RADIUS を使用した VPN 3000 コンセントレータと VPN Client 4.x for Windows 間のユーザ認証とアカウンティングのための IP セキュリティ設定例

目次

概要

このドキュメントでは、Cisco VPN 3000 コンセントレータと Cisco VPN Client 4.x for Microsoft Windows の間に、ユーザ認証とアカウンティングのために RADIUS を使用する IPSec トンネルを設定する方法について説明しています。 このドキュメントでは、VPN 3000 コンセントレータに接続するユーザの認証用の RADIUS の設定を簡単にするために、Cisco Secure Access Control Server (ACS) for Windows の使用を推奨しています。 VPN 3000 コンセントレータでのグループとは、1 つのエンティティとして処理されるユーザの集まりです。 ユーザを個々に設定する場合に対して、グループを設定すると、システム管理が簡素化され、設定作業の合理化が可能です。

Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS サーバを使用して Cisco VPN Client (4.x for Windows) と PIX 500 シリーズ セキュリティ アプライアンス 7.x の間にリモ

ート アクセス VPN 接続を設定する方法については、『Microsoft Windows 2003 IAS RADIUS 認証を使用する PIX/ASA 7.x と Cisco VPN Client 4.x for Windows 設定例』を参照してください。

ユーザ認証に RADIUS を使用してルータと Cisco VPN Client 4.x の間の接続を設定する方法については、『RADIUS を使用した Cisco IOS ルータと Cisco VPN Client 4.x for Windows 間の IPSec の設定』を参照してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure ACS for Windows RADIUS が、他のデバイスで適切にインストールされていて、動作する。
- Cisco VPN 3000 コンセントレータが設定されており、HTML インターフェイスで管理できる。

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 Secure ACS for Windows バージョン 4.0
- イメージ ファイル 4.7.2.B の Cisco VPN 3000 シリーズ コンセントレータ
- Cisco VPN Client 4.x

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。

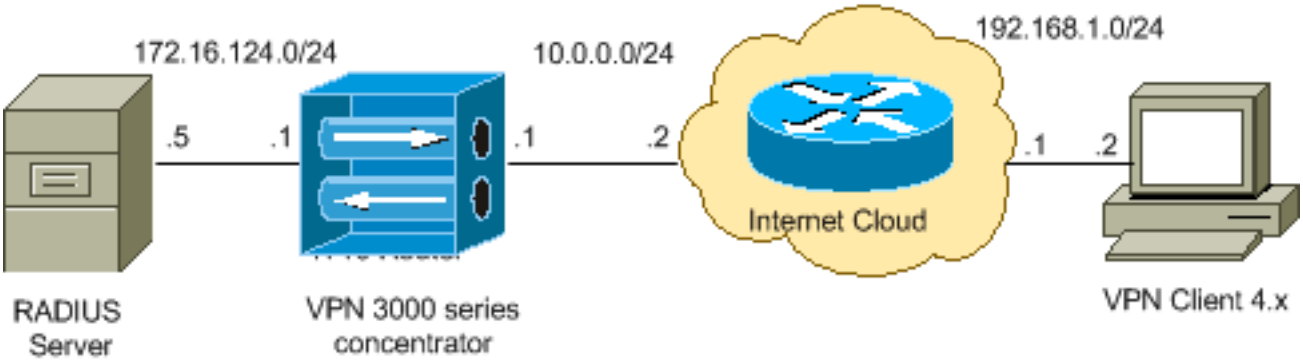
設定

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: このセクション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。



注: この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能なものではありません。 これらは、ラボ環境で使用された RFC 1918 のアドレスです。

VPN 3000 コンセントレータでのグループの使用

Cisco Secure ACS for Windows と VPN 3000 コンセントレータの両方でグループを定義できますが、グループの使用方法は異なります。 手順を簡素化するために、次の作業を実行します。

- 最初のトンネルを確立する際には、**VPN 3000 コンセントレータで 1 つのグループを設定します。** これは通常、トンネル グループと呼ばれ、事前共有キー（グループ パスワード）を使用して VPN 3000 コンセントレータへの暗号化されたインターネット キー エクスチェンジ（IKE）セッションを確立するために使用されます。 これは、VPN コンセントレータに接続しようとするすべての Cisco VPN Client で設定する必要がある同じグループ名とパスワードです。
- ポリシー管理に標準 RADIUS 属性とベンダー固有属性（VSA）を使用する**グループを、Cisco Secure ACS for Windows サーバ上で設定します。** VPN 3000 コンセントレータで使用する必要がある VSA は RADIUS（VPN 3000）属性です。
- **Cisco Secure ACS for Windows RADIUS サーバでユーザを設定し、これらのユーザを同じサーバ上で設定されたグループのいずれかに割り当てます。** グループに定義された属性がユーザに継承され、ユーザの認証時に Cisco Secure ACS for Windows がこれらの属性を VPN コンセントレータに送信します。

VPN 3000 コンセントレータでのグループとユーザ属性の使用方法

VPN 3000 コンセントレータでは、VPN コンセントレータでトンネル グループを認証し、RADIUS でユーザを認証してから、受信した属性を整理する必要があります。 VPN コンセントレータでは、認証を VPN コンセントレータで行う場合も RADIUS で行う場合も、属性は次の優先順位で使用されます。

1. **ユーザ属性**：これらの属性は他の属性よりも常に優先されます。
2. **トンネル グループ属性**：ユーザの認証時に戻されなかったすべての属性は、トンネル グループ属性によって書き込まれます。
3. **ベース グループ属性**：ユーザ属性やトンネル グループ属性で欠如しているすべての属性は、VPN コンセントレータのベース グループ属性によって書き込まれます。

VPN 3000 シリーズ コンセントレータの設定

このセクションの手順を実行して、IPSec 接続に必要なパラメータを Cisco VPN 3000 コンセントレータで設定し、RADIUS サーバで認証を行う VPN ユーザに AAA クライアントを設定します

。

このラボ設定では、VPN コンセントレータへのアクセスはまずコンソール ポートを介して行われ、次の出力で示すように最低限の設定が追加されます。

```
Login: admin
!--- The password must be "admin". Password:***** Welcome to Cisco Systems VPN 3000 Concentrator
Series Command Line Interface Copyright (C) 1998-2005 Cisco Systems, Inc. 1) Configuration 2)
Administration 3) Monitoring 4) Save changes to Config file 5) Help Information 6) Exit Main ->
1 1) Interface Configuration 2) System Management 3) User Management 4) Policy Management 5)
Tunneling and Security 6) Back Config -> 1 This table shows current IP addresses. Intf Status IP
Address/Subnet Mask MAC Address ----------------------------------------------------------------
-------------- Ether1-Pri| DOWN | 10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not
Configured| 0.0.0.0/0.0.0.0 | Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | --------------------
---------------------------------------------------------- DNS Server(s): DNS Server Not
Configured DNS Domain Name: Default Gateway: Default Gateway Not Configured 1) Configure
Ethernet #1 (Private) 2) Configure Ethernet #2 (Public) 3) Configure Ethernet #3 (External) 4)
Configure Power Supplies 5) Back Interfaces -> 1 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 1 1)
Disable 2) Enable using DHCP Client 3) Enable using Static IP Addressing Ethernet Interface 1 ->
[ ] 3 This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----
---------------------------------------------------------------------------- Ether1-Pri| DOWN |
10.1.1.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 | Ether3-
Ext|Not Configured| 0.0.0.0/0.0.0.0 | ----------------------------------------------------------
--------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default Gateway:
Default Gateway Not Configured > Enter IP Address Ethernet Interface 1 -> [ 10.1.1.1 ]
172.16.124.1 20 02/14/2007 09:50:18.830 SEV=3 IP/2 RPT=3 IP Interface 1 status changed to Link
Down. 21 02/14/2007 09:50:18.830 SEV=3 IP/1 RPT=3 IP Interface 1 status changed to Link Up. 22
02/14/2007 09:50:18.950 SEV=3 IP/1 RPT=4 IP Interface 1 status changed to Link Up. > Enter
Subnet Mask 23 02/14/2007 09:50:19.460 SEV=3 IP/2 RPT=4 IP Interface 1 status changed to Link
Down. Ethernet Interface 1 -> [ 255.255.255.0 ] 1) Interface Setting (Disable, DHCP or Static
IP) 2) Set Public Interface 3) Select IP Filter 4) Select Ethernet Speed 5) Select Duplex 6) Set
MTU 7) Set Port Routing Config 8) Set Bandwidth Management 9) Set Public Interface IPSec
Fragmentation Policy 10) Set Interface WebVPN Parameters 11) Back Ethernet Interface 1 -> 11
This table shows current IP addresses. Intf Status IP Address/Subnet Mask MAC Address ----------
---------------------------------------------------------------------- Ether1-Pri| Up |
172.16.124.1/255.255.255.0 | 00.03.A0.89.BF.D0 Ether2-Pub|Not Configured| 0.0.0.0/0.0.0.0 |
Ether3-Ext|Not Configured| 0.0.0.0/0.0.0.0 | ------------------------------------------------
--------------------------- DNS Server(s): DNS Server Not Configured DNS Domain Name: Default
Gateway: Default Gateway Not Configured 1) Configure Ethernet #1 (Private) 2) Configure Ethernet
#2 (Public) 3) Configure Ethernet #3 (External) 4) Configure Power Supplies 5) Back Interfaces -
>
```

クイック コンフィギュレーションに VPN コンセントレータが表示され、次の項目が設定されます。

- 時間/日付
- **Configuration > Interfaces** でインターフェイス/マスク（public=10.0.0.1/24、private=172.16.124.1/24）
- **Configuration > System > IP routing > Default_Gateway** でデフォルトのゲートウェイ（10.0.0.2）

この段階で、VPN コンセントレータは、内部ネットワークから HTML を介してアクセスできます。

注: VPN コンセントレータを外部から管理している場合、次の手順も行います。

1. **Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1. Private（Default）**の順に選択

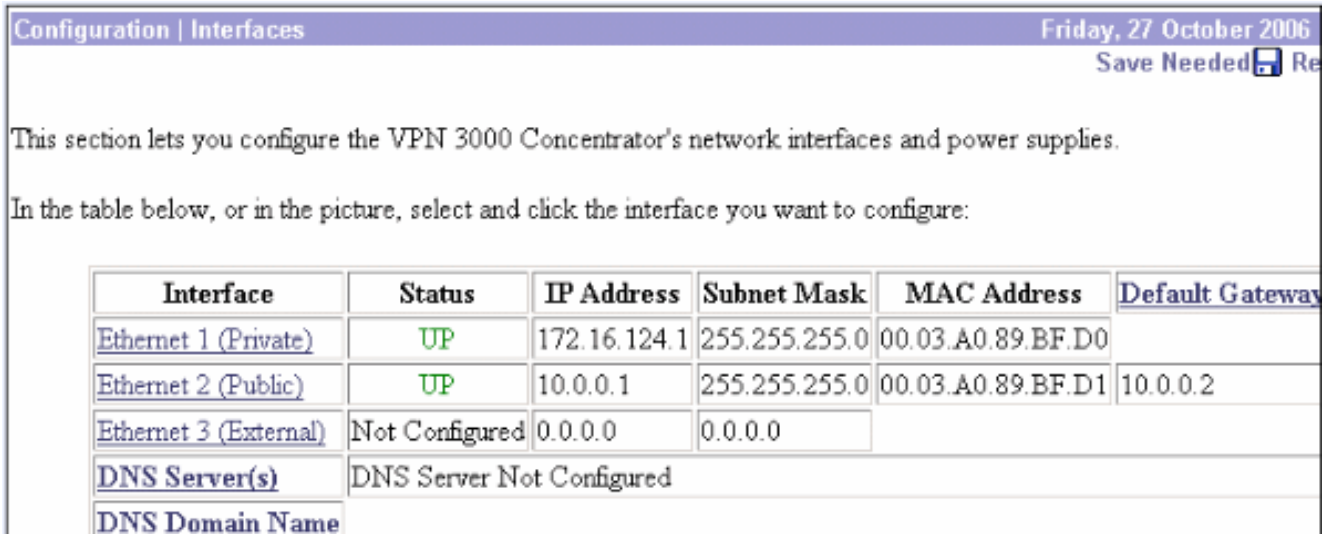
します。

2. **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation** の順に選択し、外部マネージャの IP アドレスを追加します。

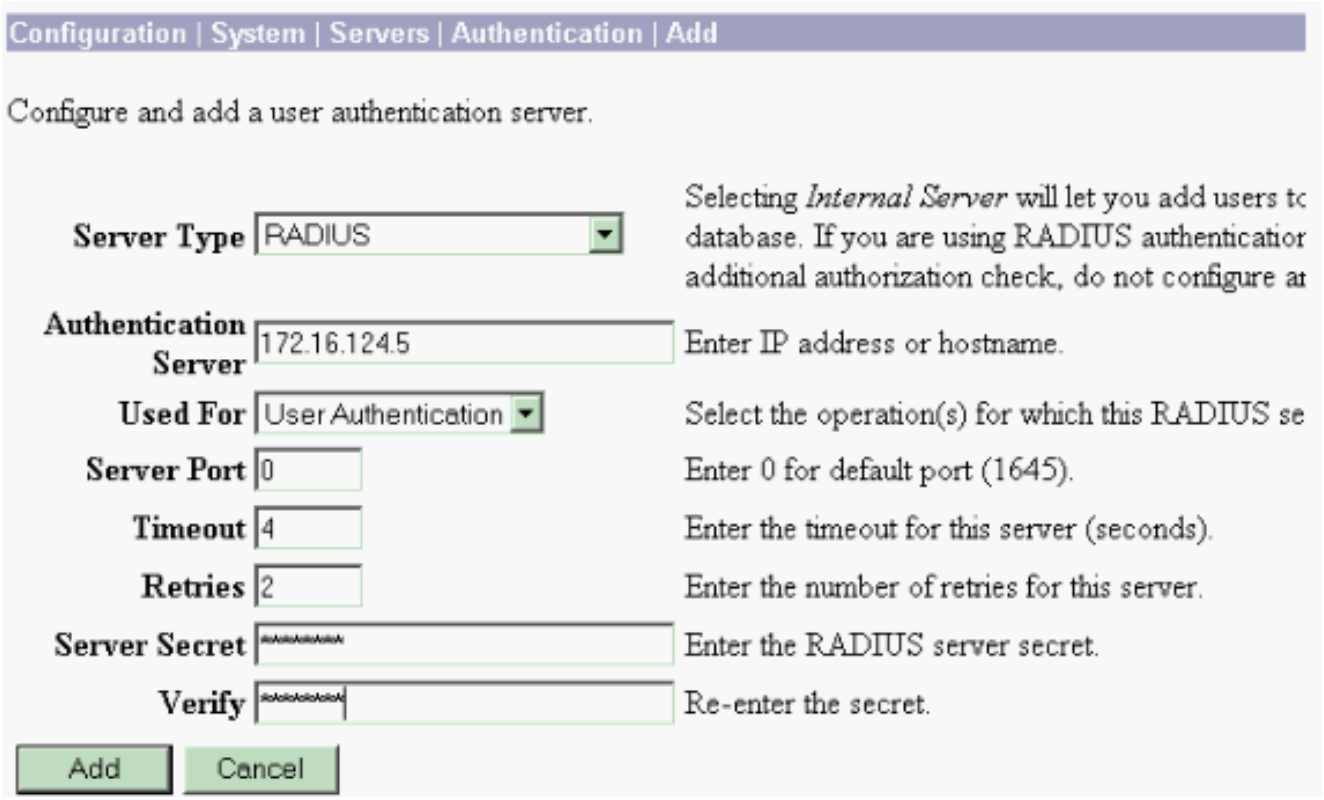
これらの手順が必要になるのは、VPN コンセントレータを外部から管理している場合だけです。

これら 2 つの手順が完了したら、残りの手順は Web ブラウザを使用して、今設定したインターフェイスの IP に接続して GUI で実行できます。 この例ではこの段階で、VPN コンセントレータは、内部ネットワークから HTML を介してアクセスできます。

1. GUI の起動後、インターフェイスを再確認するために、**Configuration > Interfaces** を選択します。



2. これらの手順を実行して、Cisco Secure ACS for Windows RADIUS サーバを VPN 3000 コンセントレータの設定に追加します。**Configuration > System > Servers > Authentication** の順に選択し、左側のメニューから **Add** を選択します。

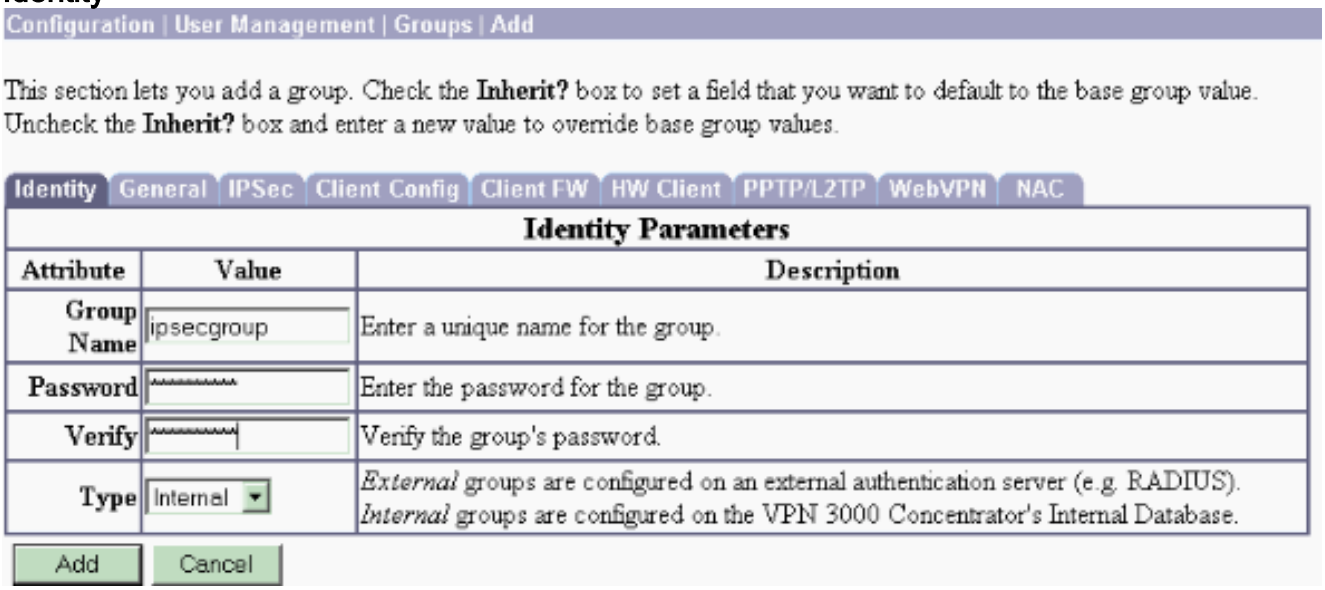


サーバのタイプとして **RADIUS** を選択し、Cisco Secure ACS for Windows RADIUS サーバ用に次のパラメータを追加します。 その他のパラメータは、すべてデフォルト状態のままにしておきます。**Authentication Server**：Cisco Secure ACS for Windows RADIUS サーバの

IP アドレスを入力します。**Server Secret**：RADIUS サーバ シークレットを入力します。 このシークレットは、Cisco Secure ACS for Windows 設定で VPN 3000 コンセントレータを設定したときと同じものを指定する必要があります。**Verify**：確認用にパスワードを再入力します。これにより、VPN 3000 コンセントレータのグローバル設定に認証サーバが追加されます。 このサーバは、認証サーバが具体的に定義されている場合を除き、すべてのグループで使用されます。 あるグループに認証サーバが設定されていない場合は、グローバル認証サーバに戻されます。

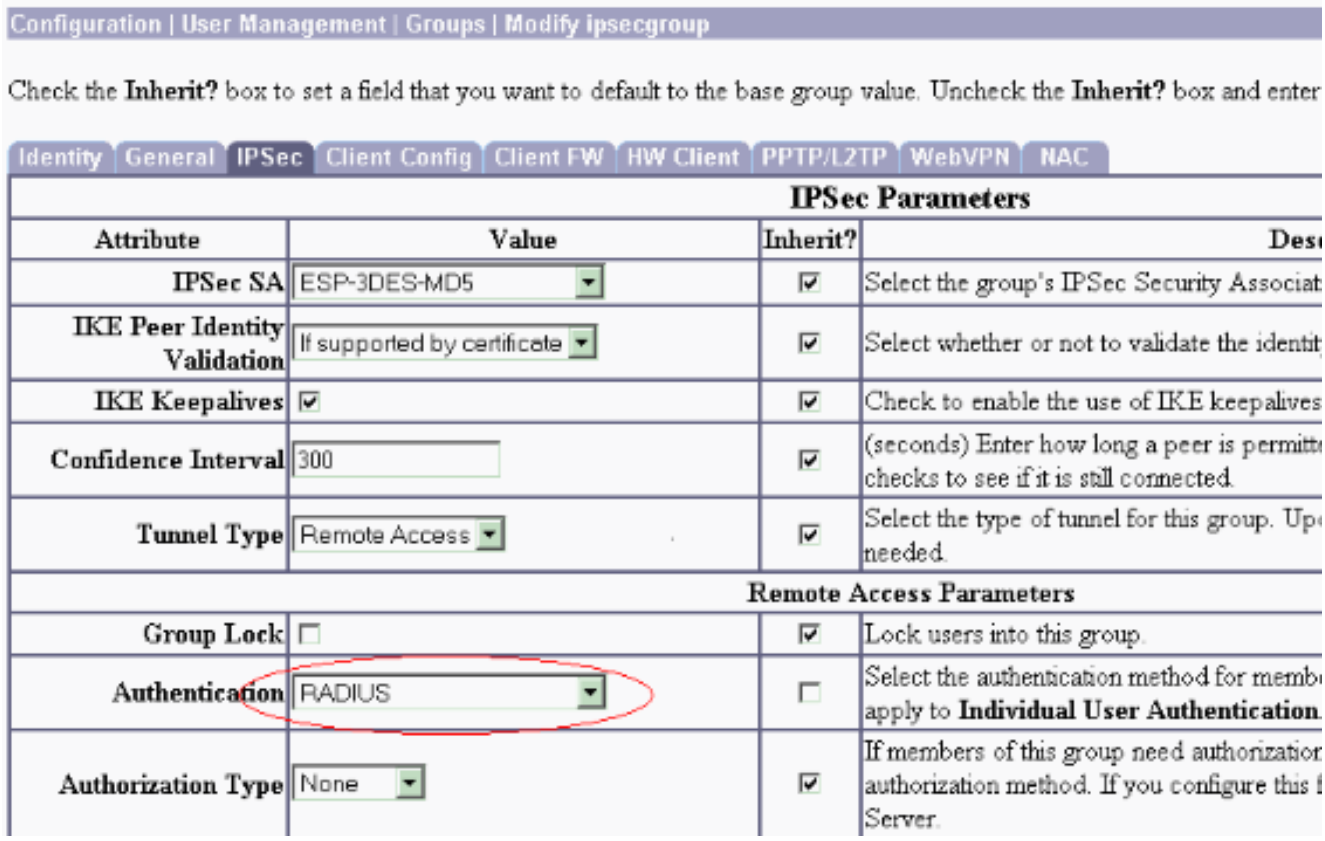
3. 次の手順を実行して、VPN 3000 コンセントレータでトンネル グループを設定します。左側のメニューから **Configuration > User Management > Groups** の順に選択し、**Add** をクリックします。Configuration タブでこれらのパラメータを変更するか、追加します。 これらのパラメータをすべて変更するまで、Apply はクリックしないでください。**注:** VPN また、これらのパラメータは、VPN 3000 コンセントレータのベース グループのデフォルト設定が変更されていないことを前提としています。

Identity



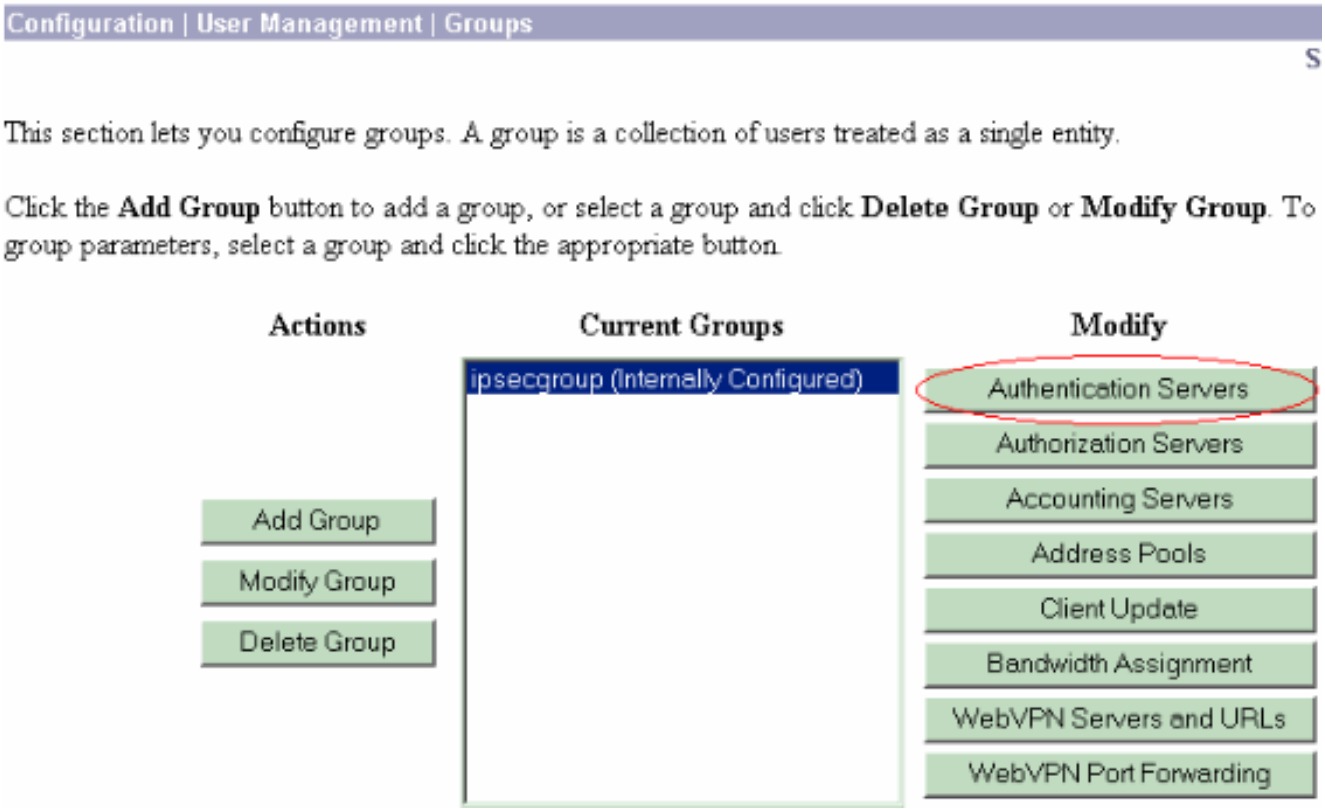
Group Name：グループ名を入力します。 たとえば、IPsecUsers を使用します。**Password**：グループのパスワードを入力します。 これは IKE セッションの事前共有キーです。**Verify**：確認用にパスワードを再入力します。**Type**：この値は、デフォルトの「Internal」のままにしてください。

IPSec



Tunnel Type：**Remote-Access** を選択します。**Authentication**：RADIUS。 この設定により、ユーザの認証に使用する方法が VPN コンセントレータに指示されます。**Mode Config**：**Mode Config** を確認します。[Apply] をクリックします。

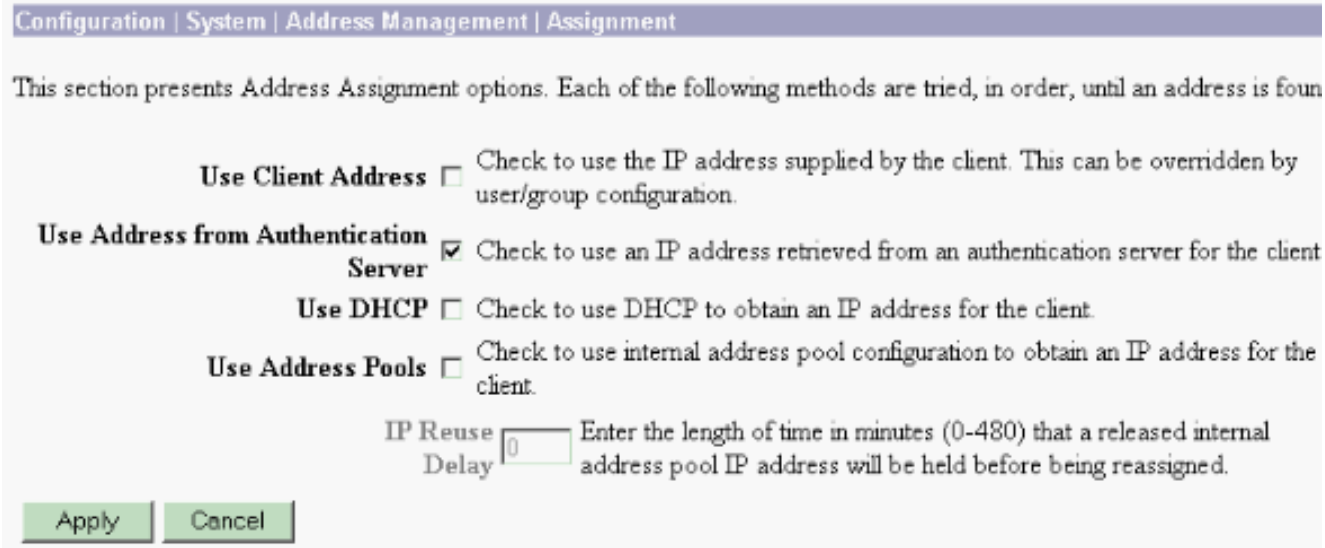
4. これらの手順を実行して、VPN 3000 コンセントレータで複数の認証サーバを設定します。グループの定義後、このグループを選択して、Modify カラムの下で **Authentication Servers** をクリックします。 グローバル サーバに存在しないサーバであっても、個別の認証サーバを各グループに対して定義できます。



サーバのタイプとして **RADIUS** を選択し、Cisco Secure ACS for Windows RADIUS サーバ用に次のパラメータを追加します。 その他のパラメータは、すべてデフォルト状態のまま

にしておきます。**Authentication Server**：Cisco Secure ACS for Windows RADIUS サーバの IP アドレスを入力します。**Server Secret**：RADIUS サーバ シークレットを入力します。 このシークレットは、Cisco Secure ACS for Windows 設定で VPN 3000 コンセントレータを設定したときと同じものを指定する必要があります。**Verify**：確認用にパスワードを再入力します。

5. **Configuration > System > Address Management > Assignment** の順に選択して、**Use Address from Authentication Server** にチェックを入れます。これにより、クライアントの認証後、RADIUS サーバに作成された IP プール内の IP アドレスを VPN Client に割り当てられるようになります。

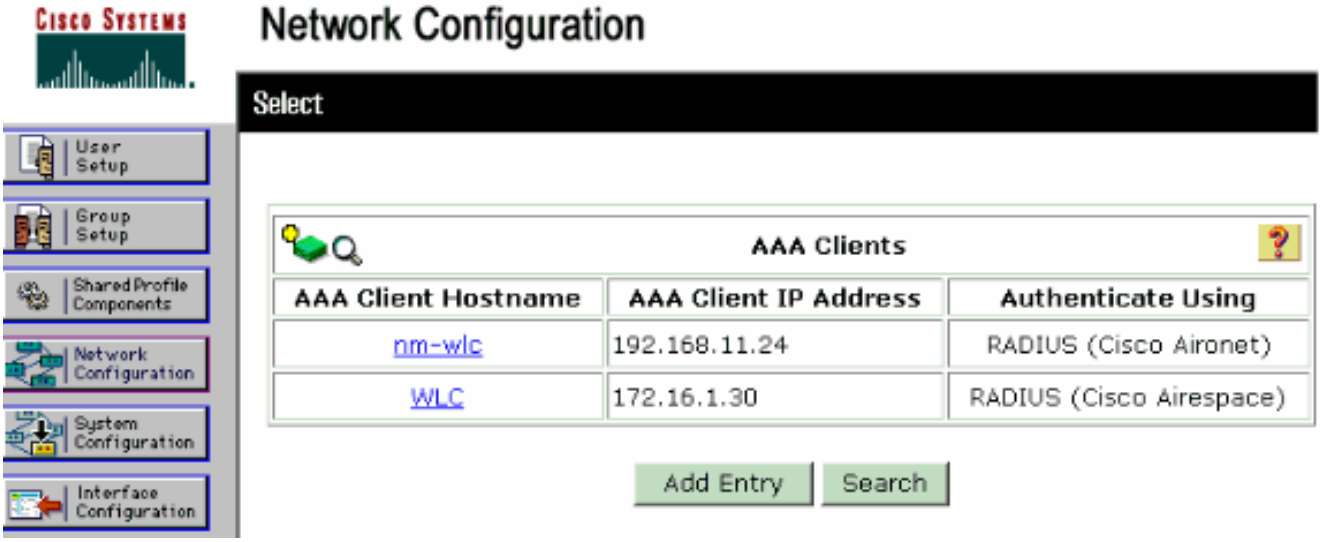


RADIUS サーバの設定

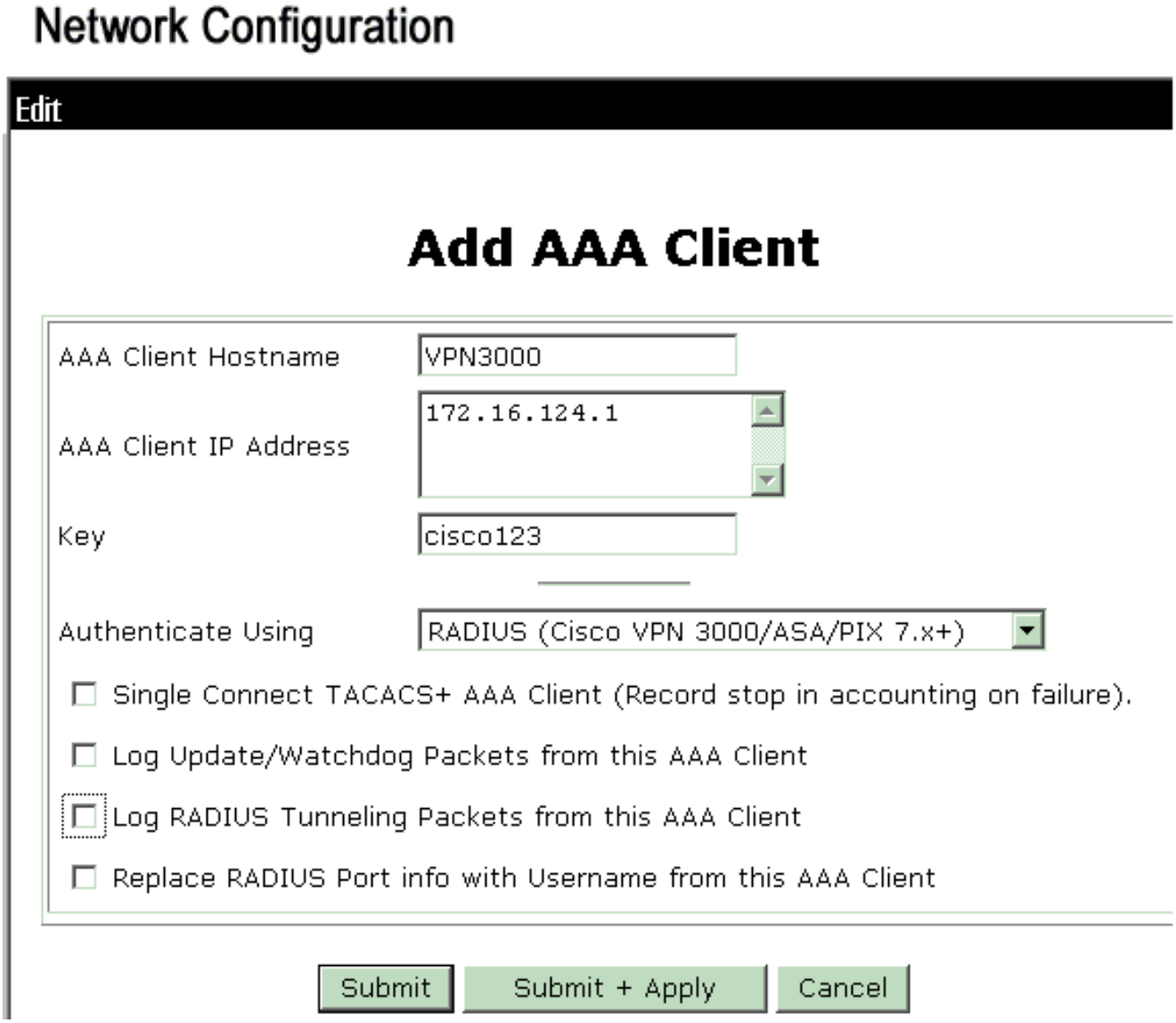
このセクションでは、Cisco VPN 3000 シリーズ コンセントレータ - AAA クライアントから転送された VPN Client ユーザ認証用の RADIUS サーバとして Cisco Secure ACS を設定するために必要な手順を説明しています。

ACS Admin アイコンをダブルクリックして、Cisco Secure ACS for Windows RADIUS サーバが稼働している PC 上で管理セッションを起動します。 必要に応じて、適切なユーザ名とパスワードでログインします。

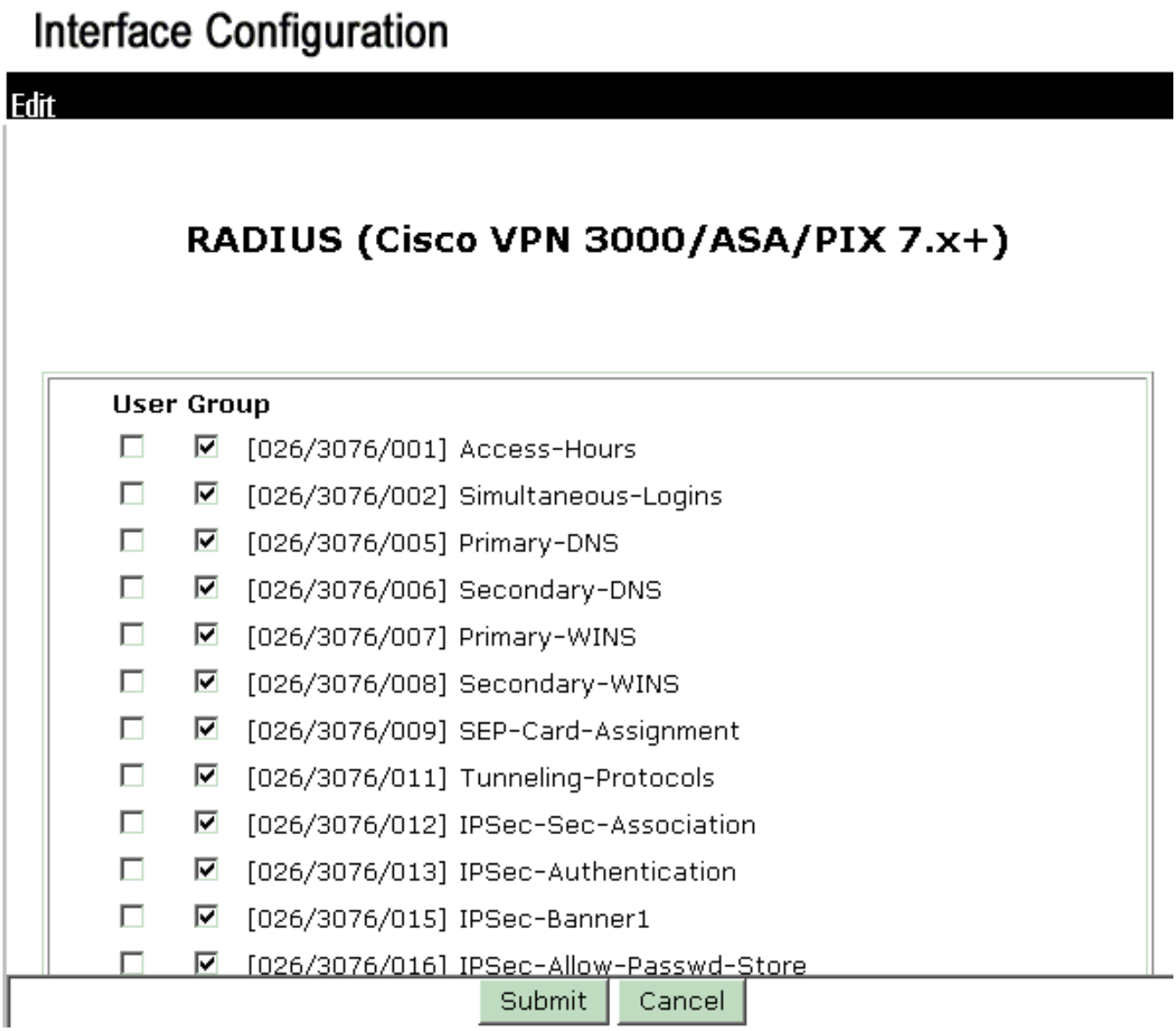
1. これらの手順を実行して、Cisco Secure ACS for Windows サーバの設定に VPN 3000 コンセントレータを追加します。**[Network Configuration]** を選択して **[Add Entry]** をクリックし、RADIUS サーバに AAA クライアントを追加します。



これらのパラメータを VPN 3000 コンセントレータに追加します。

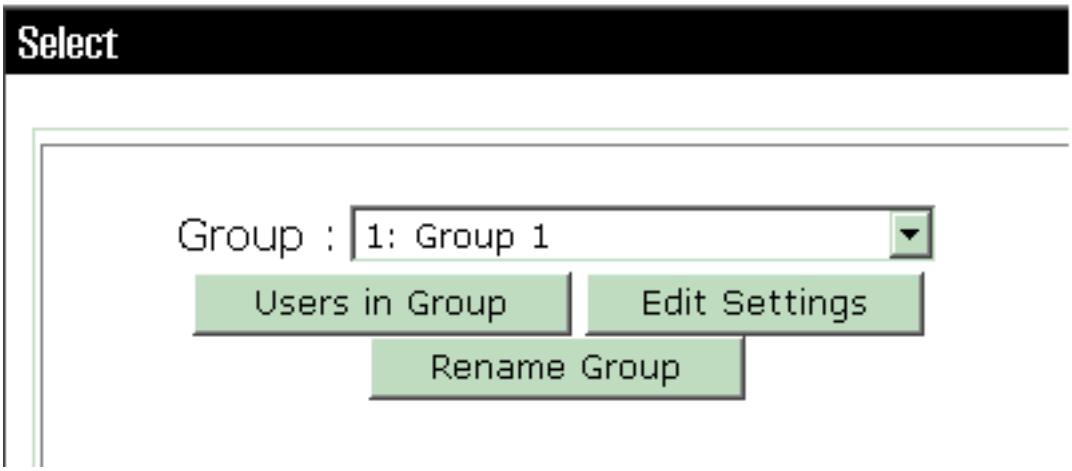


AAA クライアントは- VPN 3000 コンセントレータの... **hostname** —ホスト名入力します（DNS 解決のために）。**AAA Client IP Address**：VPN 3000 コンセントレータの IP アドレスを入力します。**Key**：RADIUS サーバ シークレットを入力します。 ここには、VPN コンセントレータへの認証サーバの追加時に設定したものと同じシークレットを指定する必要があります。**Authenticate Using**：**RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** を選択します。これにより、VPN 3000 VSA で Group 設定ウィンドウが表示されるようになります。[Submit] をクリックします。**[Interface Configuration]** を選択し、**[RADIUS] (Cisco VPN 3000/ASA/PIX 7.x+)** をクリックして、**[Group [26] Vendor-Specific]** にチェックマークを入れます。

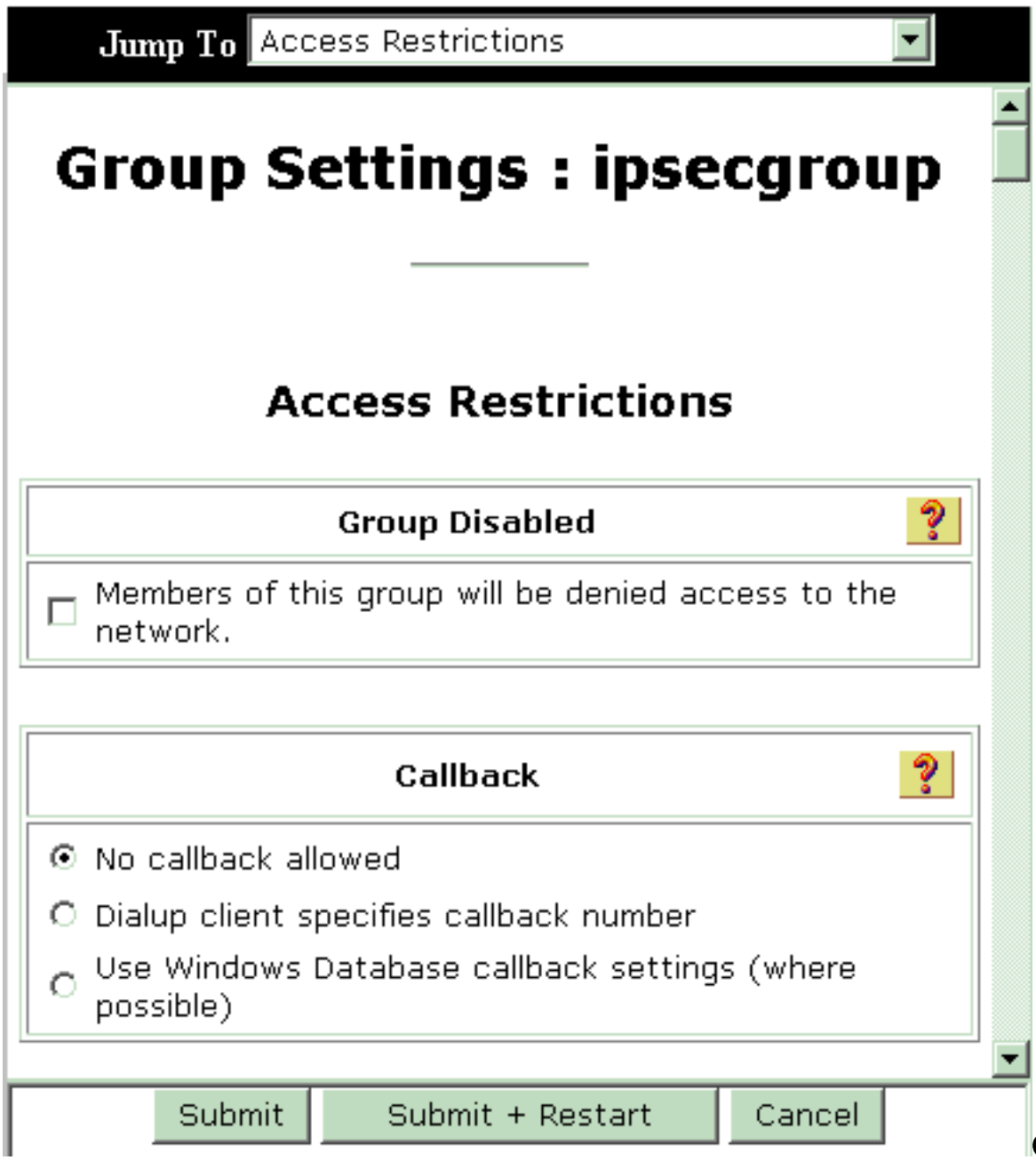


注: 'RADIUS 26 たとえば、Interface Configuration > RADIUS （Cisco VPN 3000 ） の順に選択 し、利用可能 な属性すべてが 026 から開始することがわかって下さい。 これはこれらのベンダ別の属性すべてが IETF RADIUS 26 規格の下で下ることを示します。 これらの属性は、デフォルトでは User Setup や Group Setup に表示されません。 これらがグループ Setup で表示されるようにするには、RADIUS で認証を行う AAA クライアント（この場合は VPN 3000 コンセントレータ）をネットワーク設定に作成します。 次に、User Setup、Group Setup、またはその両方に表示させたい属性をインターフェイス設定から選び、チェックマークを入れます。使用可能な属性とその用途については、『RADIUS の属性』を参照してください。[Submit] をクリックします。

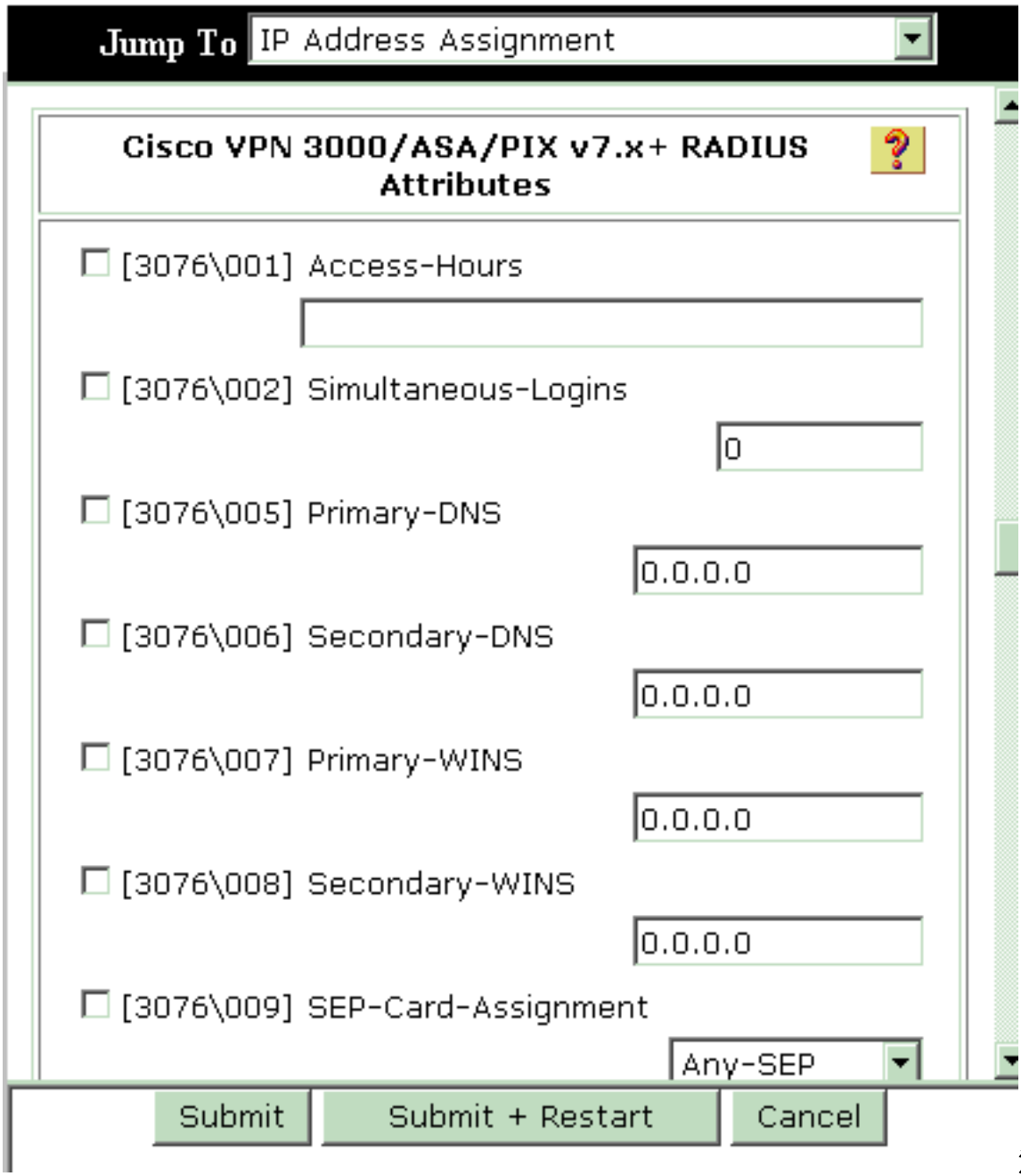
2. これらの手順を実行して、Cisco Secure ACS for Windows の設定にグループを追加します。**Group Setup** を選択してから、Group 1 などいずれかのテンプレート グループを選択し、**Rename Group** をクリックします。



名前を、組織に適した「ipsecgroup」のような名前に変更します。 これらのグループにはユーザが追加されるため、そのグループの実際の用途を反映したグループ名を付けてください。 すべてのユーザを同じグループに追加する場合は、「VPN ユーザ グループ」と命名できます。**[Edit Settings]** をクリックして、新しくリネームしたグループのパラメータを編集します。

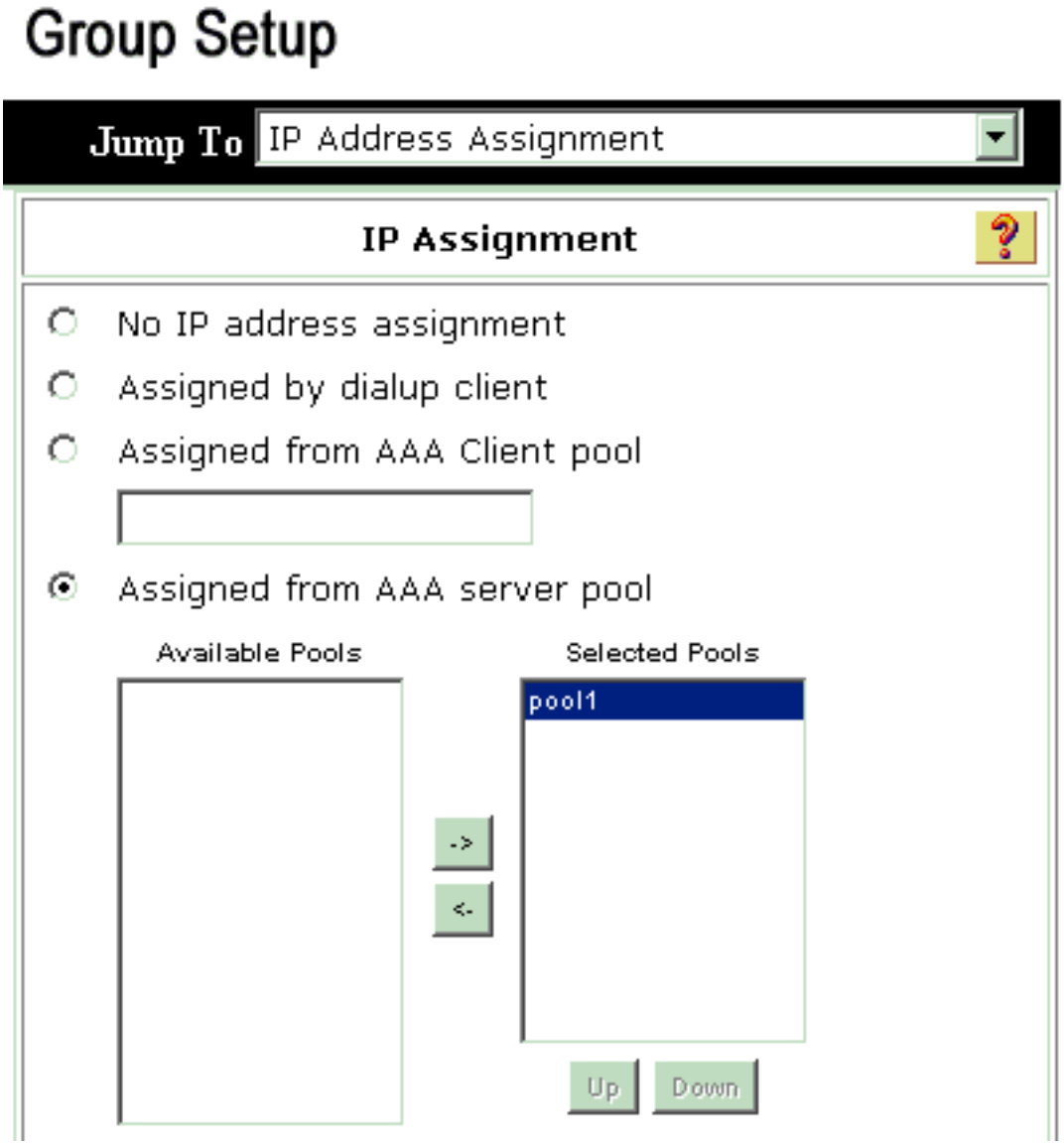


Cisco VPN 3000 RADIUS をクリックし、これらの推奨属性を設定します。 これにより、このグループに割り当てられているユーザに Cisco VPN 3000 RADIUS 属性が継承されるため、すべてのユーザのポリシーを Cisco Secure ACS for Windows で集中管理できます。



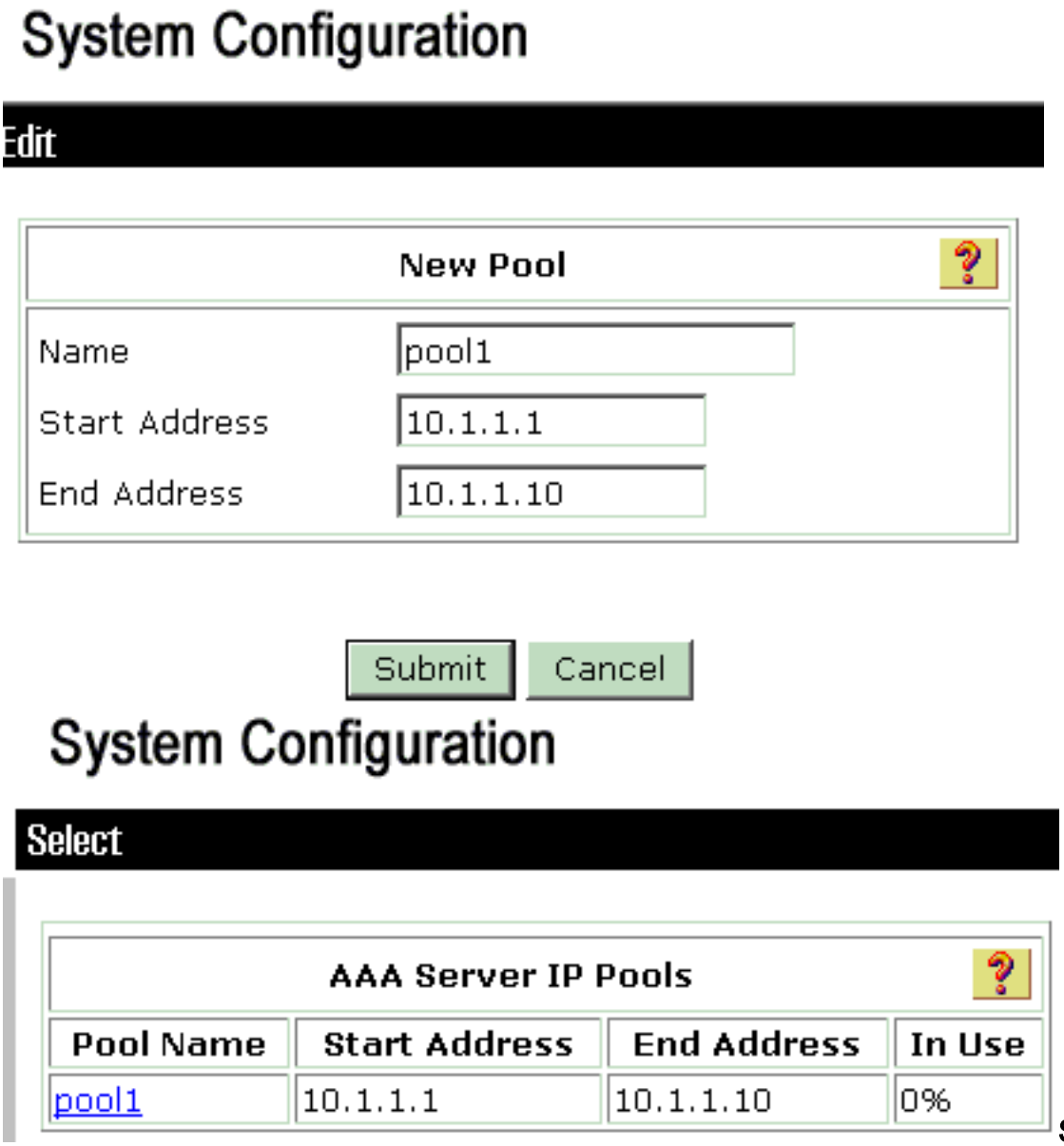
注: 技術的には、「VPN 3000 シリーズ コンセントレータの設定」の手順 3 でトンネル グループが設定されていて、VPN コンセントレータのベース グループが元のデフォルト設定から変更されていない限り、VPN 3000 RADIUS 属性を設定する必要はありません。**推奨される VPN 3000 属性：Primary-DNS**：プライマリ DNS サーバの IP アドレスを入力します。**Secondary-DNS**：セカンダリ DNS サーバの IP アドレスを入力します。**Primary-WINS**：プライマリ WINS サーバの IP アドレスを入力します。**Secondary-WINS**：セカンダリ WINS サーバの IP アドレスを入力します。**Tunneling-Protocols**：**IPsec** を選択します。 これにより、IPSec クライアント接続のみが許可されるようになります。 PPTP や L2TP は許可されません。**IPsec-Sec-Association**：**ESP-3DES-MD5** と入力します。 これにより、ご使用のすべての IPSec クライアントが最も高度な暗号を使用して接続するようになります。**IPsec-Allow-Password-Store**：**Disallow** を選択し、ユーザが VPN Client にパスワードを保存**できない**ようにします。**IPsec-Banner**：ユーザの接続時に表示されるウェルカム メッセージ バナーを入力します。 「MyCompany 従業員用 VPN アクセスへようこそ」などのメッセージを入力します。**IPsec-Default Domain**：会社のドメイン名を入力します。 「mycompany.com」のようにします。この属性セットは、必須ではありません。 ただし、

VPN 3000 コンセントレータのベース グループ属性が変更されているかどうかわからない場合は、これらの属性を設定することを推奨いたします。**Simultaneous-Logins**：ユーザが同じユーザ名で同時にログインできる数を入力します。 推奨値は 1 または 2 です。**SEP-Card-Assignment**：**Any-SEP** を選択します。**IPsec-Mode-Config**：**ON** を選択します。**IPsec over UDP**：IPSec over UDP プロトコルを使用してこのグループのユーザを接続させる場合を除き、**OFF** を選択します。 ON を選択した場合でも、VPN Client は IPSec over UDP をローカルでディセーブルにし、通常どおり接続することができます。4001 ～ 49151 の範囲の UDP ポート番号 **IPSec over UDP ポート選択**。 これは IPSec over UDP がオンになっているときだけ使用されます。次の属性セットを使用できるようにするためには、VPN コンセントレータで何らかの設定が必要になります。 これは上級ユーザのみに推奨します。**Access-Hours**：この属性を使用するためには、VPN 3000 コンセントレータで **Configuration > Policy Management** の順に選択し、アクセス時間の範囲を設定する必要があります。 あるいは、Cisco Secure ACS for Windows で設定可能なアクセス時間を使用してこの属性を管理してください。**IPsec-Split-Tunnel-List**：この属性を使用するためには、VPN コンセントレータで **Configuration > Policy Management > Traffic Management** の順に選択し、ネットワーク リストを設定してください。 ネットワーク リストとは、クライアントに対して送信されたネットワークのリストであり、リスト内のネットワークへのデータのみを暗号化するようにクライアントに対して指示します。**IP assignment in Group setup** を選択して **Assigned from AAA server Pool** にチェックマークを入れ、VPN Client ユーザの認証後にこれらのユーザに IP アドレスが割り当てられるようにします。



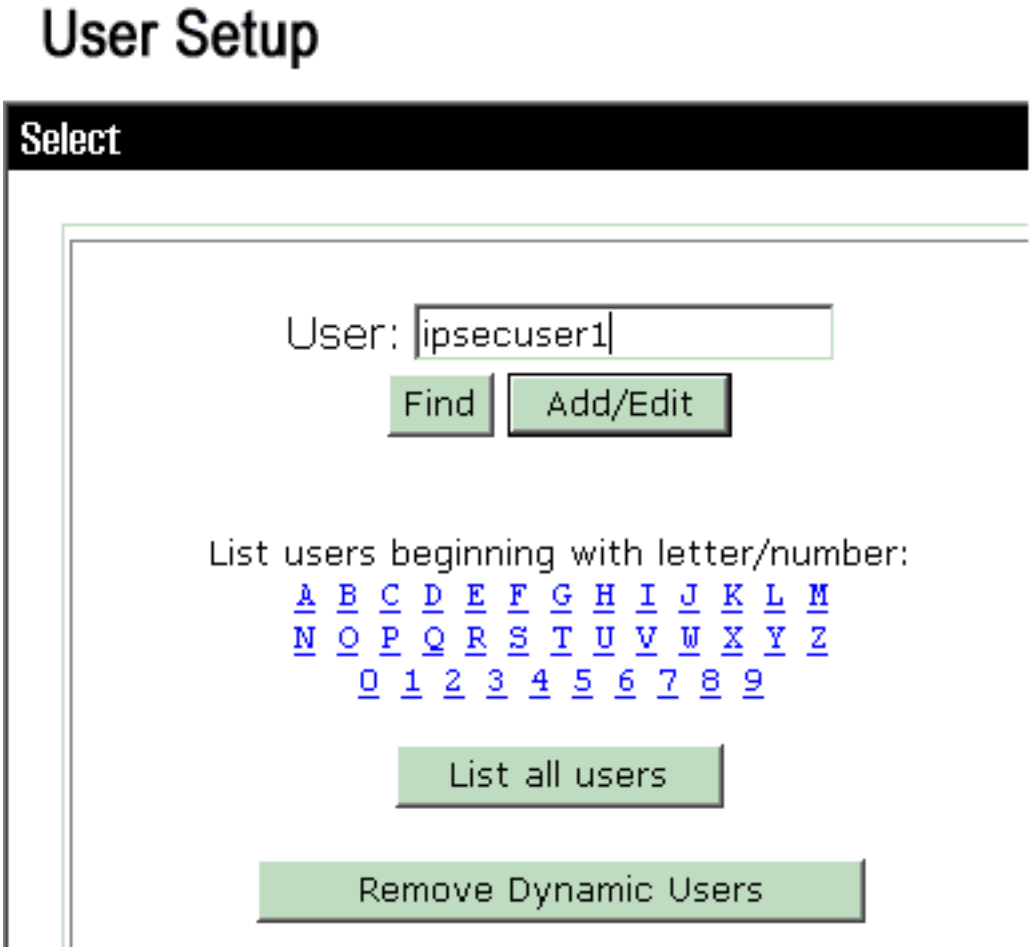
System configuration > IP pools の順に選択して VPN Client ユーザ用の IP プールを作成し、**Submit**

をクリックします。

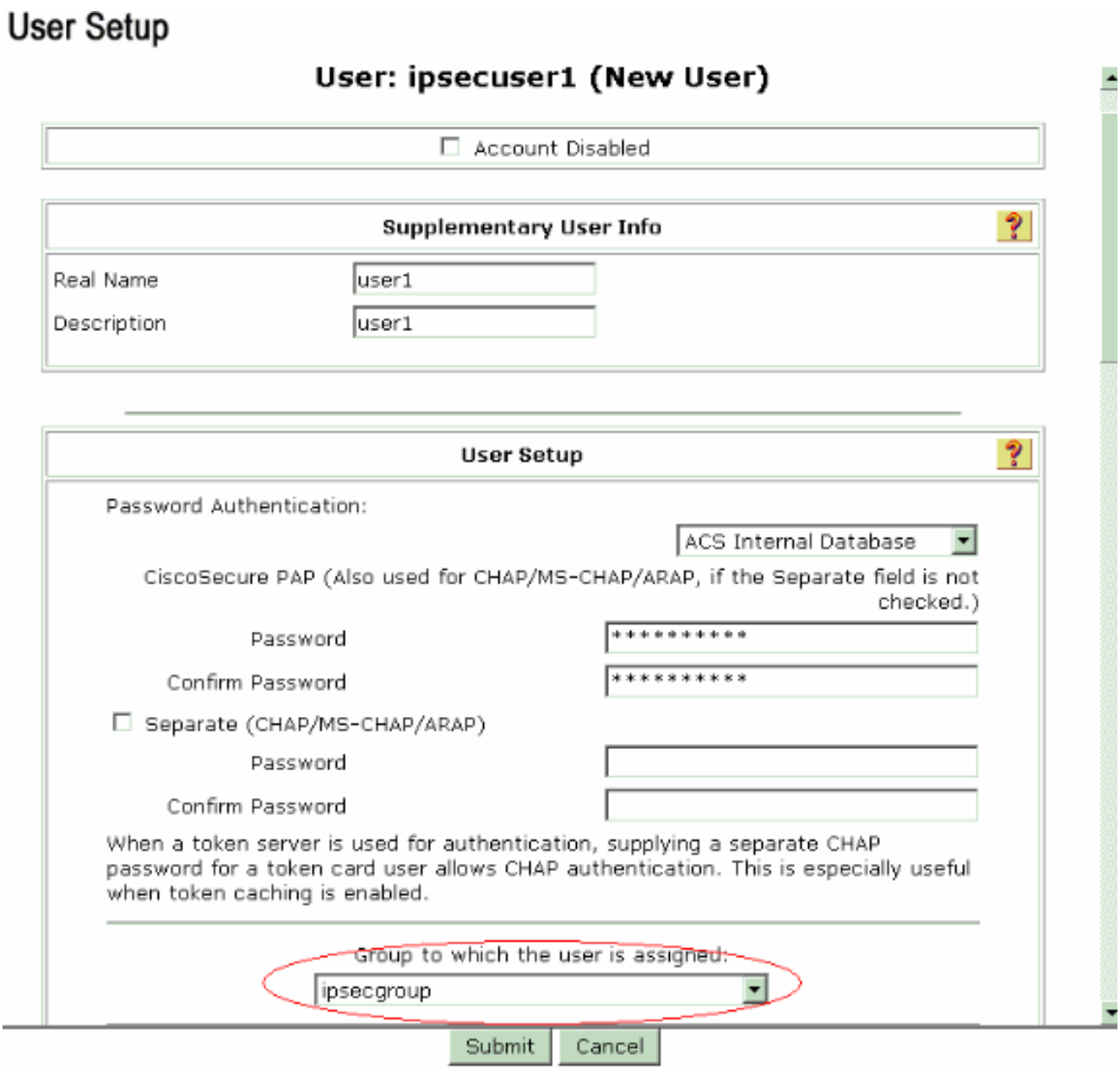


Submit > Restart を選択し、設定を保存して新しいグループをアクティブにします。グループを追加するには、これらの手順を繰り返します。

3. **Cisco Secure ACS for Windows でユーザを設定します。**[User Setup] を選択し、ユーザ名を入力して、[Add/Edit] をクリックします。



ユーザ設定のセクションでこれらのパラメータを設定します。

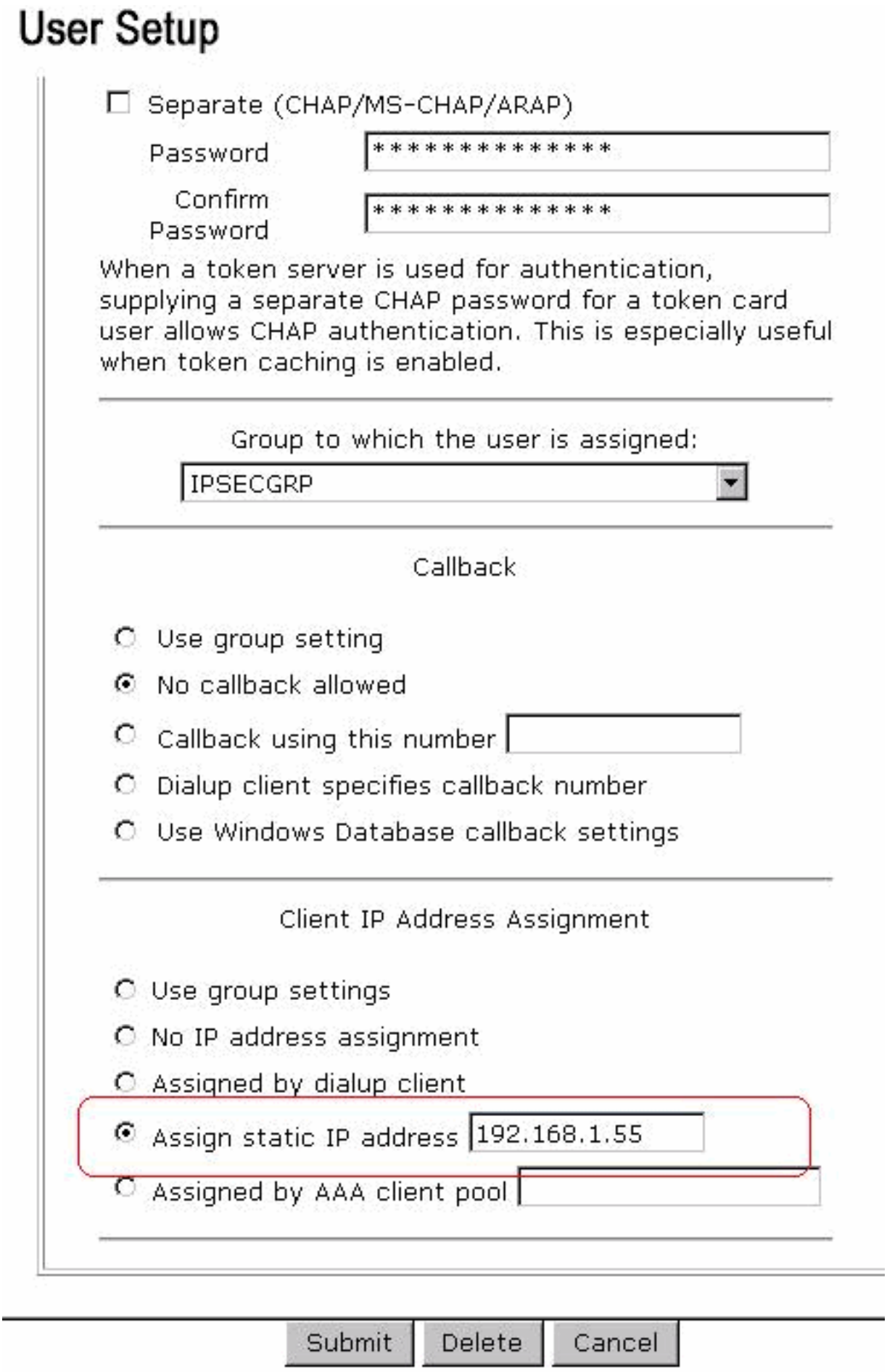


Password Authentication：**ACS Internal Database** を選択します。**Cisco Secure PAP - Password**：ユーザのパスワードを入力します。**Cisco Secure PAP - Confirm Password**：新規ユーザのパスワードを再入力します。**Group to which the user is assigned**：前のステップで作成したグループの名前を選択します。[Submit] をクリックし、ユーザ設定を保存してアクティブにします。ユーザを追加するには、これらの手順を繰り返します。

VPN Client ユーザへの固定 IP アドレスの割り当て

次の手順を実行します。

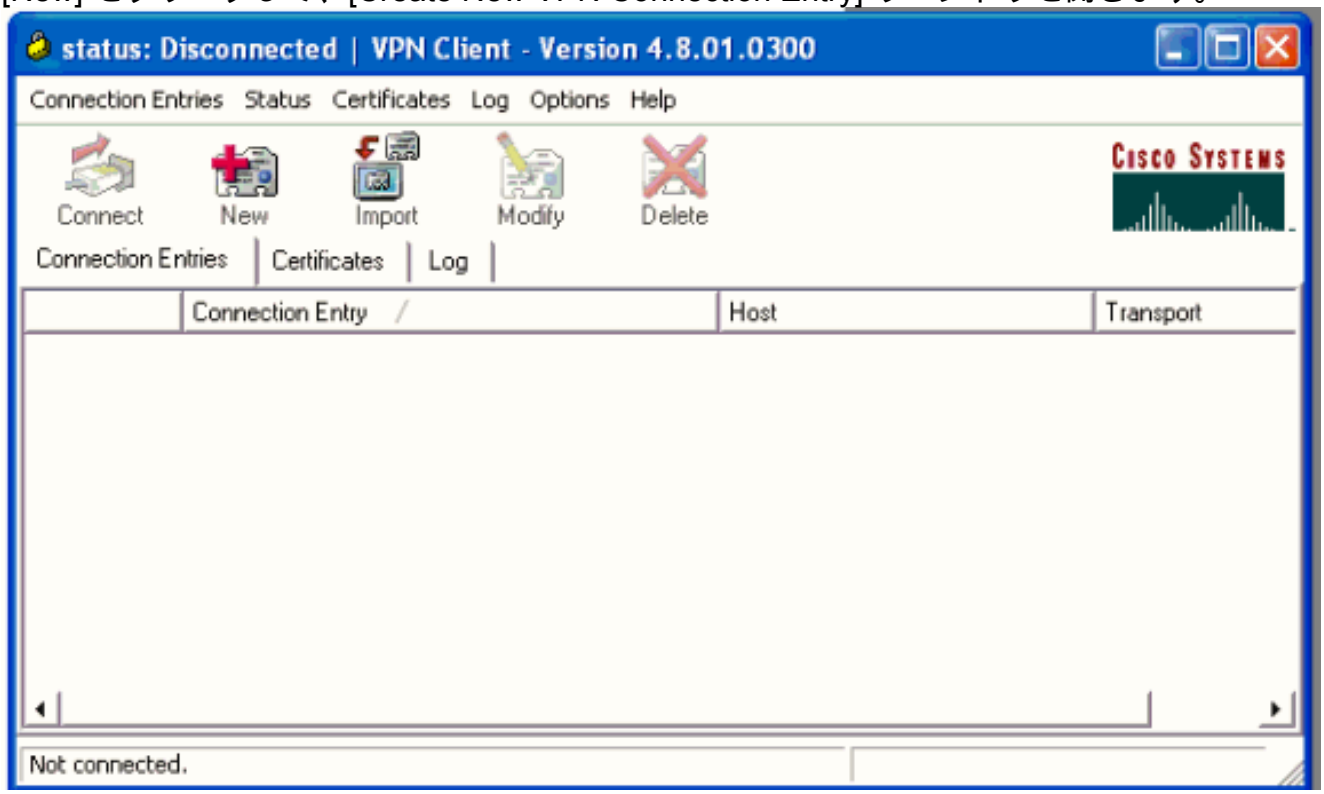
1. 「IPSECGRP」という名前で新しい VPN グループを作成します。
2. 固定 IP アドレスの受信を要求するユーザを作成し、**IPSECGRP** を選択します。 Client IP Address Assignment で割り当てた固定 IP アドレスを記入し、[Assign static IP address] を選択します。



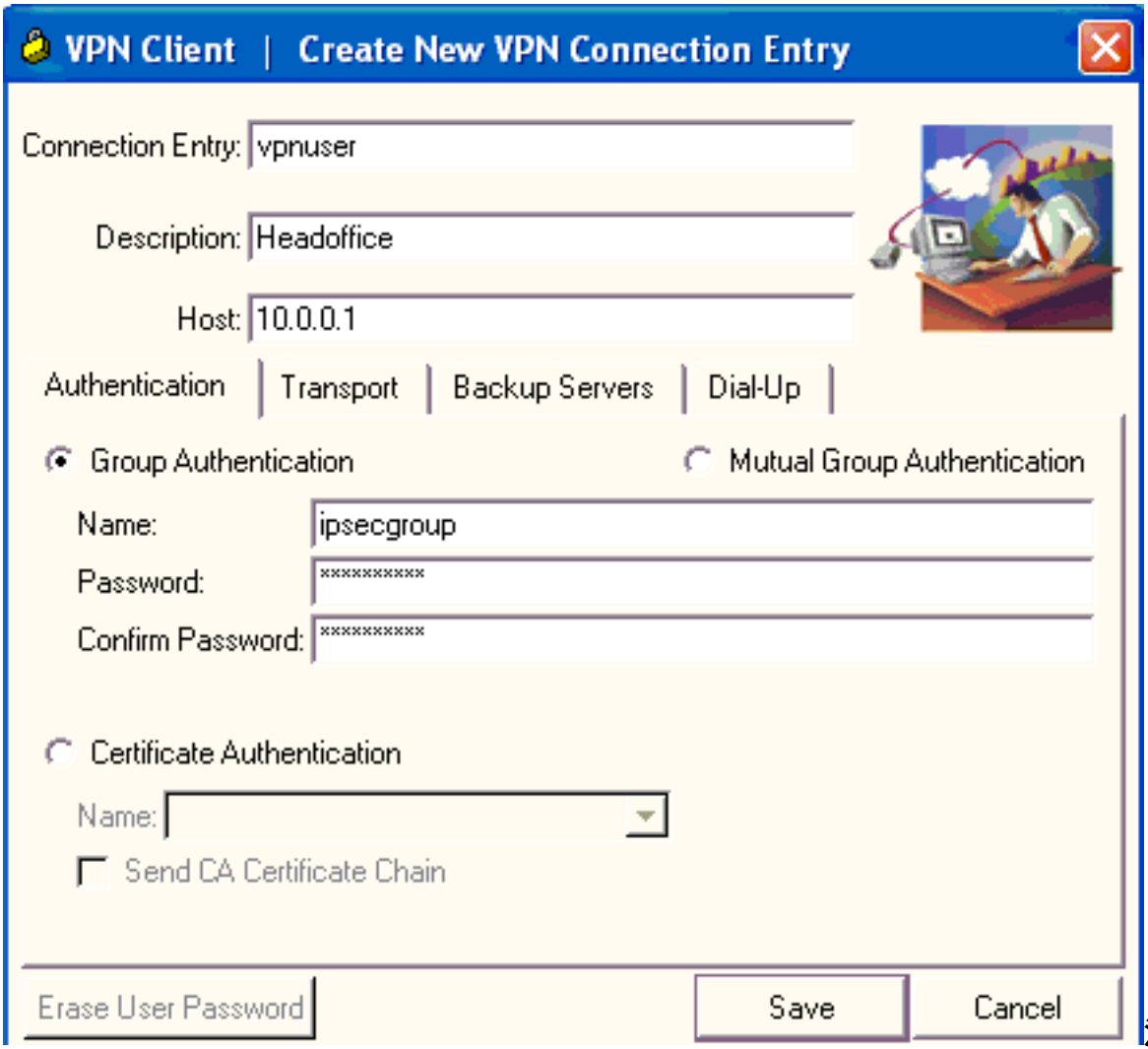
[VPN Client の設定]

このセクションでは、VPN Client 側の設定について説明しています。

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. プロンプトが表示されたら、エントリに名前を割り当てます。 必要であれば説明も入力できます。 VPN 3000 コンセントレータのパブリック インターフェイス IP アドレスを Host カラムに指定し、**Group Authentication** を選択します。 次に、グループ名とパスワードを入力します。 **Save** をクリックして、新しい VPN 接続エントリを作成します。

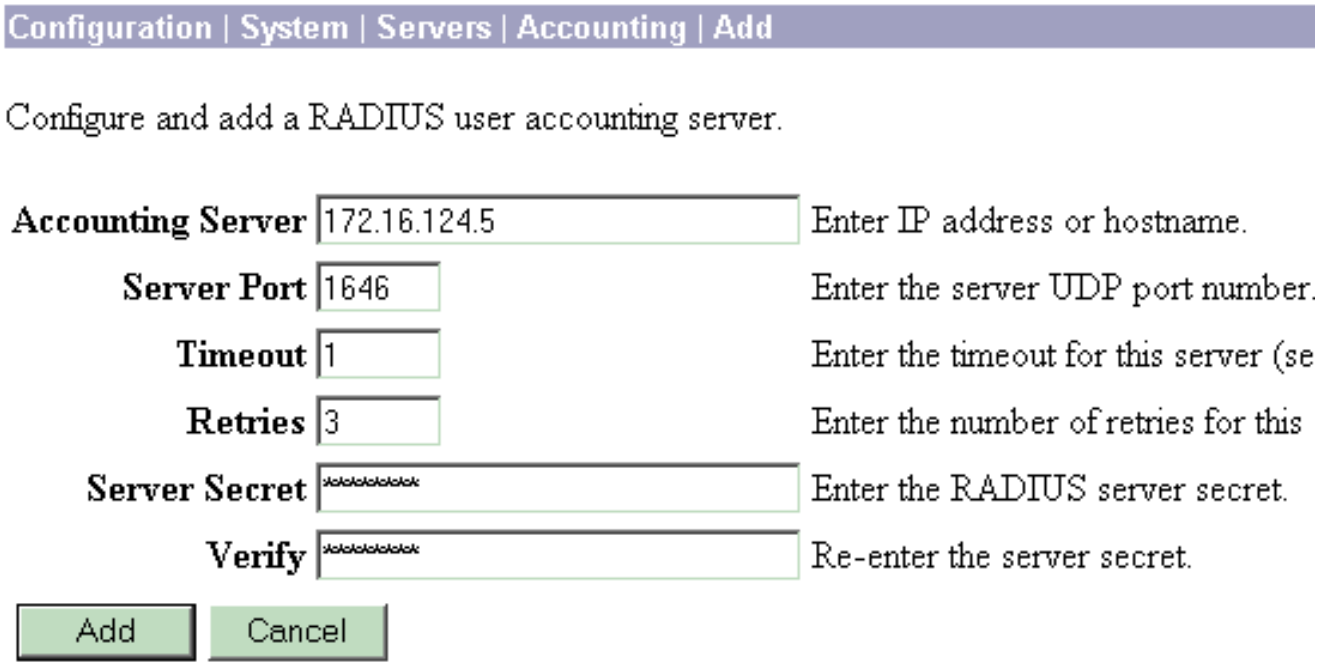


注: Cisco VPN 3000　VPN Client

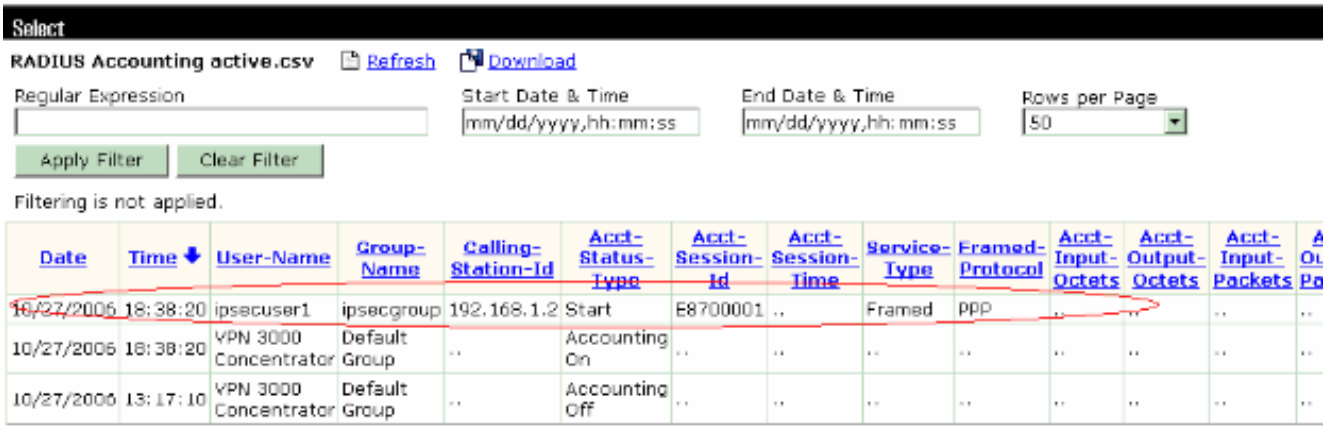
アカウンティングの追加

認証が機能するようになると、アカウンティングを追加できます。

1. VPN 3000 で、**Configuration > System > Servers > Accounting Servers** の順に選択し、**Cisco Secure ACS for Windows** サーバを追加します。
2. Configuration > User Management > Groups の順に選択 し、グループを強調表示し、**Acct を**『Modify』 をクリック するとき各グループに個々のアカウンティング サーバを追加できます。 **サーバ。** 次に、アカウンティング サーバの IP アドレスとサーバ シークレットを入力します。



Cisco Secure ACS for Windows で、アカウンティング記録は次の出力のように表示されます。



確認

このセクションでは、設定が正常に機能していることを確認します。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

VPN コンセントレータの確認

VPN 3000 コンセントレータ側で **Administration > Administer Sessions** の順に選択し、リモート VPN トンネルの確立を確認します。

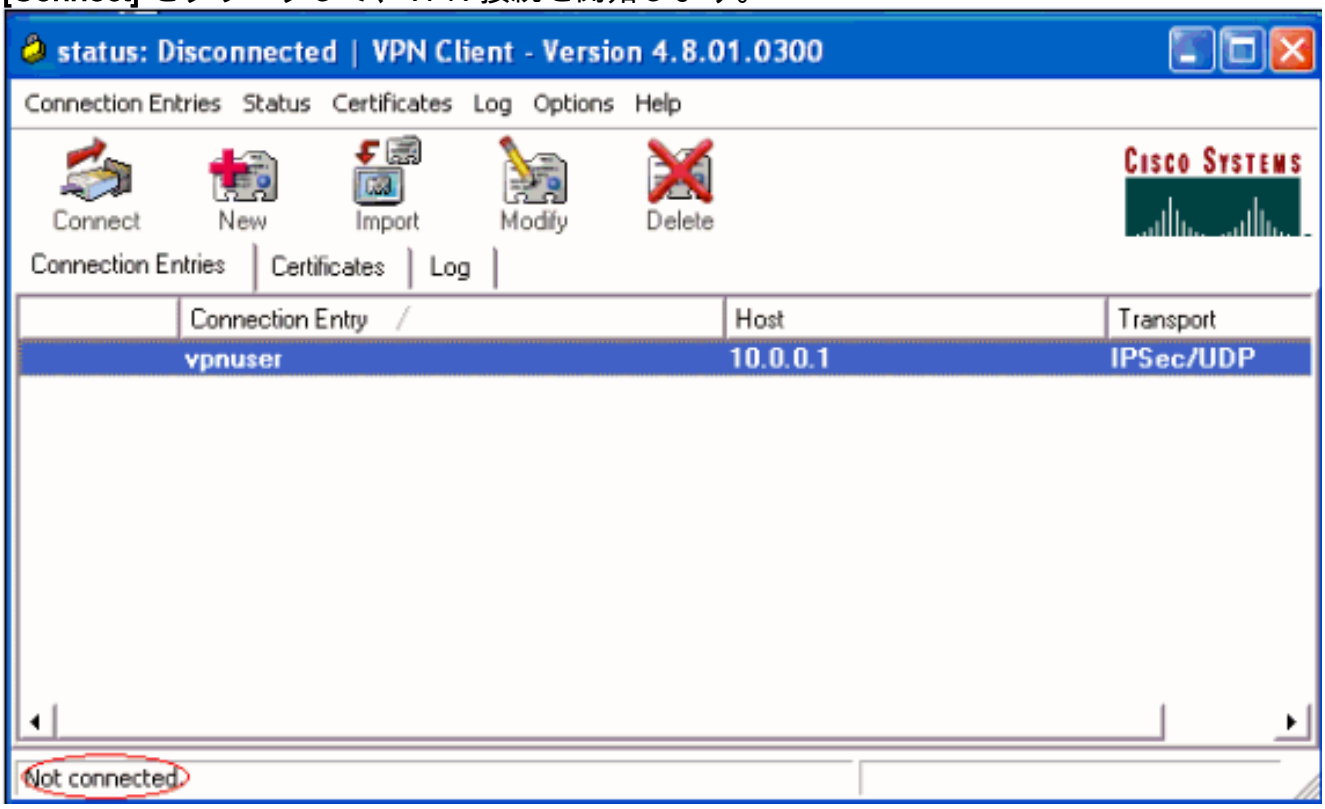
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

Username	Assigned IP Address Public IP Address	Group	Protocol Encryption	Login Time Duration	Client Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token	Actions
ipsecuser1	10.1.1.9 192.168.1.2	ipsecgroup	IPSec 3DES-168	Oct 27 17:22:14 0:05:11	WinNT 4.8.01.0300	0 8056	N/A	[Logout	Ping]

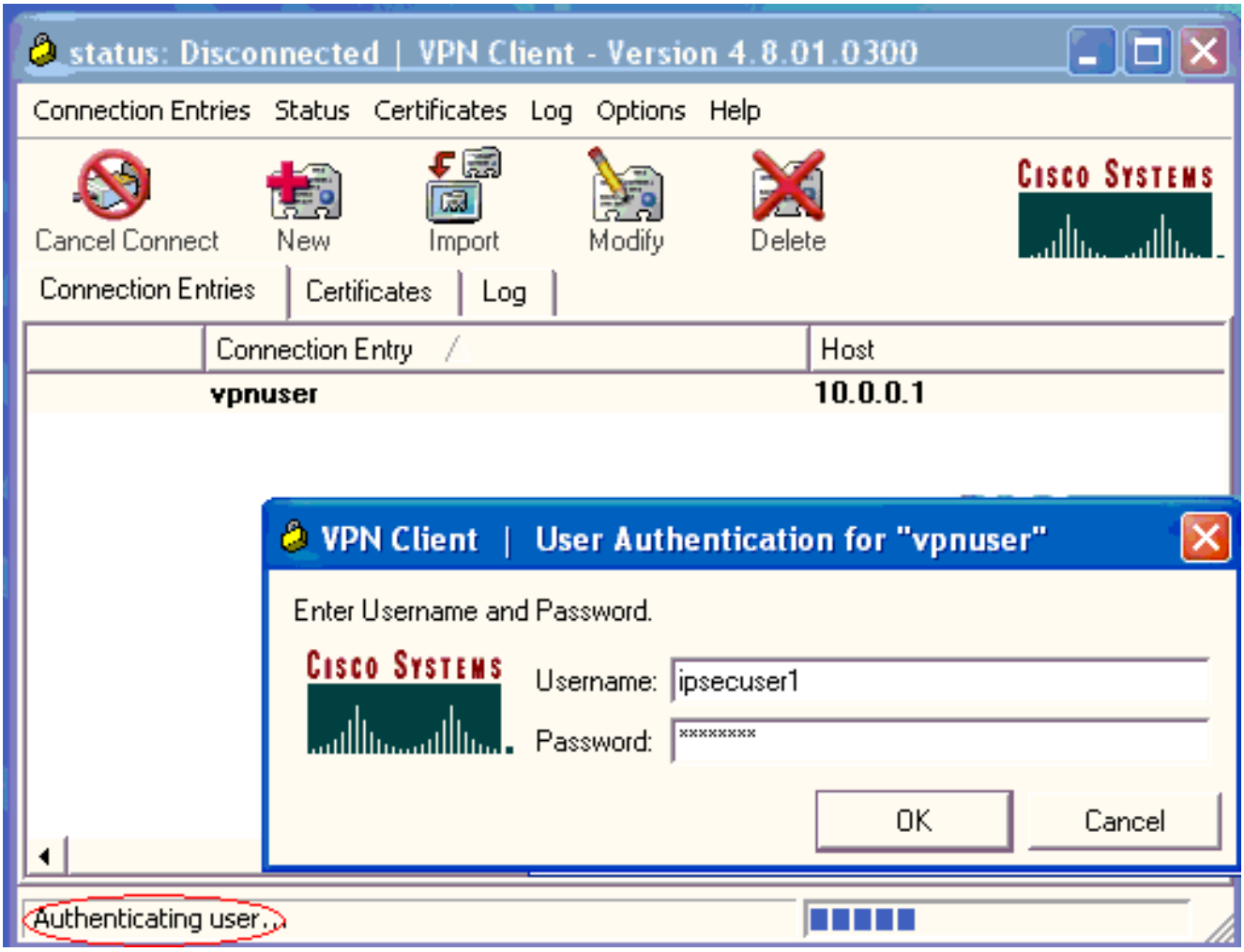
VPN Client の確認

VPN Client を確認するには、次のステップを実行します。

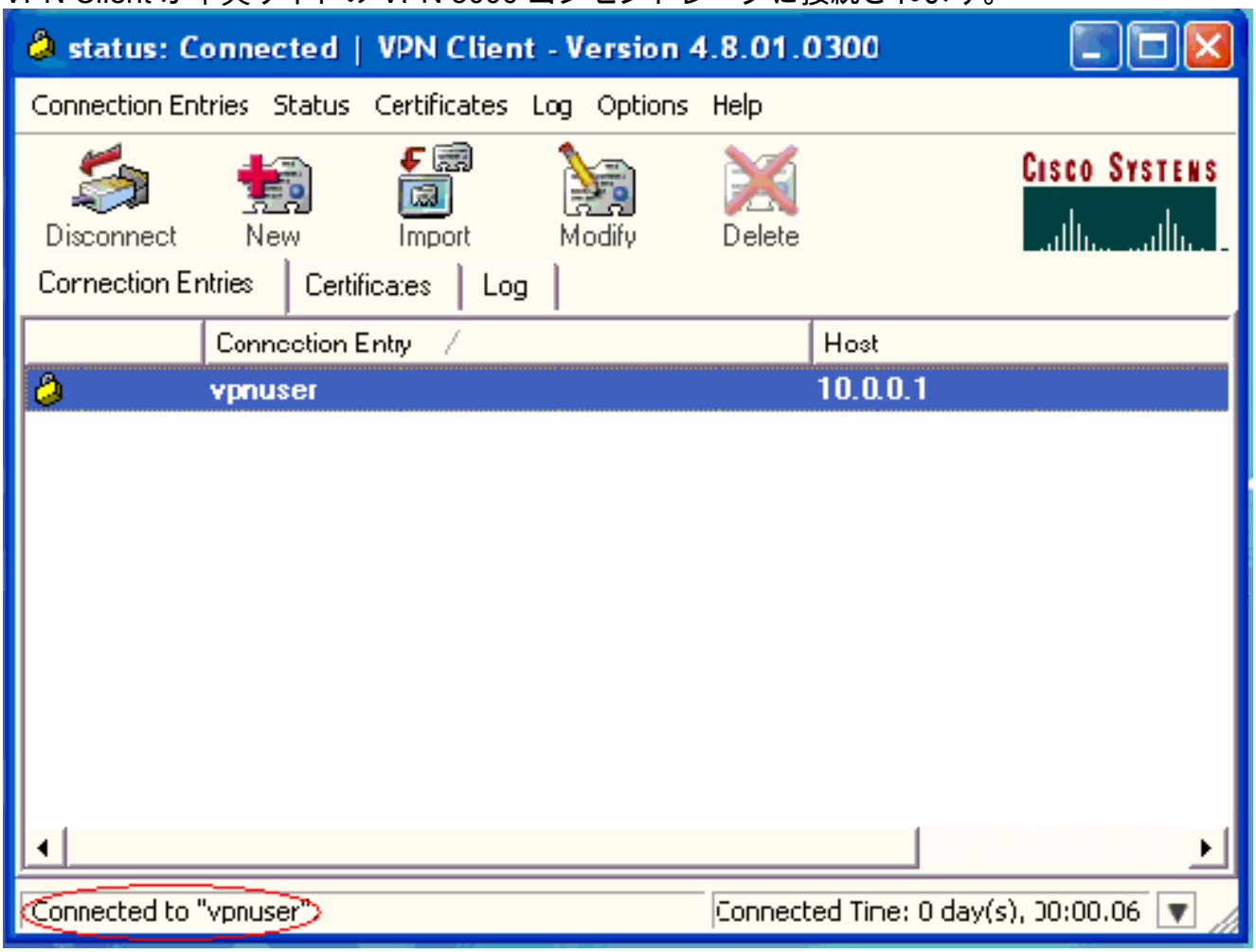
1. **[Connect]** をクリックして、VPN 接続を開始します。



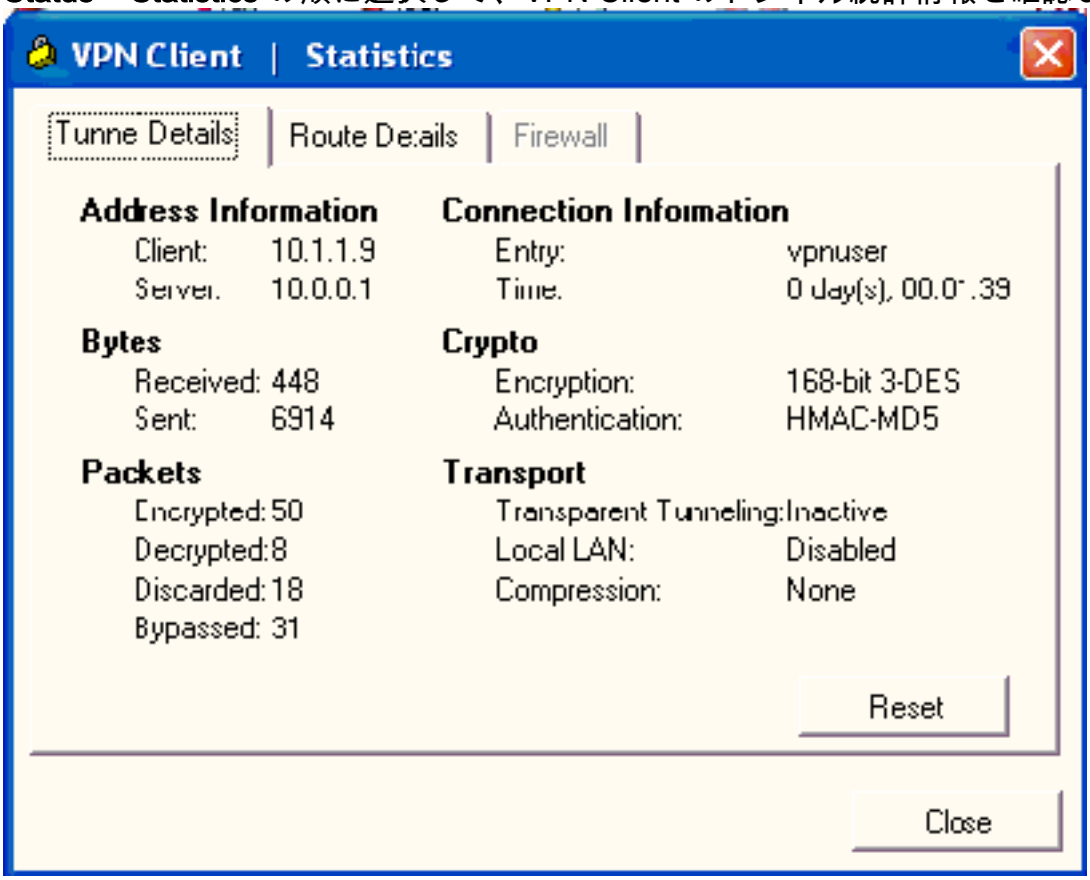
2. ユーザ認証用の次のウィンドウが表示されます。 有効なユーザ名とパスワードを入力して、VPN 接続を確立します。



3. VPN Client が中央サイトの VPN 3000 コンセントレータに接続されます。



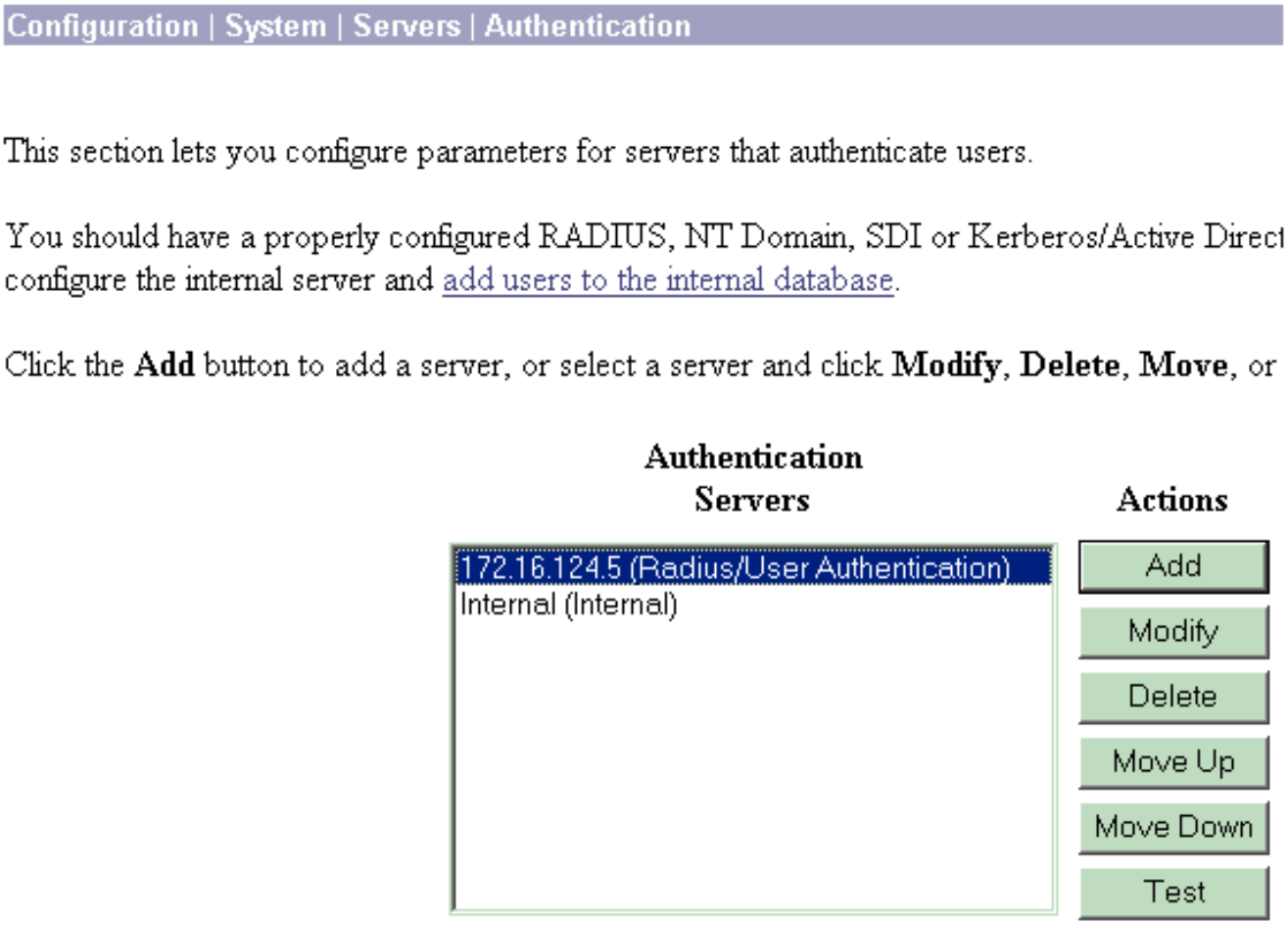
4. **Status > Statistics** の順に選択して、VPN Client のトンネル統計情報を確認します。



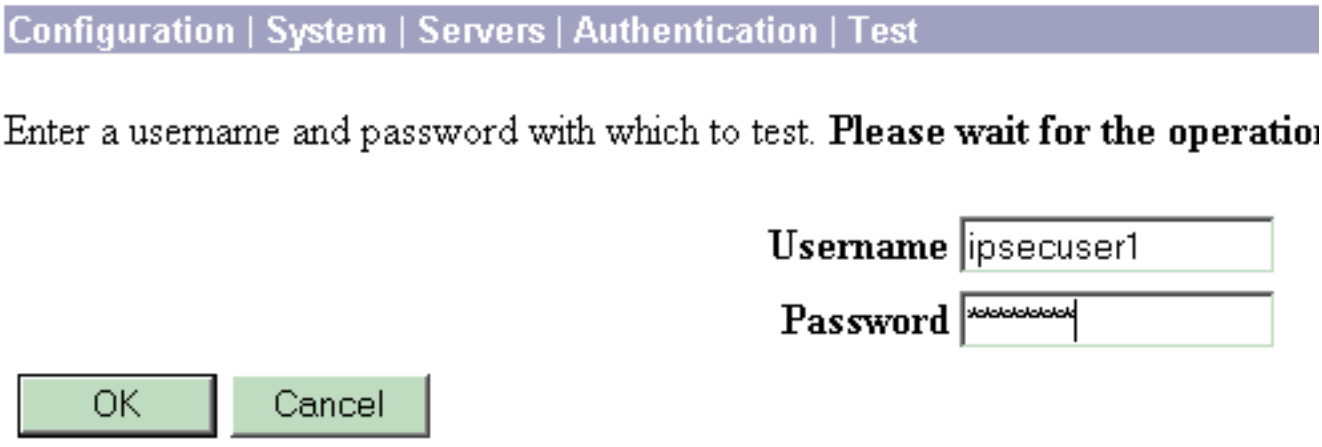
トラブルシューティング

次の手順に従って、設定のトラブルシューティングを行います。

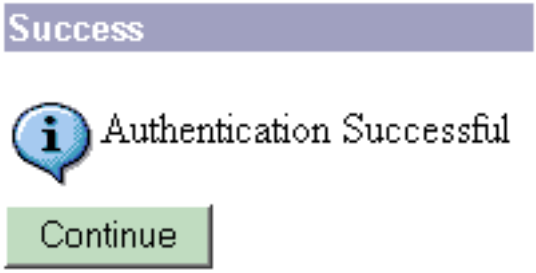
1. **Configuration > System > Servers > Authentication** の順に選択し、次の手順を実行して、RADIUS サーバと VPN 3000 コンセントレータの間の接続を確認します。[サーバ]を選択してから **[Test]** をクリックします。



RADIUS ユーザ名とパスワードを入力し、[OK] をクリックします。



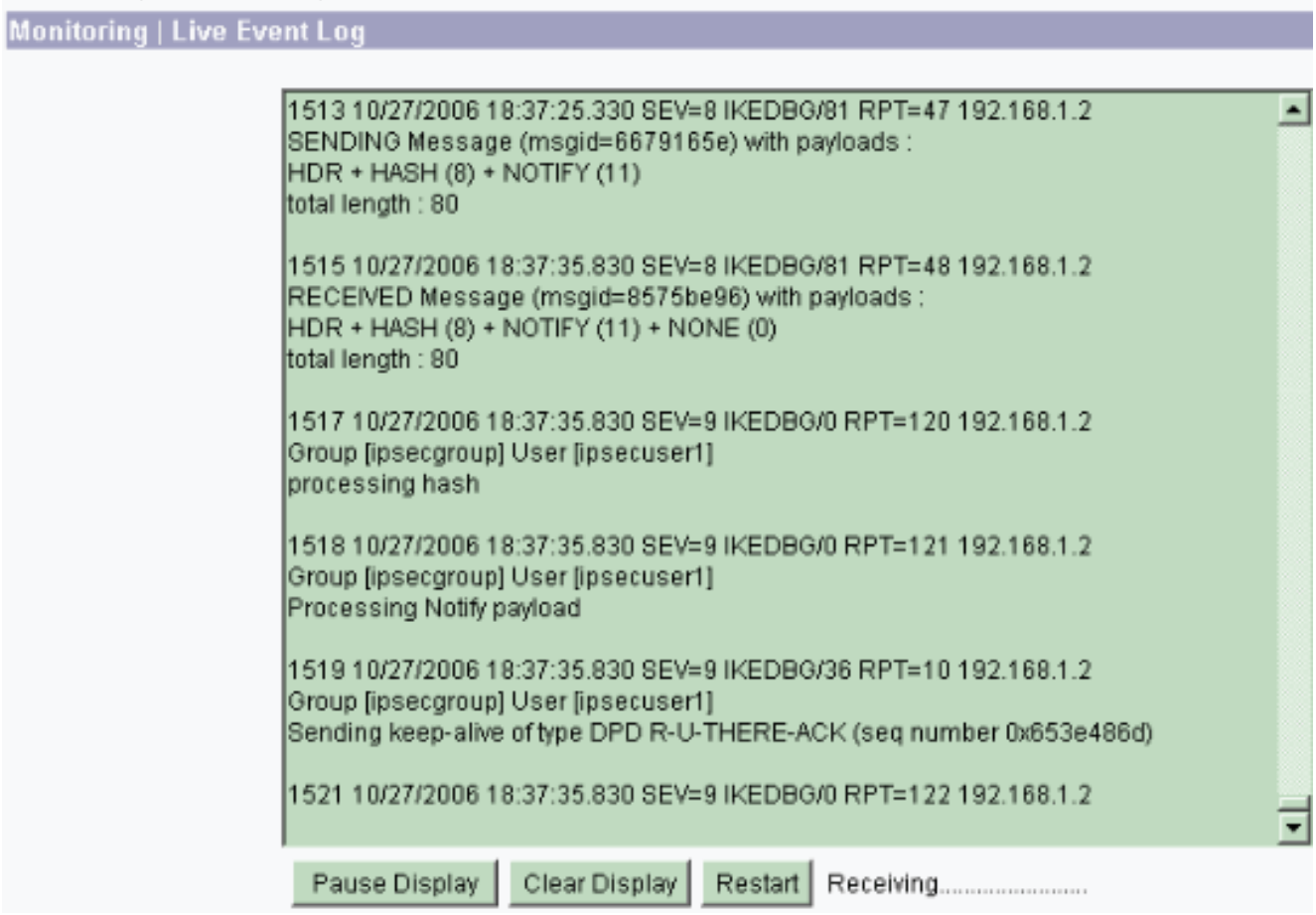
認証が成功したことを示すメッセージが表示されます。



2. 認証が失敗した場合は、設定に問題があるか、IP 接続に問題があります。 ACS サーバの Failed Attempts Log で、この失敗に関連するメッセージがないか確認します。このログにメッセージが表示されない場合は、IP 接続に問題があると考えられます。 RADIUS 要求が RADIUS サーバに到達していません。 RADIUS（1645）パケットの発着を許可する VPN 3000 コンセントレータ インターフェイスに適用されているフィルタを確認してください。

テスト認証が成功しても VPN 3000 コンセントレータへのログインが引き続き失敗する場合は、コンソール ポート経由で Filterable Event Log を確認してください。接続が機能しない場合、AUTH、IKE、および IPsec というイベント クラスを VPN コンセントレータに追加できます。これには、**Configuration > System > Events > Classes > Modify (Severity to Log=1-9, Severity to Console=1-3)** の順に選択します。 AUTHDBG、AUTHDECODE、IKEDBG、IKEDECODE、IPSECDBG、および IPSECDECODE も使用できますが、これらは情報が多すぎます。 RADIUS サーバから受け渡される属性について詳しい情報が必要な場合は、AUTHDECODE、IKEDECODE、および IPSECDECODE を使用すると、Severity to Log=1-13 レベルの情報を入手できます。

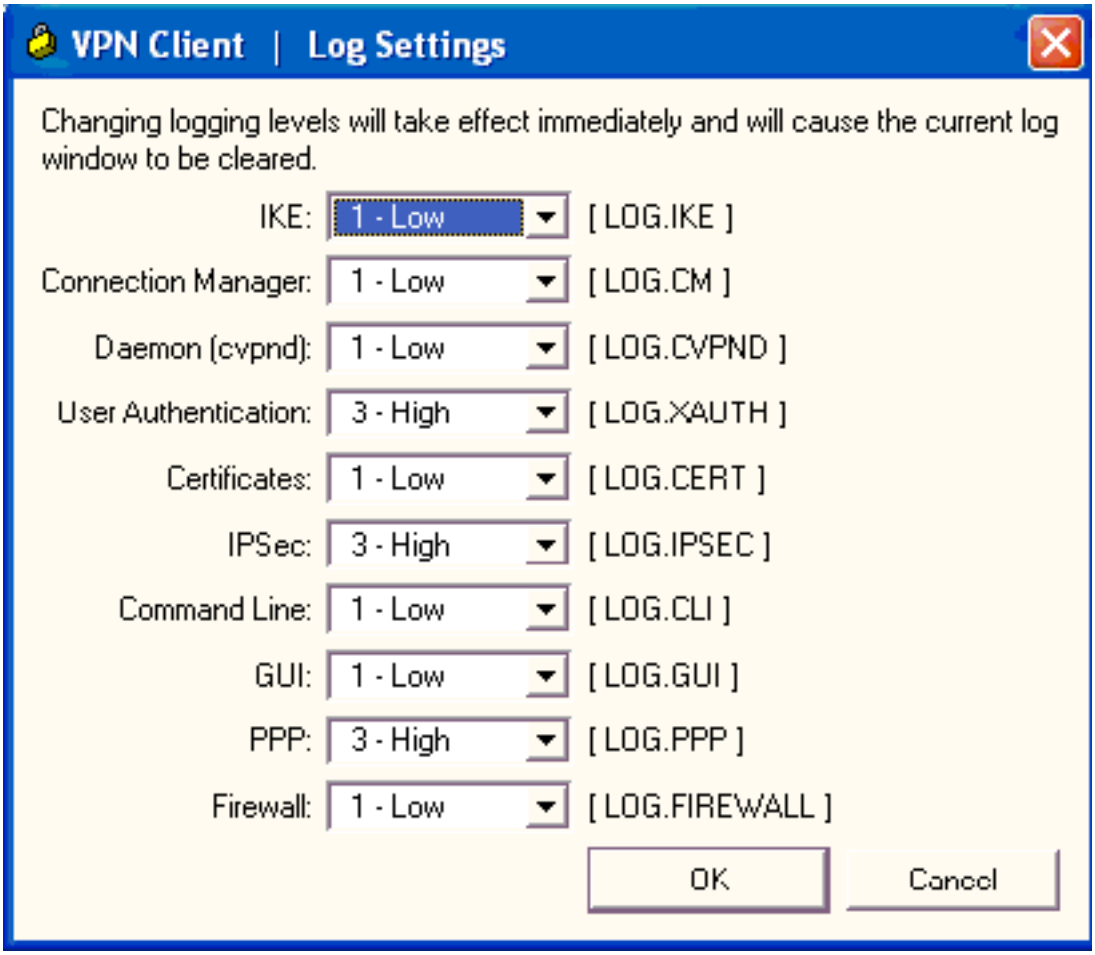
3. **Monitoring > Event Log** でイベント ログを取得します。



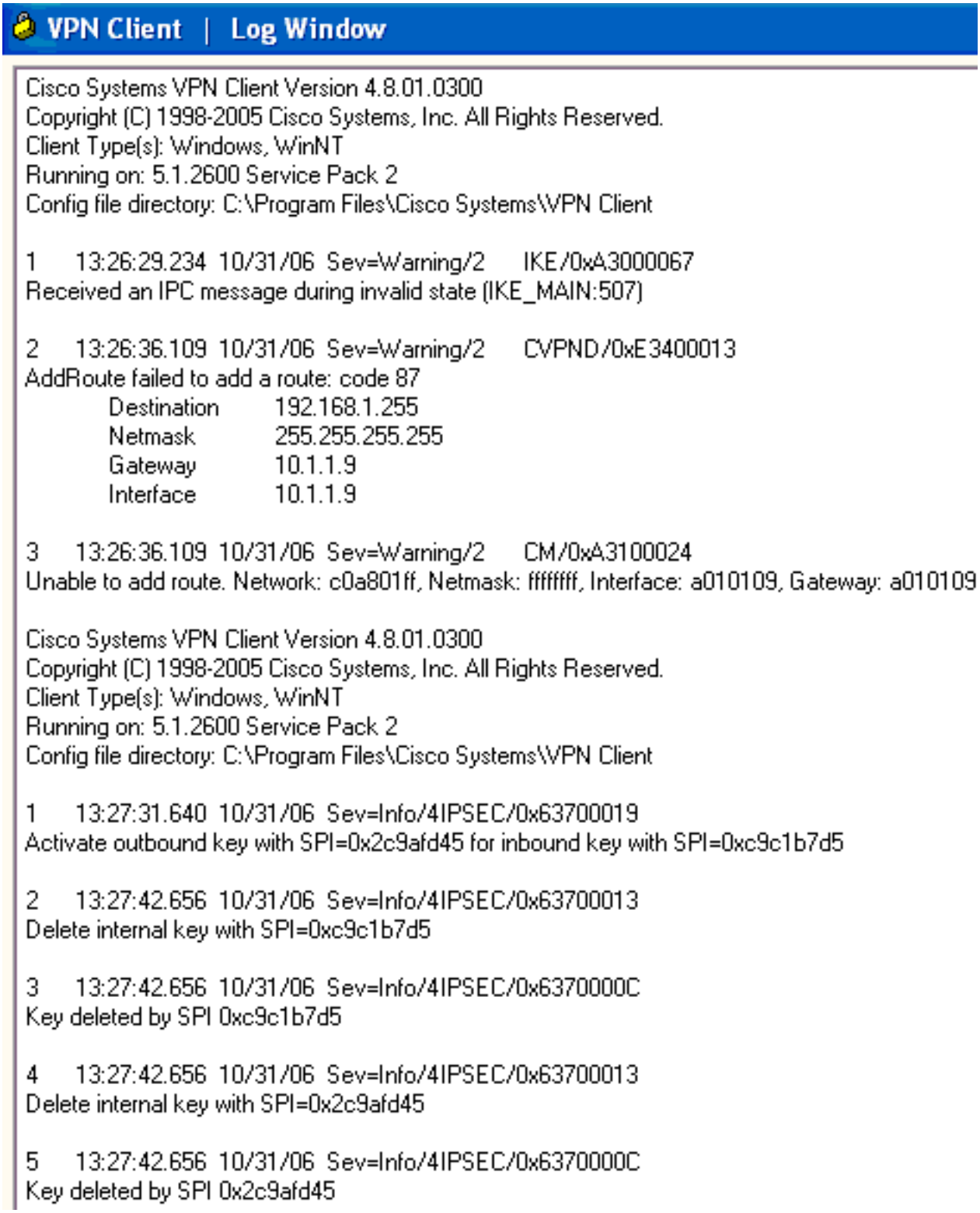
VPN Client 4.8 for Windows のトラブルシューティング

VPN Client 4.8 for Windows のトラブルシューティングを行うには、次のステップを実行します。

1. **Log > Log settings** の順に選択して、VPN Client でログ レベルを有効にします。



2. VPN Client でログ エントリを表示するには、**Log > Log Window** の順に選択します。



関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN Client に関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコル
- Cisco Secure ACS for Windows に関するサポート ページ
- RADIUS 設定
- テクニカルサポートとドキュメント - Cisco Systems