフトウェアのバージョンだけで利用可能。 利用できなかったら、**debug tacacs だけを**使用して下さい。

AAA 問題を解決するこれらのコマンドを使用して下さい:

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

ここのサンプル デバッグ 出力は ACS TACACS+ サーバの認証の成功および許可 プロセスを表示します。

```
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
```

RADIUS の使用

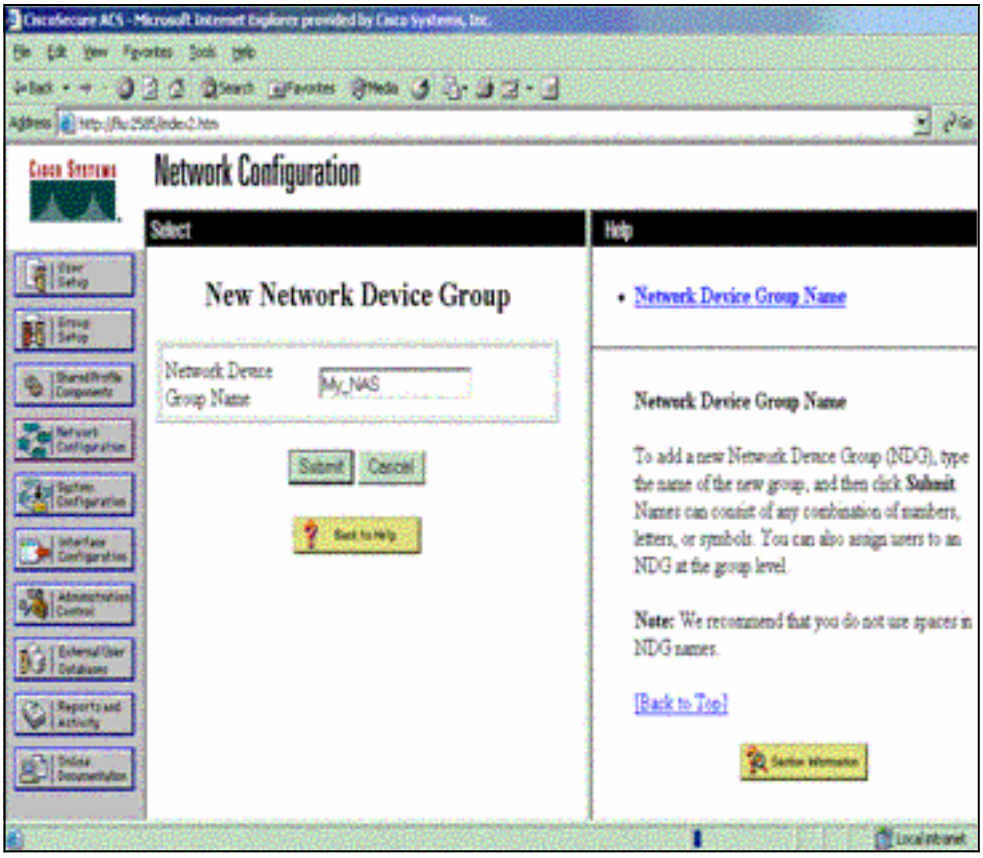
設定 RADIUS

RADIUS を使用するために、認証をここに示されているように vendor-specific属性 26 で、送信されるべき許可 パラメータ（autocommand）の RADIUSサーバでされるために強制するようにRADIUSサーバを設定して下さい:

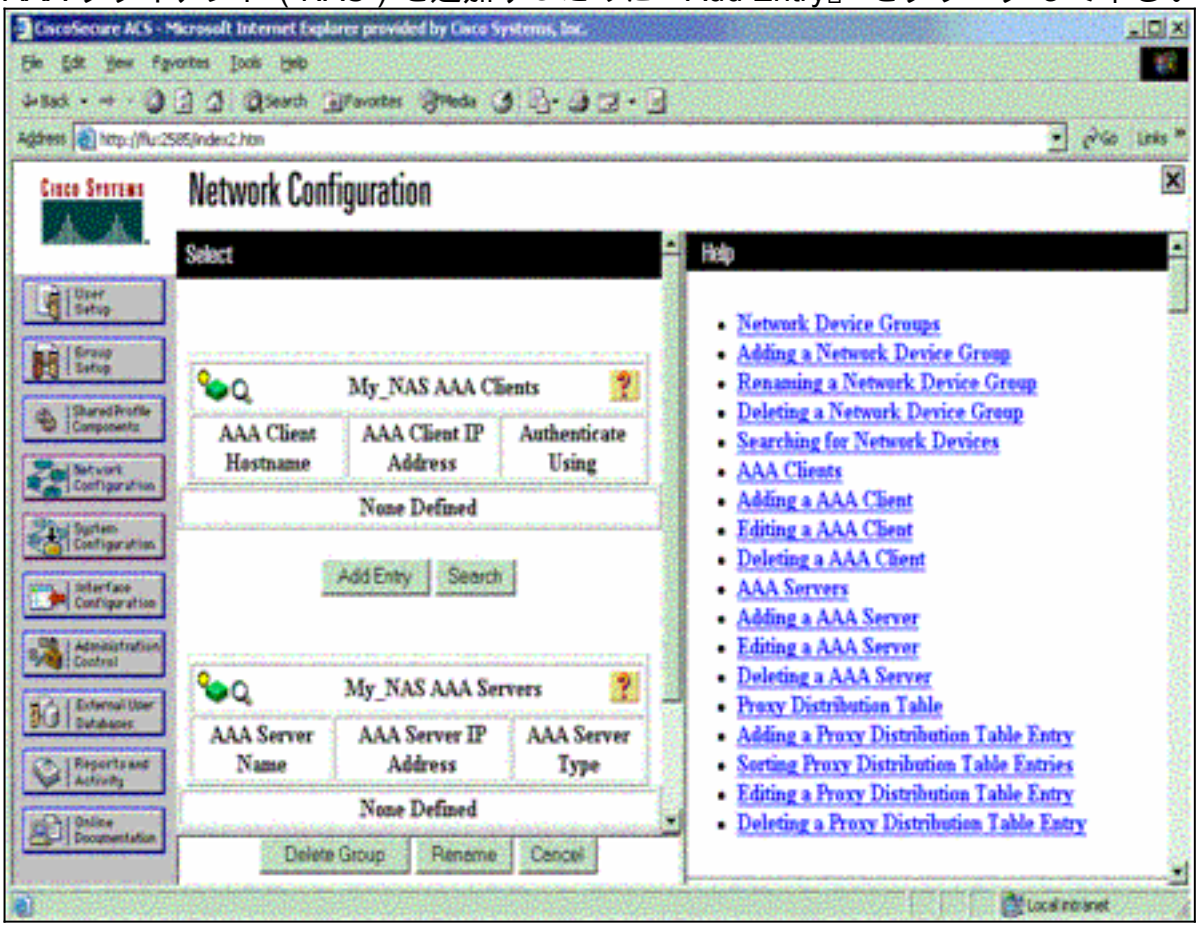
```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authorization exec default group radius local
radius-server host 10.48.66.53 auth-port 1645
   acct-port 1646 key cisco123
```

Windows のための RADIUS Secure ACS を on Cisco 設定するためにこれらのステップを完了して下さい:

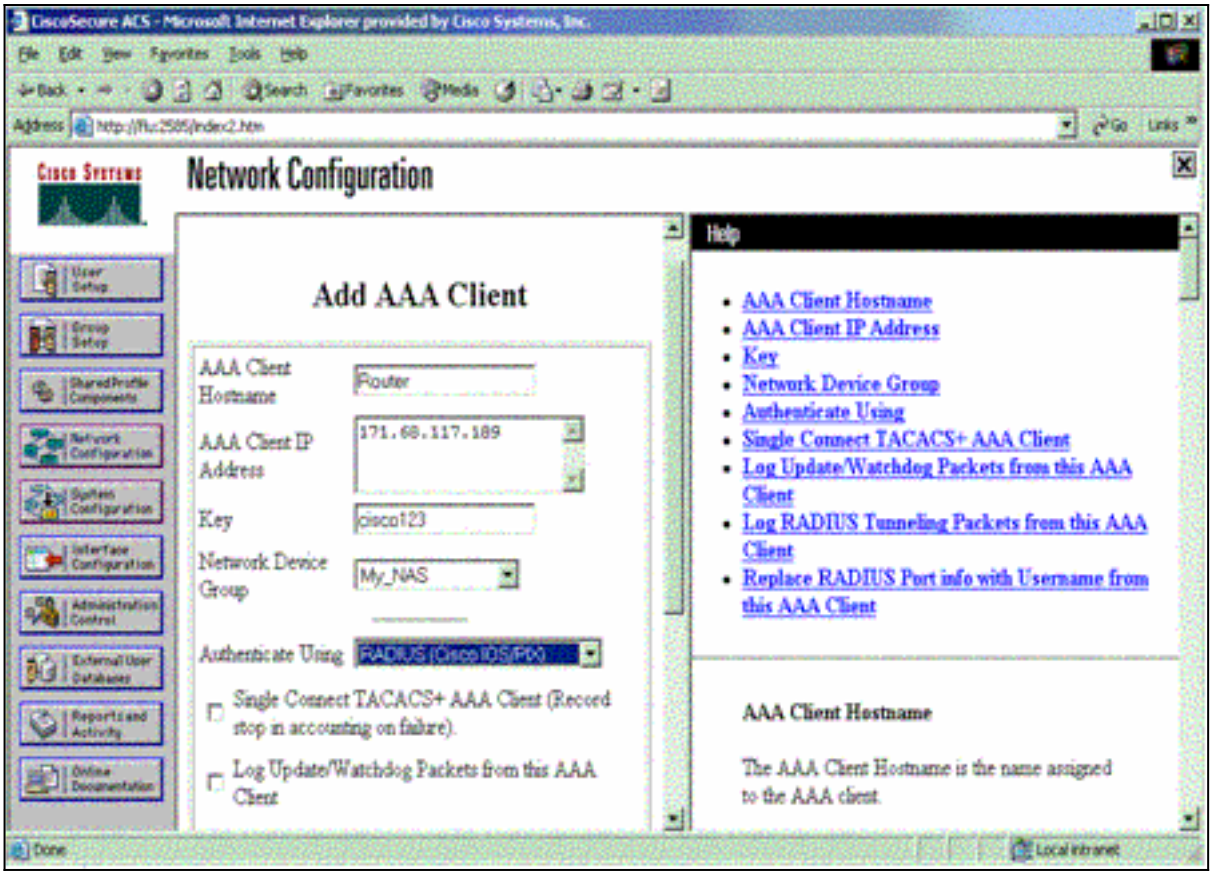
1. http:// *<IP_address か DNS_name>:2002* の形にある Webブラウザを開き、ACS サーバのアドレスを入力して下さい。（この例は 2002 年のデフォルトポートを使用します。）admin としてログイン。
2. [Network Configuration] をクリックします。 NAS が含まれているネットワーク デバイス グループを作成するために『Add Entry』 をクリック して下さい。 グループの名前を入力し、『SUBMIT』 をクリック して下さい。



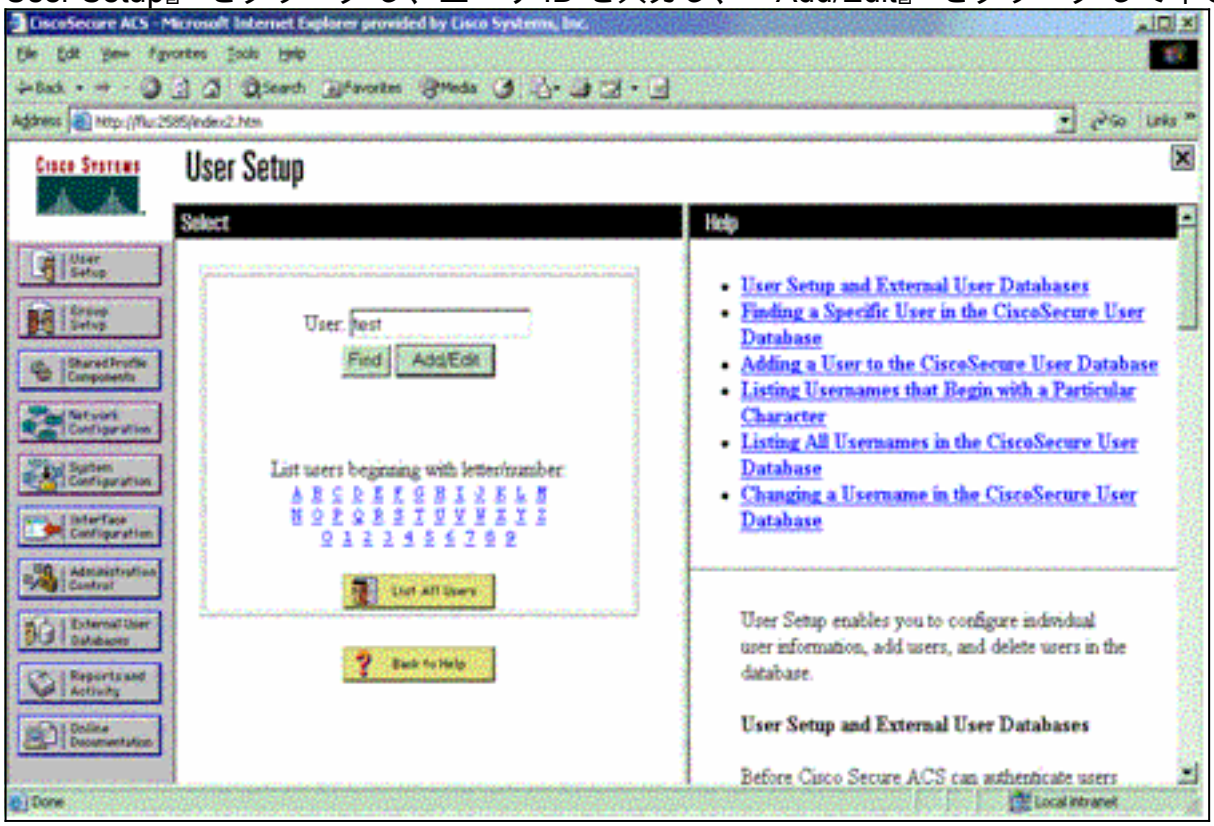
3. AAA クライアント（NAS）を追加するために『Add Entry』 をクリック して下さい。



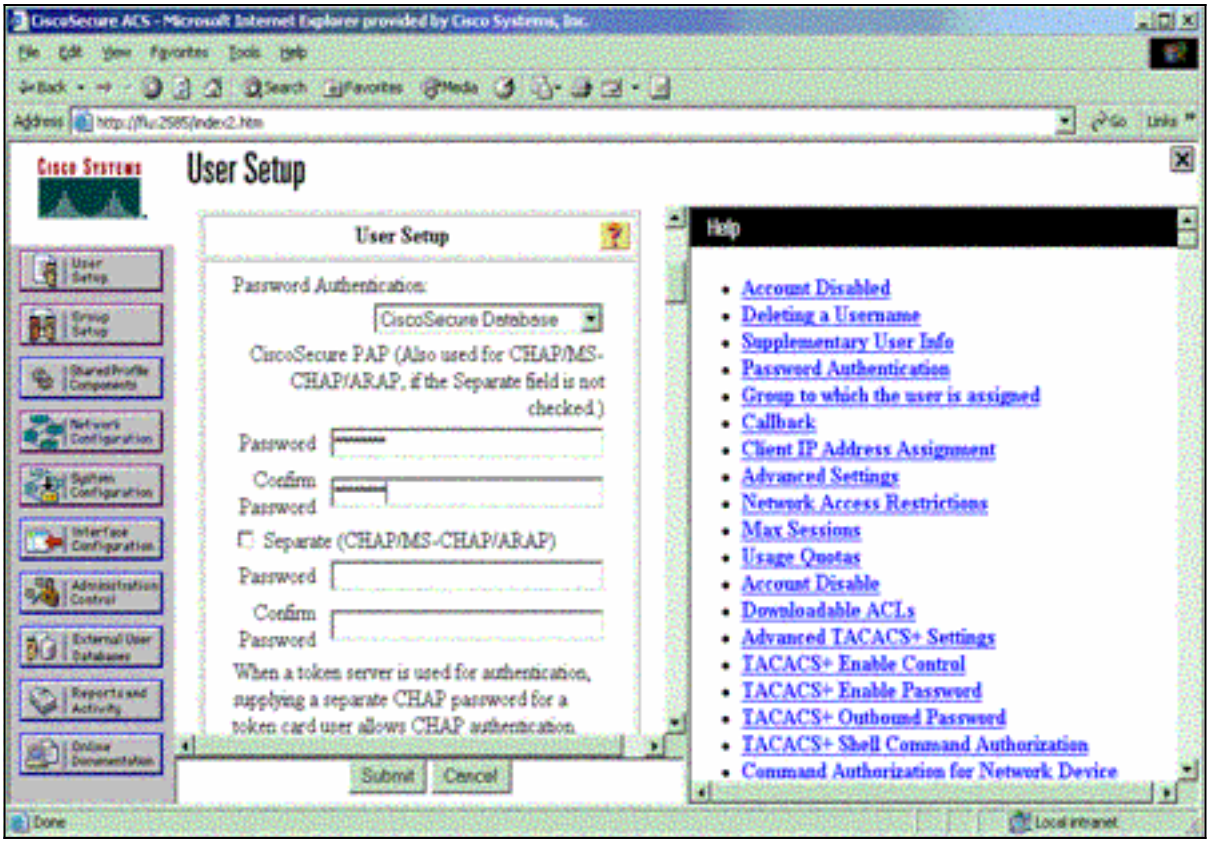
4. ホスト名、IP アドレスおよび AAAサーバと NAS 間の通信を暗号化するのに使用されるキーを入力して下さい。 認証方式として（**Cisco IOS/PIX**）『RADIUS』 を選択 して下さい。終了したら、変更を加えるために **+Restart** を『SUBMIT』 をクリック して下さい。



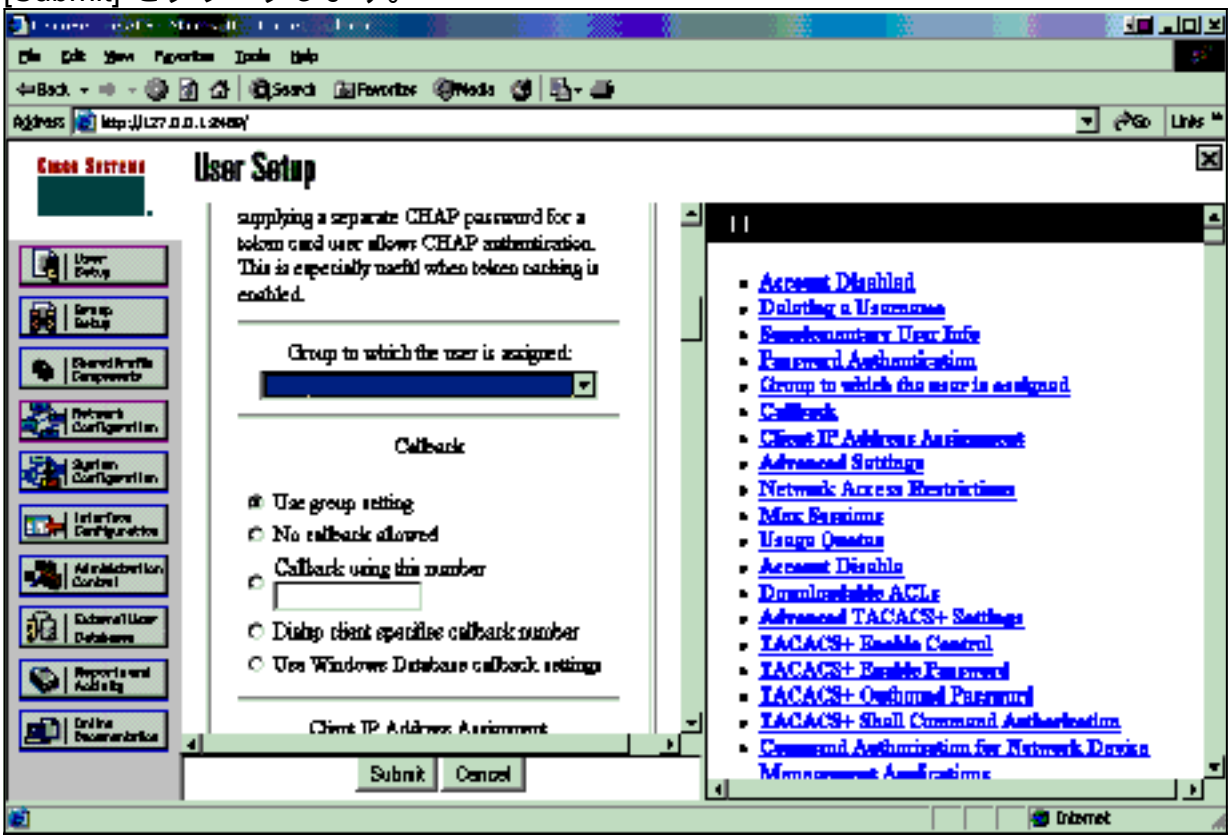
5. 『User Setup』 をクリック し、ユーザ ID を入力し、『Add/Edit』 をクリック して下さい。



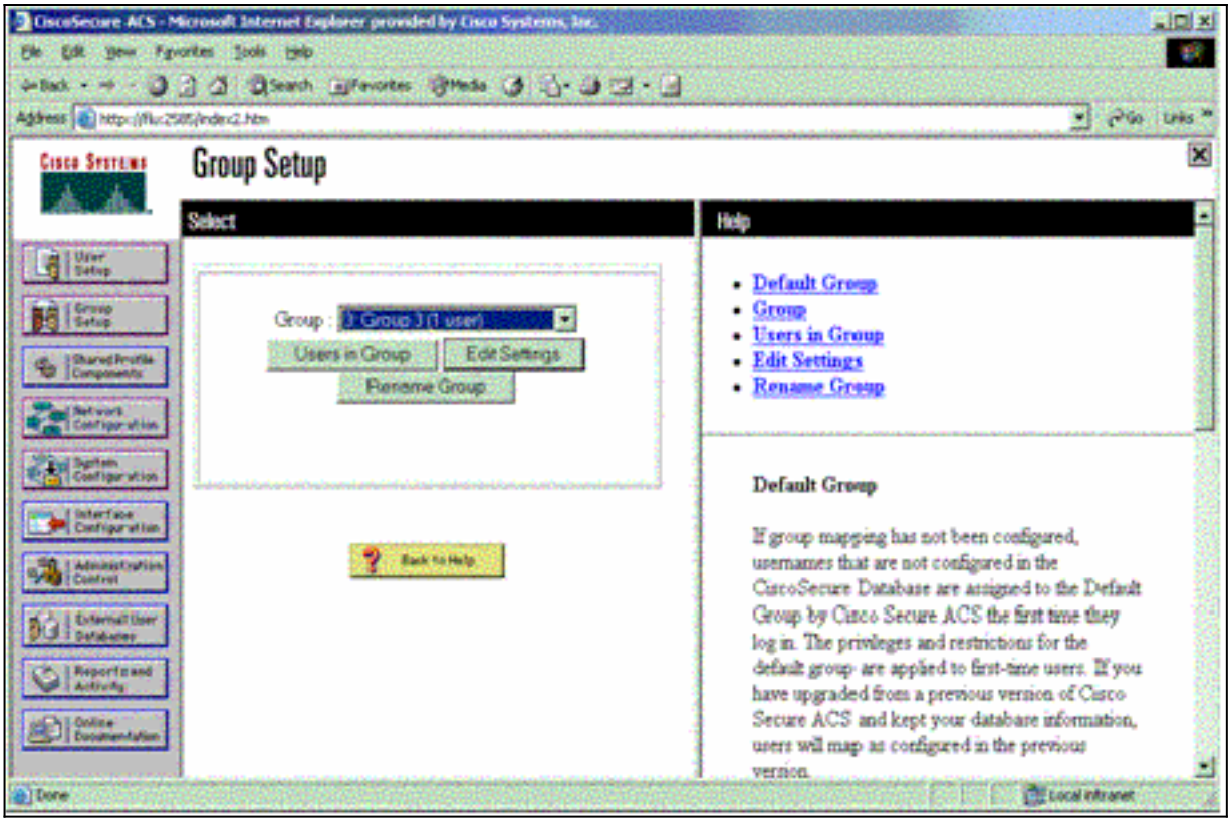
6. ユーザを認証するためにデータベースを選択して下さい。（この例で、ユーザは「テスト」であり、ACS の内部データベースは認証のために使用されます）。 ユーザ向けのパスワードを入力し、パスワードを確認して下さい。



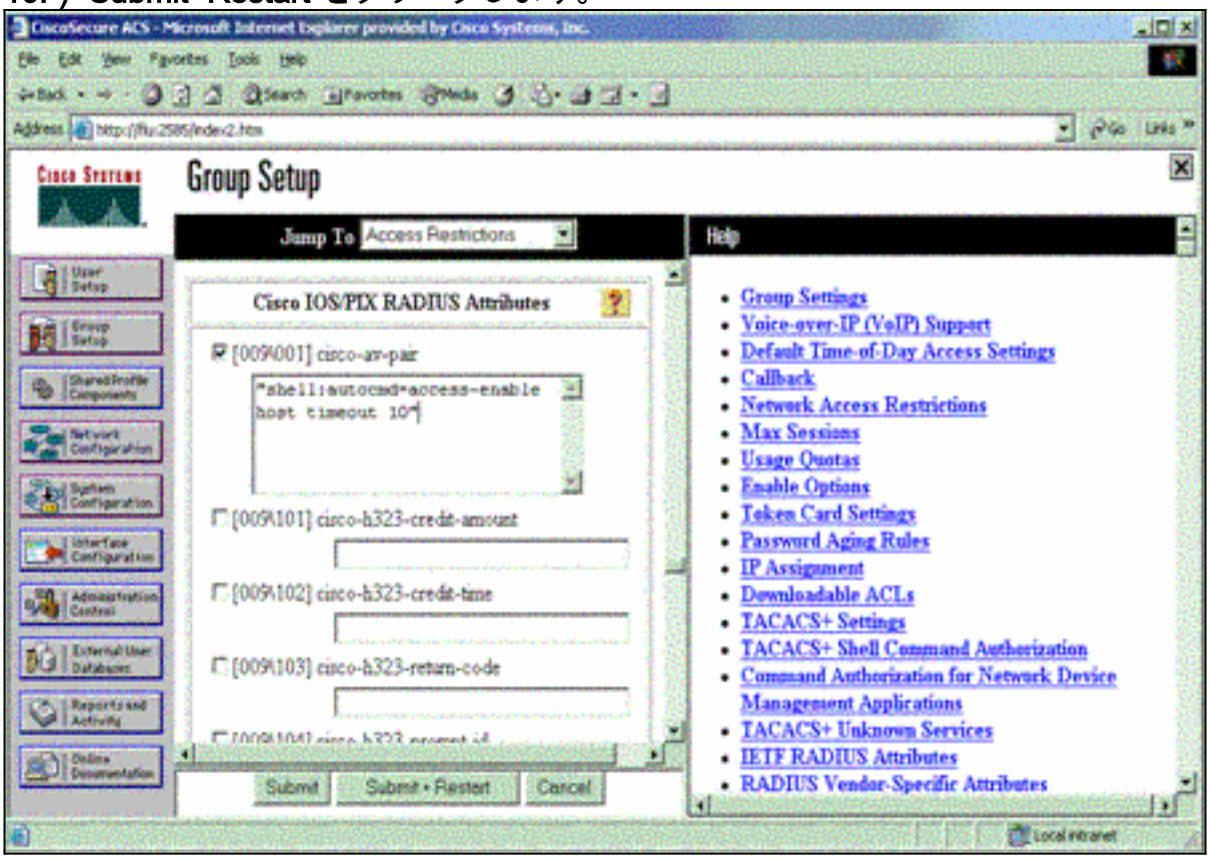
7. ユーザが割り当てられる選択し、**使用 グループ設定を**チェックして下さいグループを。[Submit] をクリックします。



8. ユーザが前の手順で割り当てられたグループを『Group Setup』 をクリック し、選択して下さい。 Edit Settings をクリックします。



9. Cisco IOS/PIX RADIUS特性 セクションにスクロールして下さい。 **cisco-av-pair** があるようにボックスを確認して下さい。 ユーザの認証の成功に実行された **shell コマンドを**入力して下さい。 （ この例は**シェルを**使用します: **autocmd=access-enable ホスト タイムアウトは 10.** ） **Submit+Restart** をクリックします。



RADIUS を解決して下さい

RADIUS 問題を解決する NAS のこれらの **debug コマンドを**使用して下さい。

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。

- debug tacacs - RADIUS に関する情報を表示します。

AAA 問題を解決するこれらのコマンドを使用して下さい:

- **debug aaa authentication**：AAA/TACACS+ 認証に関する情報を表示します。
- **debug aaa authorization**：AAA/TACACS+ 許可に関する情報を表示します。

ここのサンプル デバッグ 出力は RADIUS のために設定される ACS の認証の成功および許可 プロセスを表示します。

```
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
```

関連情報

- Cisco IOS Lock and Key セキュリティ
- 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
- RADIUS に関するサポート ページ
- Requests for Comments (RFC)
- テクニカルサポートとドキュメント - Cisco Systems