IPsec zwischen einem VPN 300-Concentrator und einem VPN-Client 4.x für Windows mit RADIUS für die Konfiguration der Benutzerauthentifizierung und -abrechnung (Beispiel)

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie ein IPsec-Tunnel zwischen einem Cisco VPN 3000-Konzentrator und einem Cisco VPN Client 4.x für Microsoft Windows erstellt wird, der RADIUS für die Benutzerauthentifizierung und -abrechnung verwendet. In diesem Dokument wird der Cisco Secure Access Control Server (ACS) für Windows empfohlen, um die RADIUS-Konfiguration zu vereinfachen und Benutzer zu authentifizieren, die eine Verbindung zu einem VPN 3000-Konzentrator herstellen. Eine Gruppe auf einem VPN 300-Konzentrator ist eine Gruppe von Benutzern, die als eine Einheit behandelt werden. Die Konfiguration von Gruppen kann im Gegensatz zu einzelnen Benutzern die Systemverwaltung vereinfachen und Konfigurationsaufgaben optimieren.

Weitere Informationen finden Sie unter PIX/ASA 7.x und Cisco VPN Client 4.x für Windows mit Microsoft Windows 2003 IAS RADIUS Authentication Configuration Example zum Einrichten der Remotezugriff-VPN-Verbindung zwischen einem Cisco VPN Client (4.x für Windows) und der PIX 500 Security Appliance 7.x, die einen Microsoft Windows 2003 Internet Authentication Service (RADIIAS) verwendet. US-Server.

Unter Konfigurieren von IPsec zwischen einem Cisco IOS-Router und einem Cisco VPN-Client 4.x für Windows mithilfe von RADIUS für die Benutzerauthentifizierung finden Sie Informationen zum Konfigurieren einer Verbindung zwischen einem Router und dem Cisco VPN Client 4.x, der RADIUS für die Benutzerauthentifizierung verwendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Secure ACS für Windows RADIUS ist installiert und funktioniert ordnungsgemäß mit anderen Geräten.
- Der Cisco VPN 3000 Concentrator wird konfiguriert und kann über die HTML-Schnittstelle verwaltet werden.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS für Windows mit Version 4.0
- Cisco VPN Concentrator der Serie 3000 mit Bilddatei 4.7.2.B
- Cisco VPN-Client 4.x

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

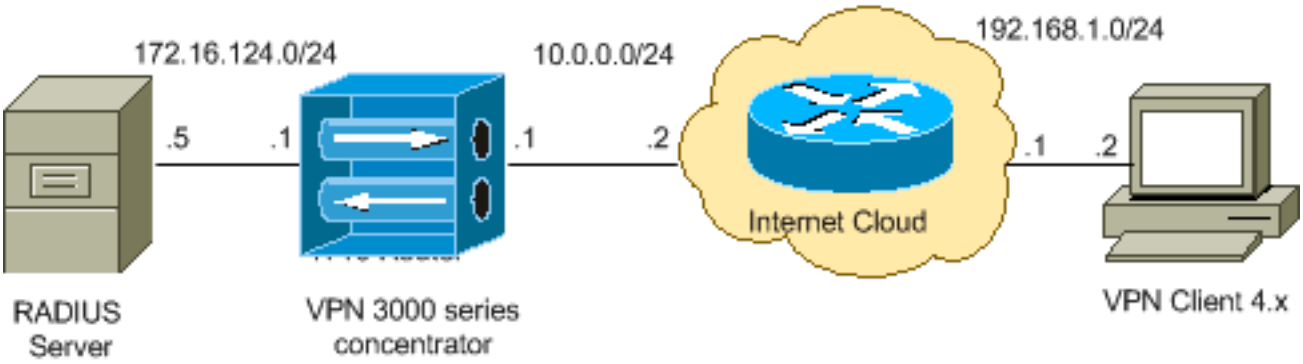
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

Benutzergruppen im VPN 300-Konzentrator

Gruppen können sowohl für Cisco Secure ACS für Windows als auch für den VPN 3000-Konzentrator definiert werden, verwenden jedoch Gruppen auf etwas andere Weise. Führen Sie diese Aufgaben aus, um die Dinge zu vereinfachen:

- **Konfigurieren Sie eine Gruppe im VPN 300-Concentrator** für den ersten Tunnel. Dies wird häufig als "Tunnel Group" (Tunnelgruppe) bezeichnet und dient zum Einrichten einer verschlüsselten Internet Key Exchange (IKE)-Sitzung mit dem VPN 3000 Concentrator mithilfe eines vorinstallierten Schlüssels (dem Gruppenkennwort). Dabei handelt es sich um denselben Gruppennamen und dasselbe Kennwort, die für alle Cisco VPN-Clients konfiguriert werden sollten, die eine Verbindung zum VPN Concentrator herstellen möchten.
- **Konfigurieren Sie Gruppen auf dem Cisco Secure ACS für Windows-Server**, die standardmäßige RADIUS-Attribute und VSAs (Vendor Specific Attributes) für die Richtlinienverwaltung verwenden. Bei den VSAs, die mit dem VPN 3000 Concentrator verwendet werden sollen, handelt es sich um die RADIUS-Attribute (VPN 3000).
- **Konfigurieren Sie Benutzer auf dem Cisco Secure ACS für Windows RADIUS-Server, und weisen Sie sie einer** auf demselben Server konfigurierten **Gruppe zu**. Die Benutzer erben die für ihre Gruppe definierten Attribute, und Cisco Secure ACS für Windows sendet diese Attribute an den VPN Concentrator, wenn der Benutzer authentifiziert wird.

Verwendung von Gruppen- und Benutzerattributen im VPN 3000-Concentrator

Nachdem der VPN 300 Concentrator die Tunnelgruppe mit dem VPN Concentrator und der Benutzer mit RADIUS authentifiziert hat, muss er die erhaltenen Attribute organisieren. Der VPN Concentrator verwendet die Attribute in der angegebenen Reihenfolge, unabhängig davon, ob die Authentifizierung im VPN Concentrator oder mit RADIUS erfolgt:

1. **Benutzerattribute** - Diese Attribute haben immer Vorrang vor anderen Attributen.
2. **Tunnelgruppenattribute** - Alle Attribute, die bei der Benutzerauthentifizierung nicht zurückgegeben wurden, werden durch die Tunnelgruppenattribute ausgefüllt.
3. **Basislitribute** - Alle Attribute, die in den Attributen Benutzer oder Tunnelgruppe fehlen,

werden durch die Attribute der VPN Concentrator Base Group ausgefüllt.

Konfiguration des VPN Concentrators der Serie 3000

Führen Sie die Schritte in diesem Abschnitt aus, um einen Cisco VPN 3000-Konzentrator für die Parameter zu konfigurieren, die für die IPsec-Verbindung erforderlich sind, sowie den AAA-Client, der dem VPN-Benutzer die Authentifizierung beim RADIUS-Server ermöglicht.

In dieser Übung wird zuerst auf den VPN Concentrator über den Konsolenport zugegriffen, und es wird eine minimale Konfiguration hinzugefügt, wie die folgende Ausgabe zeigt:

```
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 -
>
```

Der VPN-Konzentrator wird in der Schnellkonfiguration angezeigt, und diese Artikel sind konfiguriert.

- Uhrzeit/Datum
- Schnittstellen/Masken in **Konfiguration > Schnittstellen** (public=10.0.0.1/24, private=172.16.124.1/24)
- Standard-Gateway in **Konfiguration > System > IP-Routing > Default_Gateway** (10.0.0.2)

Der Zugriff auf den VPN Concentrator erfolgt über HTML aus dem internen Netzwerk.

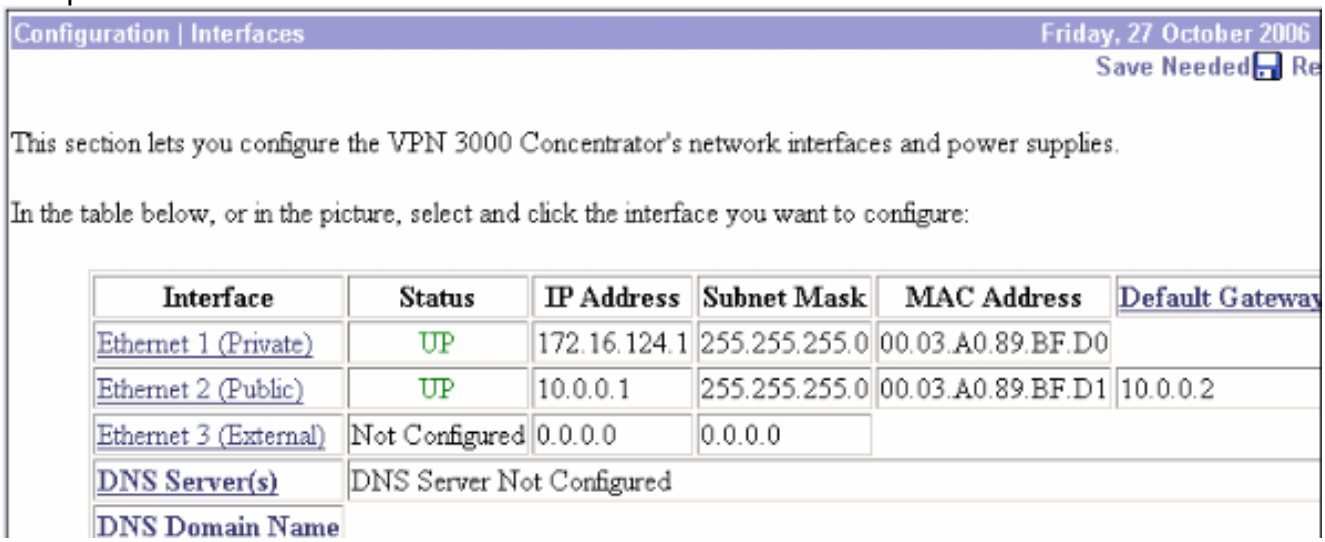
Hinweis: Wenn der VPN Concentrator von außen verwaltet wird, führen Sie auch die folgenden Schritte aus:

1. Wählen Sie **Configuration > 1-Interfaces > 2-Public > 4-Select IP Filter > 1 aus. Private (Standard)**.
2. Wählen Sie **Administration > 7-Access Rights > 2-Access Control List > 1-Add Manager Workstation**, um die IP-Adresse des externen Managers hinzuzufügen.

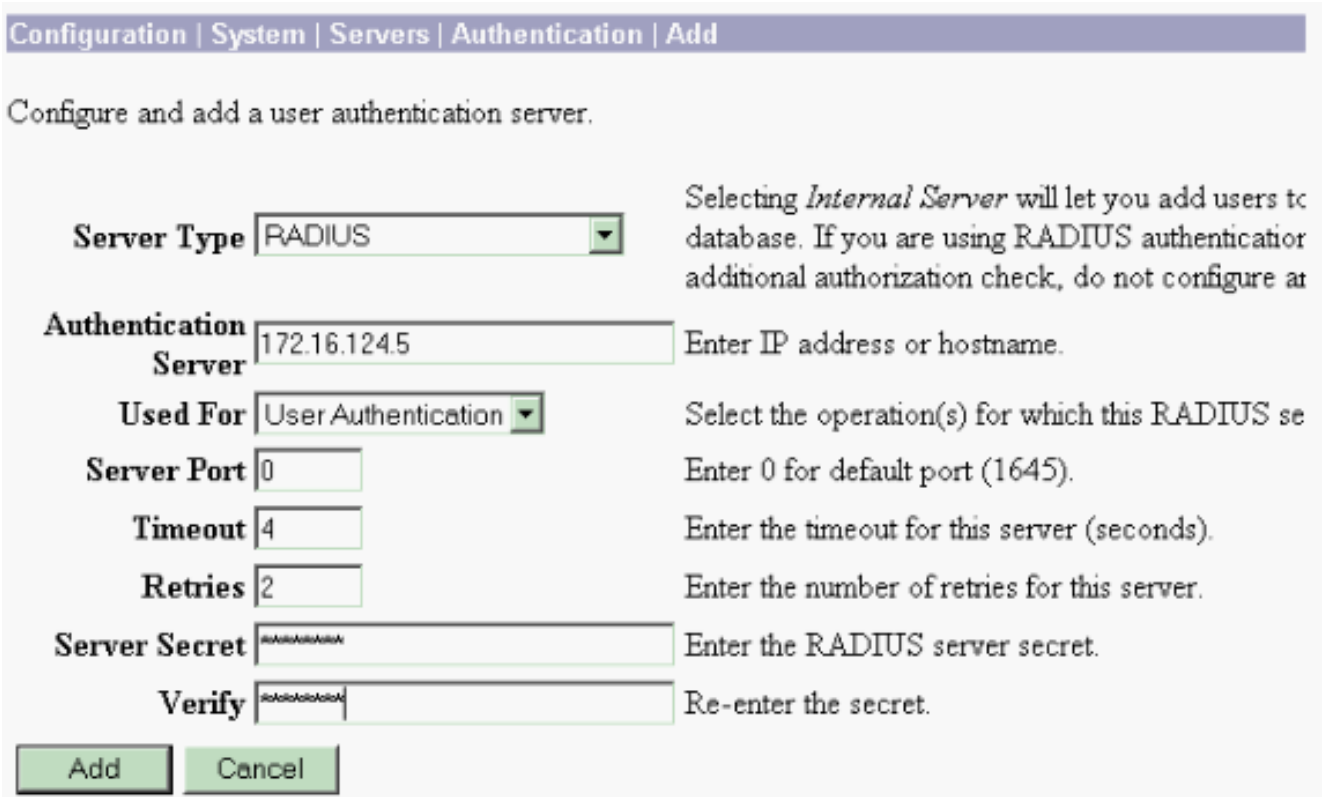
Diese Schritte sind nur erforderlich, wenn Sie den VPN Concentrator von außen verwalten.

Wenn Sie diese beiden Schritte abgeschlossen haben, können Sie die restliche Konfiguration über die Benutzeroberfläche vornehmen, indem Sie einen Webbrowser verwenden und eine Verbindung mit der IP-Adresse der soeben konfigurierten Schnittstelle herstellen. In diesem Beispiel und zu diesem Zeitpunkt ist der Zugriff auf den VPN Concentrator über HTML vom internen Netzwerk aus möglich:

1. Wählen Sie **Configuration > Interfaces (Konfiguration > Schnittstellen)** aus, um die Schnittstellen nach dem Aufrufen der Benutzeroberfläche erneut zu überprüfen.

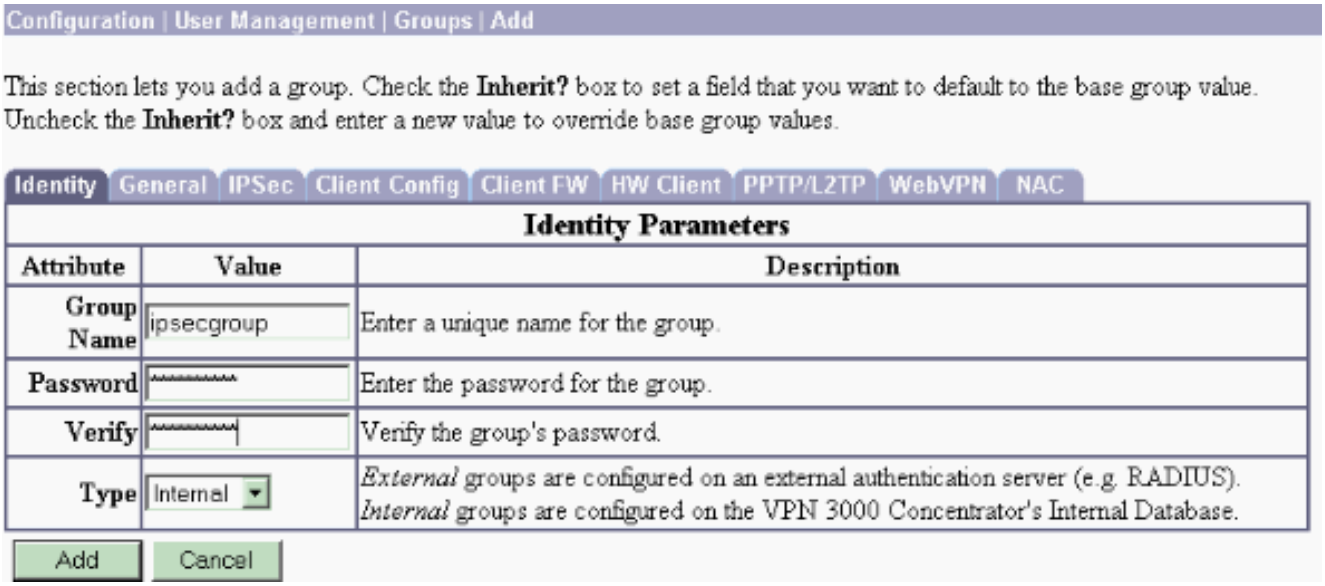


2. Führen Sie diese Schritte aus, um den Cisco Secure ACS für Windows RADIUS-Server zur Konfiguration des VPN 3000 Concentrator hinzuzufügen.Wählen Sie **Configuration > System > Servers > Authentication aus**, und klicken Sie im linken Menü auf **Add**.

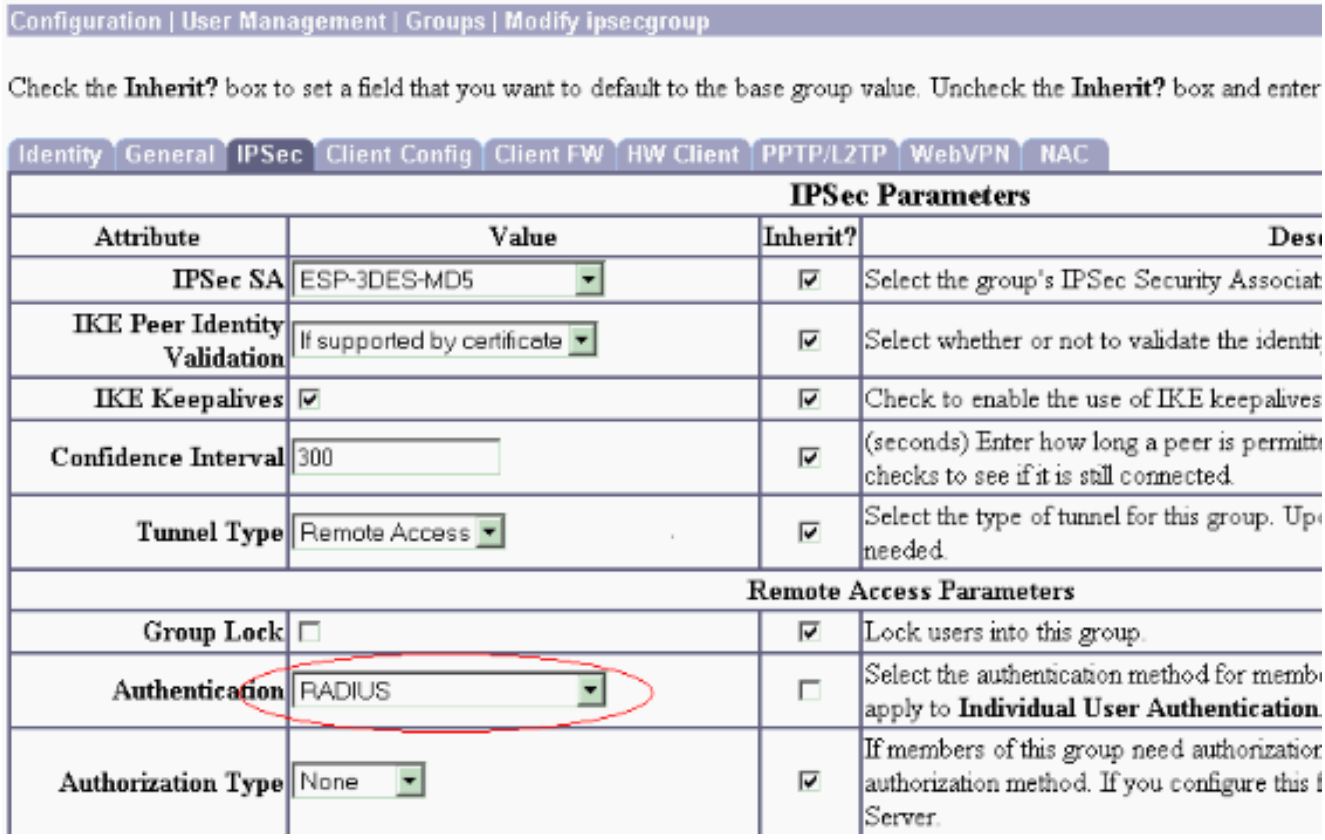


Wählen Sie den Servertyp **RADIUS** aus, und fügen Sie diese Parameter für Ihren Cisco Secure ACS für Windows RADIUS-Server hinzu. Behalten Sie alle anderen Parameter im Standardzustand bei.**Authentication Server** (Authentifizierungsserver): Geben Sie die IP-Adresse des Cisco Secure ACS für Windows RADIUS-Server ein.**Server Secret** (Servergeheimnis): Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie bei der Konfiguration des VPN 3000-Konzentrators in der Cisco Secure ACS for Windows-Konfiguration verwenden.**Verifizieren** - Geben Sie das Kennwort zur Überprüfung erneut ein.Damit wird der Authentifizierungsserver in die globale Konfiguration des VPN 3000 Concentrator aufgenommen. Dieser Server wird von allen Gruppen verwendet, außer wenn ein Authentifizierungsserver speziell definiert wurde. Wenn ein Authentifizierungsserver nicht für eine Gruppe konfiguriert ist, wird er auf den globalen Authentifizierungsserver zurückgesetzt.

3. Führen Sie diese Schritte aus, um die Tunnelgruppe auf dem VPN 3000-Konzentrator zu konfigurieren.Wählen Sie im linken Menü **Konfiguration > Benutzerverwaltung > Gruppen** aus, und klicken Sie auf **Hinzufügen**.Ändern oder fügen Sie diese Parameter auf den Registerkarten "Konfiguration" hinzu. Klicken Sie erst auf Apply, wenn Sie alle folgenden Parameter geändert haben:**Hinweis:** Diese Parameter sind das Minimum, das für VPN-Verbindungen mit Remote-Zugriff erforderlich ist. Bei diesen Parametern wird außerdem davon ausgegangen, dass die Standardeinstellungen in der Basisgruppe des VPN 3000-Konzentrators nicht geändert wurden.**Identität**



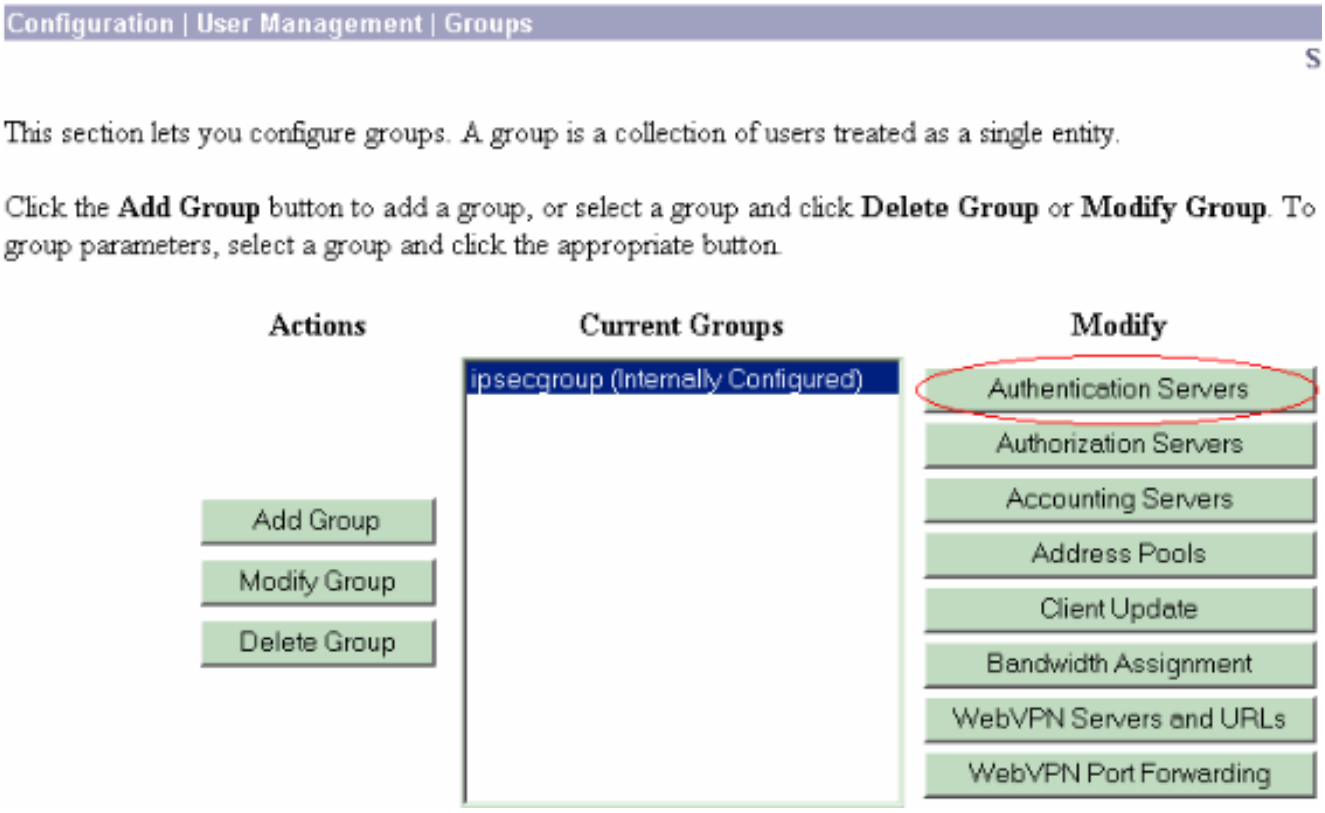
Gruppenname: Geben Sie einen Gruppennamen ein. Beispielsweise IPsecUsers.**Password** (Kennwort): Geben Sie ein Kennwort für die Gruppe ein. Dies ist der vorinstallierte Schlüssel für die IKE-Sitzung.**Verifizieren** - Geben Sie das Kennwort zur Überprüfung erneut ein.**Type** (**Typ**): Lassen Sie dies als Standard:
Intern.**IPsec**



Tunnel Type (Tunnel-Typ): Wählen Sie **Remote Access (Remote-Zugriff)**.**Authentication** (**Authentifizierung**) - RADIUS Dadurch wird dem VPN Concentrator mitgeteilt, welche Methode zur Benutzerauthentifizierung verwendet wird.**Mode Config** (**Moduskonfiguration**): **Konfig**.Klicken Sie auf **Übernehmen**.

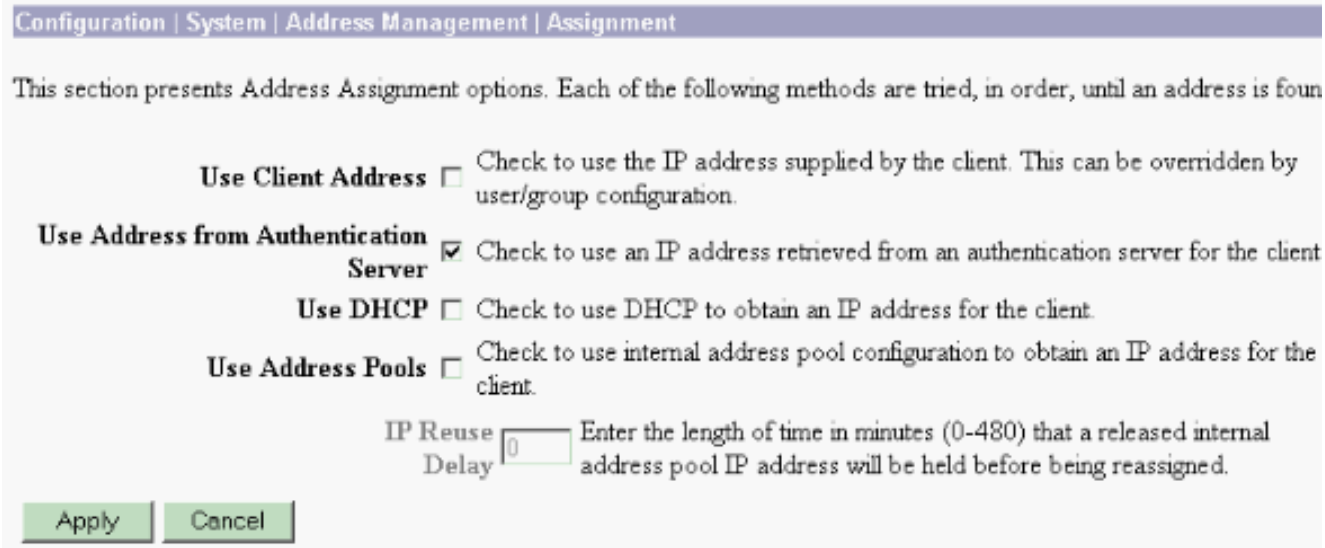
4. Führen Sie diese Schritte aus, um mehrere Authentifizierungsserver im VPN 300 Concentrator zu konfigurieren.Wenn die Gruppe definiert ist, markieren Sie diese Gruppe, und klicken Sie in der Spalte Ändern auf **Authentifizierungsserver**. Für jede Gruppe können individuelle Authentifizierungsserver definiert werden, auch wenn diese Server nicht auf den globalen Servern vorhanden

sind.



Wählen Sie den Servertyp **RADIUS aus**, und fügen Sie diese Parameter für Ihren Cisco Secure ACS für Windows RADIUS-Server hinzu. Behalten Sie alle anderen Parameter im Standardzustand bei.**Authentication Server** (Authentifizierungsserver): Geben Sie die IP-Adresse des Cisco Secure ACS für Windows RADIUS-Server ein.**Server Secret** (Servergeheimnis): Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie bei der Konfiguration des VPN 3000-Konzentrators in der Cisco Secure ACS for Windows-Konfiguration verwenden.**Verifizieren** - Geben Sie das Kennwort zur Überprüfung erneut ein.

5. Wählen Sie **Configuration > System > Address Management > Assignment (Konfiguration > System > Adressenverwaltung > Zuweisung) aus,** und aktivieren Sie **Use Address from Authentication Server (Adresse aus Authentifizierungsserver verwenden)**, um den VPN-Clients die IP-Adresse aus dem im RADIUS-Server erstellten IP-Pool zuzuweisen, sobald der Client authentifiziert
wurde.

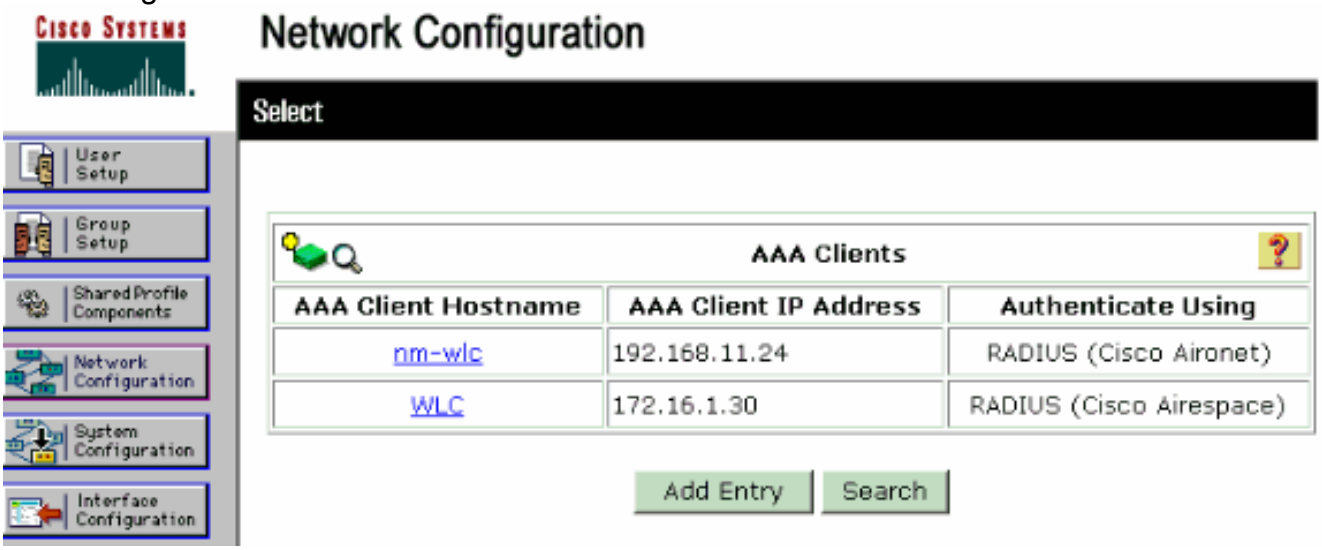


RADIUS-Serverkonfiguration

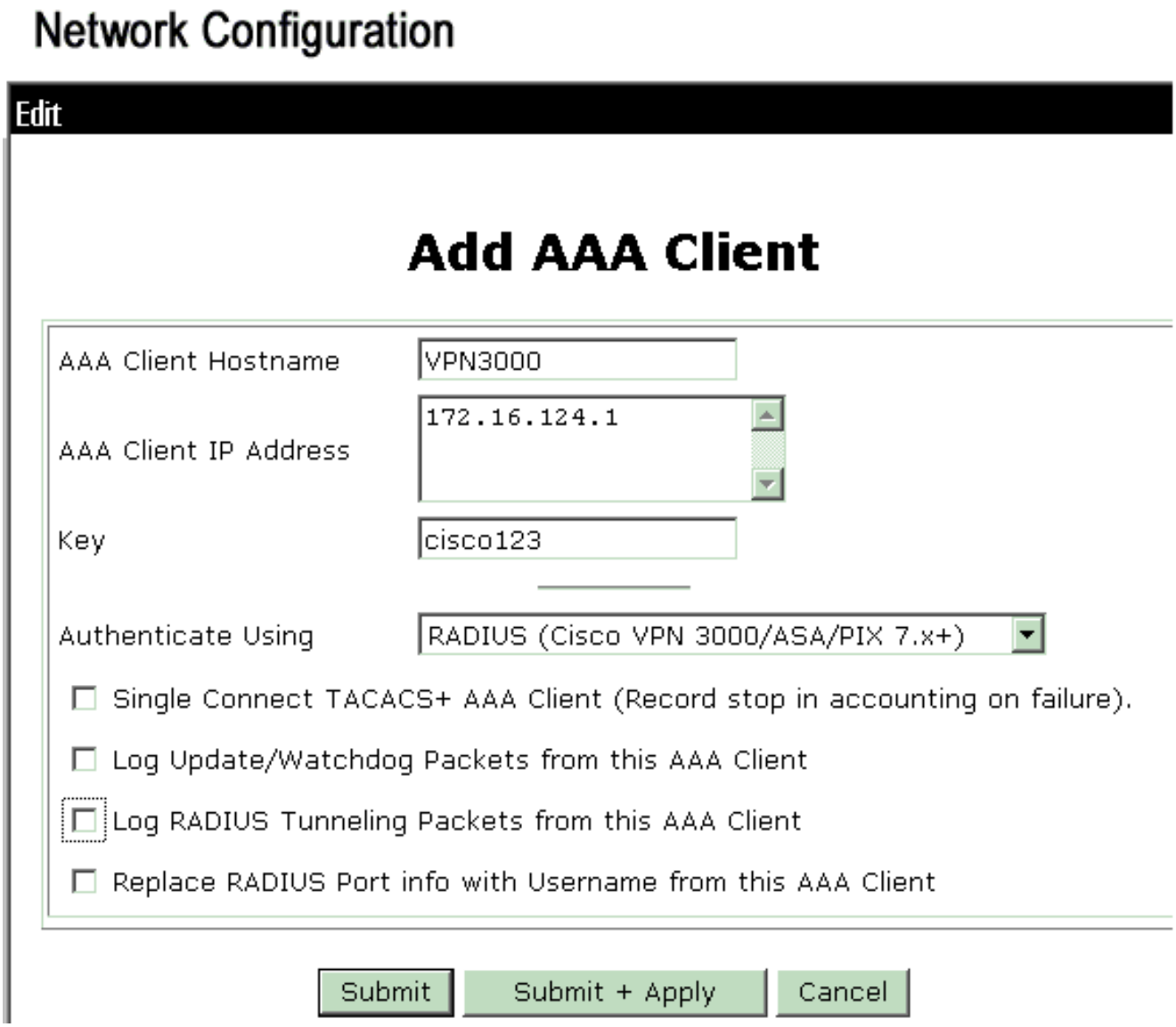
In diesem Abschnitt des Dokuments wird das erforderliche Verfahren zur Konfiguration des Cisco Secure ACS als RADIUS-Server für die vom Cisco VPN Concentrator der Serie 3000 - AAA-Client weitergeleitete VPN-Client-Benutzerauthentifizierung beschrieben.

Doppelklicken Sie auf das Symbol **ACS Admin**, um die Admin-Sitzung auf dem PC zu starten, auf dem der Cisco Secure ACS für Windows RADIUS-Server ausgeführt wird. Melden Sie sich ggf. mit dem richtigen Benutzernamen und Kennwort an.

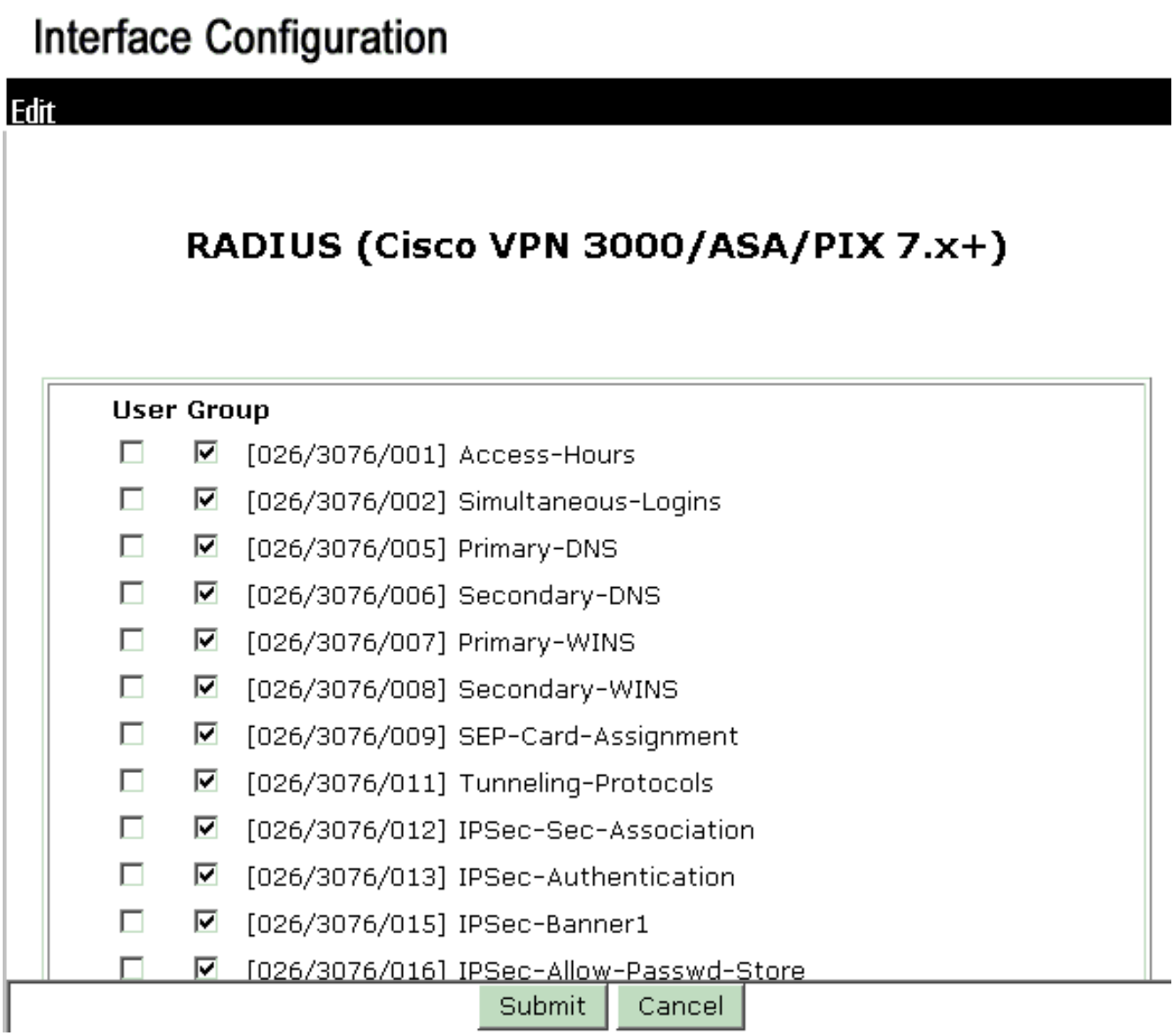
1. Gehen Sie wie folgt vor, um den VPN 300-Konzentrator der Cisco Secure ACS für Windows-Serverkonfiguration hinzuzufügen.Wählen Sie **Network Configuration** (Netzwerkkonfiguration) aus, und klicken Sie auf **Add Entry (Eintrag hinzufügen)**, um dem RADIUS-Server einen AAA-Client hinzuzufügen.



Fügen Sie die folgenden Parameter für den VPN 300-Konzentrator hinzu:

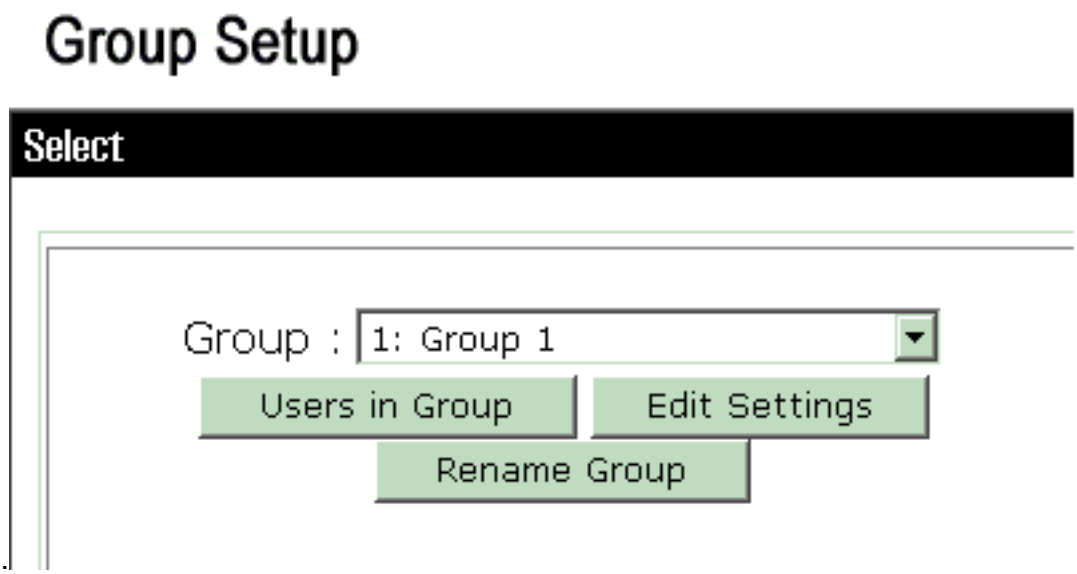


AAA-Client-Hostname - Geben Sie den Hostnamen des VPN 3000-Konzentrators (für die DNS-Auflösung) ein.**AAA-Client-IP-Adresse** - Geben Sie die IP-Adresse Ihres VPN 3000-Konzentrators ein.**Key** (Schlüssel) - Geben Sie den geheimen RADIUS-Server ein. Dies muss der gleiche geheime Schlüssel sein, den Sie beim Hinzufügen des Authentifizierungsservers im VPN Concentrator konfiguriert haben.**Authentication Using (Authentifizierung über** RADIUS) - Wählen Sie **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** aus. Dadurch können die VPN 3000 VSAs im Fenster "Gruppenkonfiguration" angezeigt werden.Klicken Sie auf **Senden**.Wählen Sie **Schnittstellenkonfiguration aus**, klicken Sie auf **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**, und aktivieren Sie **Group [26] Vendor-Specific (anbieterspezifische Gruppe
[26])**.



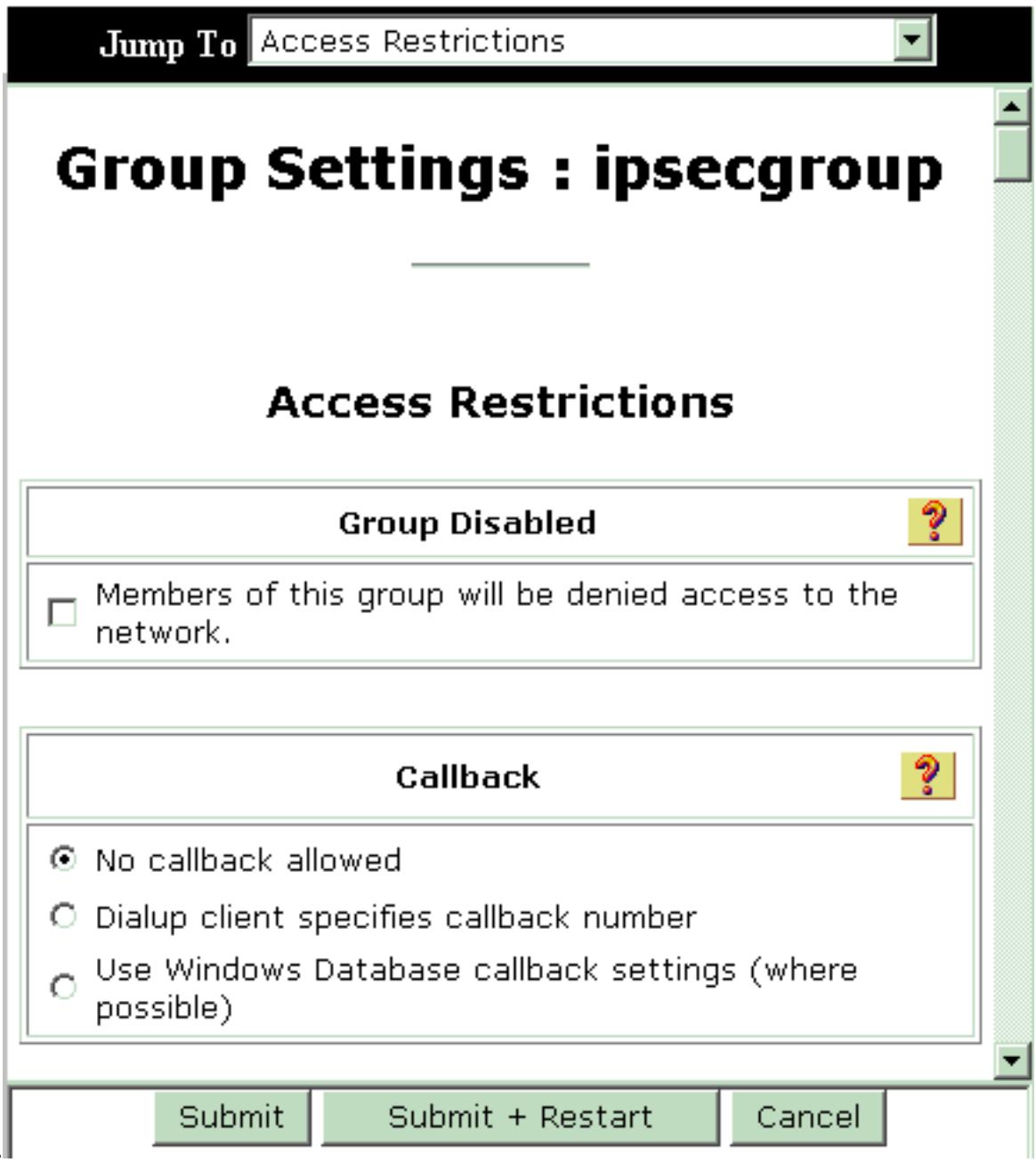
Hinweis: "RADIUS-Attribut 26" bezieht sich auf alle anbieterspezifischen Attribute. Wählen Sie beispielsweise **Interface Configuration > RADIUS (Cisco VPN 3000)** und stellen Sie sicher, dass alle verfügbaren Attribute mit 026 beginnen. Dies zeigt, dass alle diese anbieterspezifischen Attribute unter den IETF RADIUS 26-Standard fallen. Diese Attribute werden standardmäßig nicht in der Benutzer- oder Gruppeneinrichtung angezeigt. Erstellen Sie zum Aufrufen in der Gruppe-Konfiguration einen AAA-Client (in diesem Fall VPN 3000-Konzentrator), der sich in der Netzwerkkonfiguration mit RADIUS authentifiziert. Überprüfen Sie dann die Attribute, die in User Setup (Benutzereinrichtung), Group Setup (Gruppeneinrichtung) oder in beiden Optionen in der Schnittstellenkonfiguration angezeigt werden müssen.Unter RADIUS-Attribute finden Sie weitere Informationen zu den verfügbaren Attributen und deren Verwendung.Klicken Sie auf **Senden**.

2. Führen Sie diese Schritte aus, um der Cisco Secure ACS für Windows-Konfiguration Gruppen hinzuzufügen.Wählen Sie **Group Setup (Gruppeneinrichtung)** aus, wählen Sie eine der Vorlagengruppen aus, z. B. Gruppe 1, und klicken Sie auf **Gruppe**



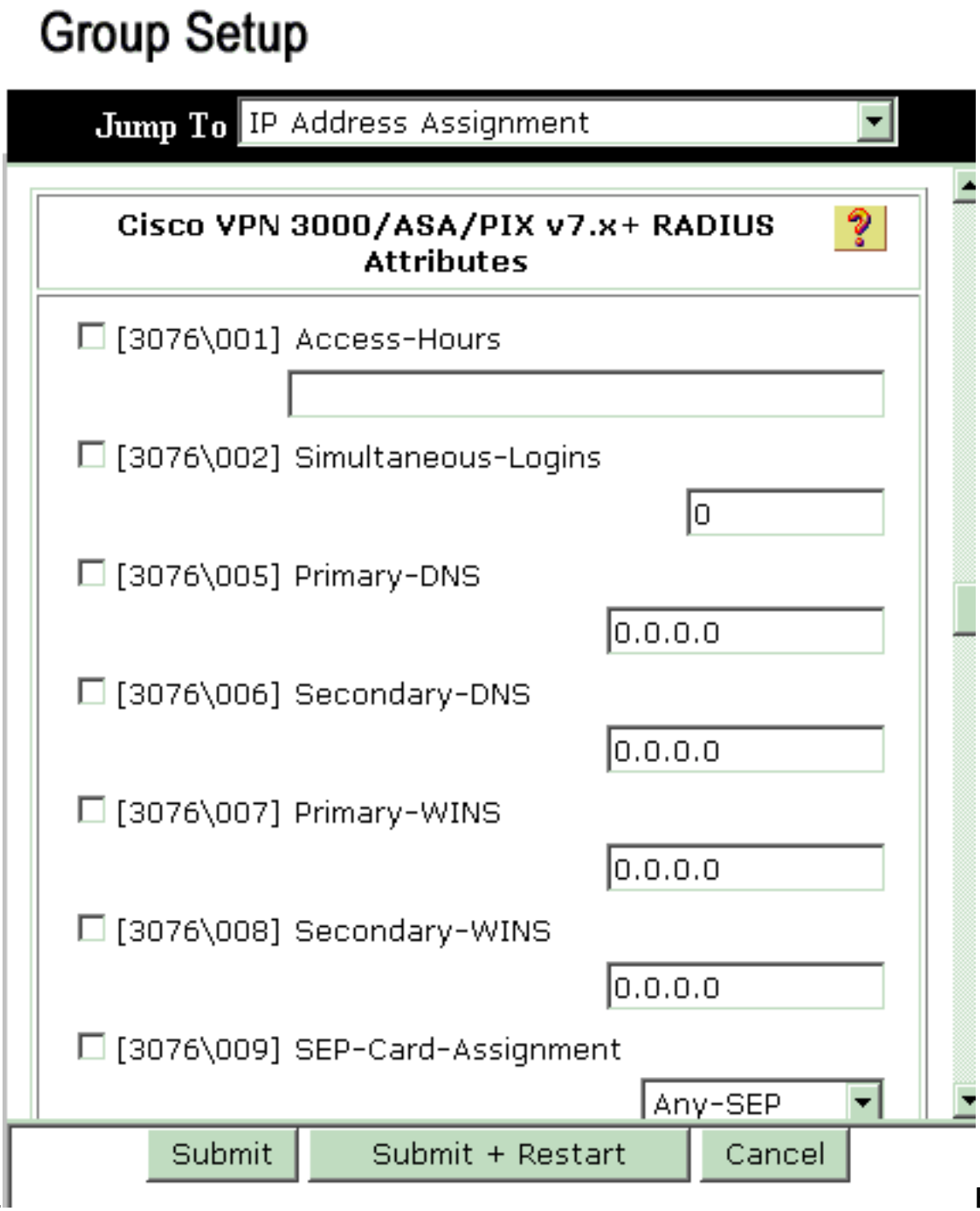
umbenennen.

Ändern Sie den Namen in eine für Ihre Organisation geeignete Form, z. B. ipsecgroup. Da diesen Gruppen Benutzer hinzugefügt werden, sollte der Gruppenname den tatsächlichen Zweck dieser Gruppe widerspiegeln. Wenn alle Benutzer derselben Gruppe angehören, können Sie diese VPN-Benutzergruppe nennen.Klicken Sie auf **Einstellungen bearbeiten**, um die Parameter in der neu umbenannten Gruppe zu



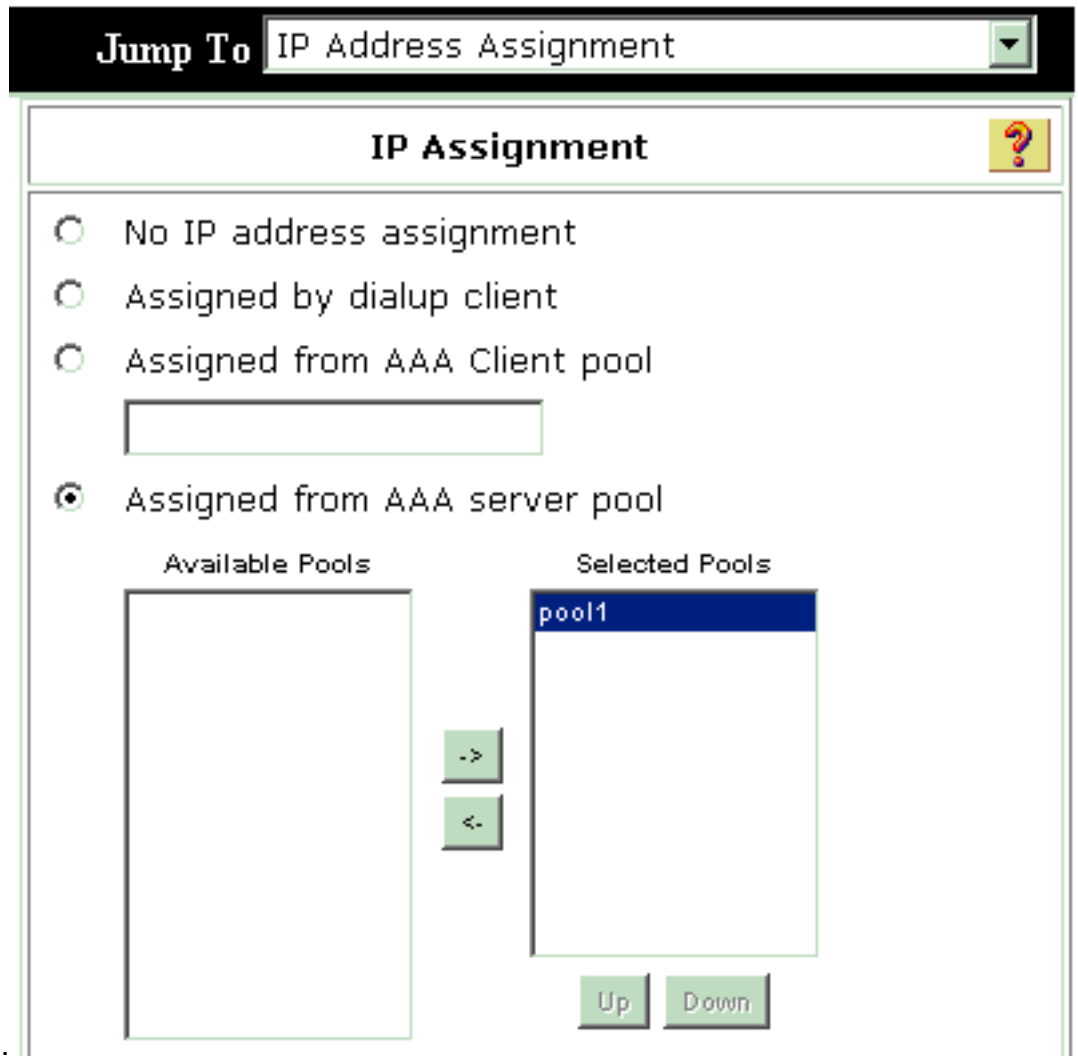
bearbeiten.

Klicken Sie auf **Cisco VPN 3000 RADIUS**, und konfigurieren Sie diese empfohlenen Attribute. Auf diese Weise können Benutzer, die dieser Gruppe zugewiesen sind, die Cisco VPN 3000 RADIUS-Attribute erben, sodass Sie Richtlinien für alle Benutzer in Cisco Secure ACS für Windows zentralisieren



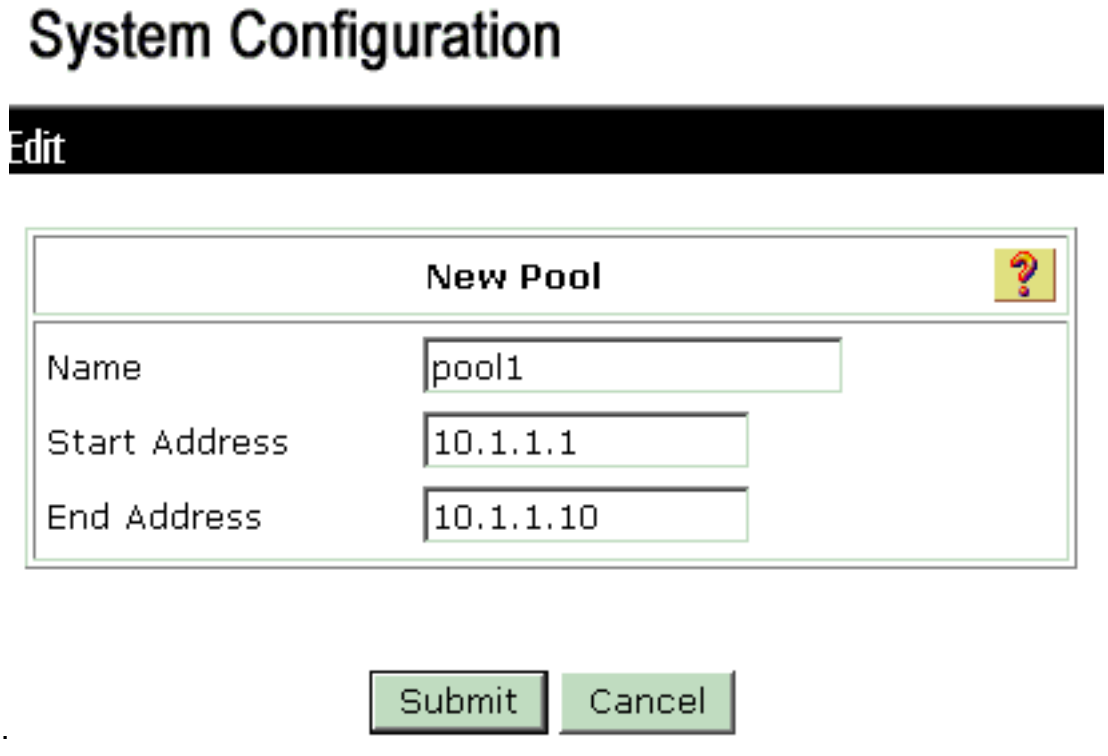
können. **Hinweis:** Technisch gesehen müssen VPN 3000 RADIUS-Attribute nicht konfiguriert werden, solange die Tunnelgruppe in Schritt 3 der Konfiguration des VPN-Konzentrators der Serie 300 eingerichtet ist und die Basisgruppe im VPN-Konzentrator nicht von den ursprünglichen Standardeinstellungen abweicht.**Empfohlene VPN 3000-Attribute:Primary-DNS** (Primärer DNS): Geben Sie die IP-Adresse Ihres primären DNS-Servers ein.**Secondary-DNS** - Geben Sie die IP-Adresse Ihres sekundären DNS-Servers ein.**Primary-WINS** - Geben Sie die IP-Adresse Ihres primären WINS-Servers ein.**Secondary-WINS** - Geben Sie die IP-Adresse Ihres sekundären WINS-Servers ein.**Tunneling-Protokolle** - Wählen Sie **IPsec** aus. Dies ermöglicht *nur* IPsec-Clientverbindungen. PPTP oder L2TP sind nicht zulässig.**IPsec-Sec-Association** - Geben Sie **ESP-3DES-MD5 ein**. Dadurch wird sichergestellt, dass alle IPsec-Clients die höchstmögliche Verschlüsselung verwenden.**IPsec-Allow-Password-Store** - Wählen Sie **Disallow (Unterbrechen)** aus, damit Benutzer ihr Kennwort nicht im VPN-Client speichern können.**IPsec-Banner** - Geben Sie ein Begrüßungs-Banner ein, das dem Benutzer bei der Verbindung angezeigt wird. Beispiel: "Willkommen beim VPN-Zugriff für Mitarbeiter von MyCompany!"**IPsec-Default Domain** - Geben Sie den Domänennamen Ihres

Unternehmens ein. Beispiel: "mycompany.com".Dieser Satz von Attributen ist nicht erforderlich. Wenn Sie sich jedoch nicht sicher sind, ob sich die Attribute der Basisgruppe des VPN 3000-Konzentrators geändert haben, empfiehlt Cisco, die folgenden Attribute zu konfigurieren:**Simultaneous-Logins**: Geben Sie die Anzahl der Anmeldeversuche eines Benutzers mit demselben Benutzernamen ein. Die Empfehlung lautet 1 oder 2.**SEP-Card-Assignment** - Wählen Sie **Any-SEP aus**.**IPsec-Mode-Config** - Wählen Sie **ON (EIN)**.**IPsec over UDP** (IPsec über UDP): Wählen Sie **AUS**, es sei denn, Sie möchten, dass Benutzer in dieser Gruppe IPsec über das UDP-Protokoll verbinden. Wenn Sie ON auswählen, kann der VPN-Client IPsec über UDP lokal deaktivieren und eine normale Verbindung herstellen.**IPsec über UDP-Port** - Wählen Sie eine UDP-Portnummer zwischen 4001 und 49151 aus. Dies wird nur verwendet, wenn IPsec über UDP ON ist.Für den nächsten Satz von Attributen müssen Sie zunächst im VPN-Concentrator etwas einrichten, bevor Sie diese verwenden können. Dies wird nur für fortgeschrittene Benutzer empfohlen.**Zugriffszeiten**: Sie müssen für den VPN 3000-Konzentrator unter **Konfiguration > Richtlinienmanagement** eine Reihe von Zugriffszeiten einrichten. Verwenden Sie stattdessen die in Cisco Secure ACS für Windows verfügbaren Zugriffszeiten, um dieses Attribut zu verwalten.**IPsec-Split-Tunnel-List**: Hierfür müssen Sie im VPN-Konzentrator unter **Konfiguration > Richtlinienmanagement > Datenverkehrsmanagement** eine Netzwerkliste einrichten. Dies ist eine Liste von Netzwerken, die an den Client gesendet werden, um den Client anzuweisen, Daten nur an die Netzwerke in der Liste zu verschlüsseln.Wählen Sie **IP-Zuweisung in der Gruppeneinrichtung aus**, und aktivieren Sie **Assigned from AAA server Pool (Aus AAA-Serverpool zugewiesen**, um die IP-Adressen nach der Authentifizierung VPN Client-Benutzern

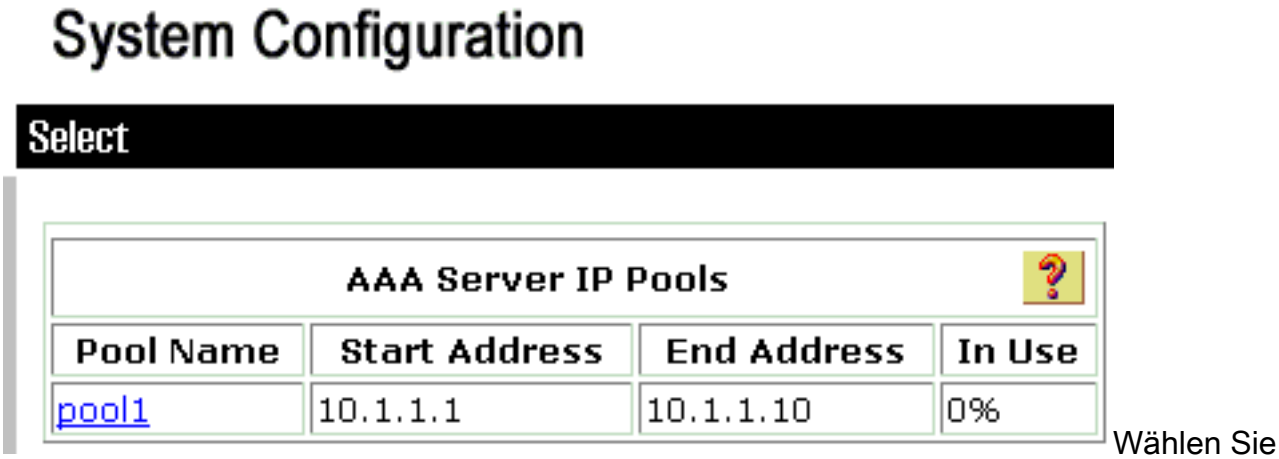


zuzuweisen. W

ählen Sie **Systemkonfiguration > IP-Pools**, um einen IP-Pool für VPN-Client-Benutzer zu erstellen, und klicken Sie auf

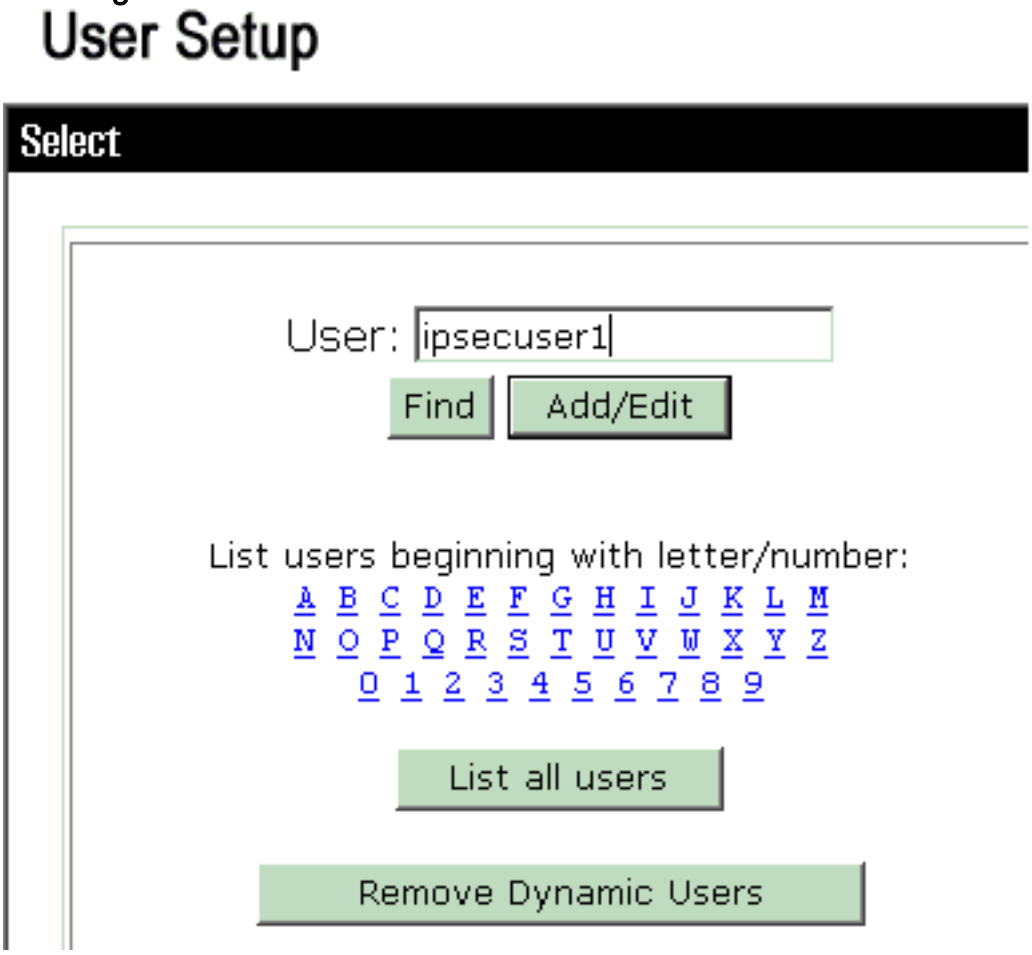


Senden.

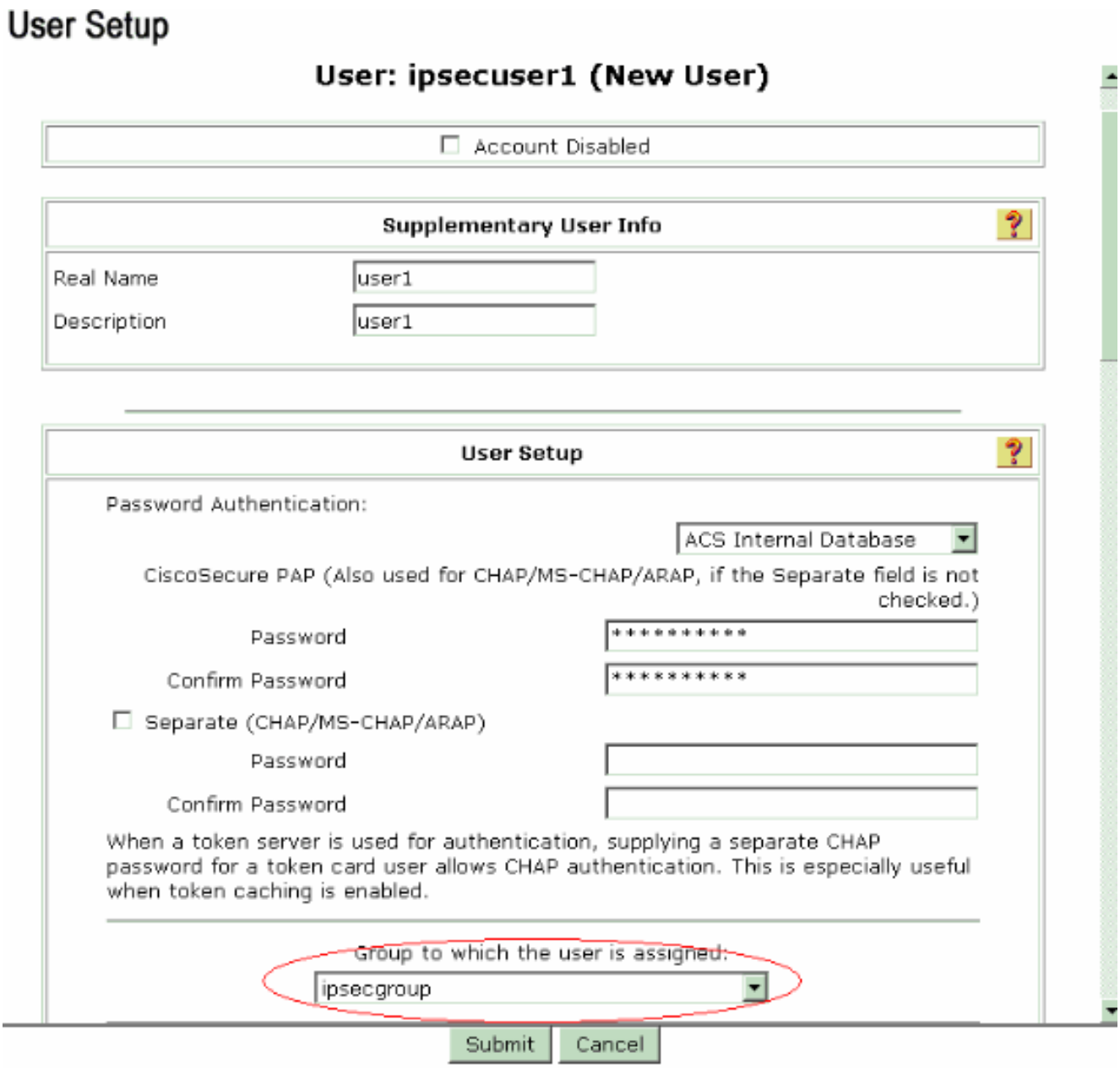


Wählen Sie **Senden** > **Neu starten**, um die Konfiguration zu speichern und die neue Gruppe zu aktivieren.Wiederholen Sie diese Schritte, um weitere Gruppen hinzuzufügen.

3. **Konfigurieren von Benutzern auf Cisco Secure ACS für Windows**Wählen Sie **User Setup**, geben Sie einen Benutzernamen ein, und klicken Sie auf **Hinzufügen/Bearbeiten**.



Konfigurieren Sie diese Parameter im Abschnitt "Benutzereinrichtung":

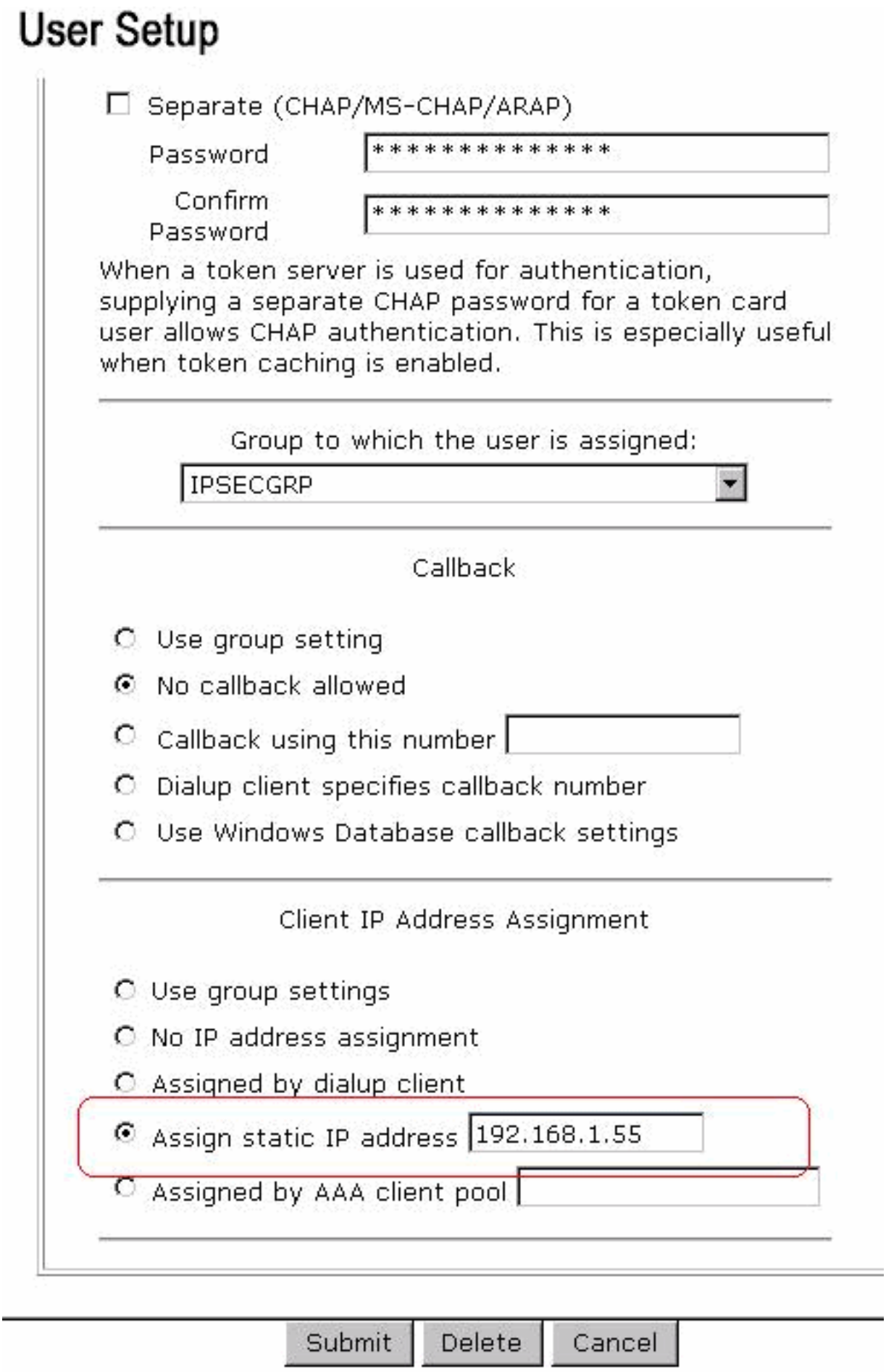


Kennwortauthentifizierung - Wählen Sie **ACS Internal Database (Interne ACS-Datenbank)** aus.**Cisco Secure PAP - Kennwort** - Geben Sie ein Kennwort für den Benutzer ein.**Cisco Secure PAP - Passwort bestätigen** - Geben Sie das Kennwort für den neuen Benutzer erneut ein.**Gruppe, der der Benutzer zugewiesen ist** - Wählen Sie den Namen der Gruppe aus, die Sie im vorherigen Schritt erstellt haben.Klicken Sie auf **Senden**, um die Benutzereinstellungen zu speichern und zu aktivieren.Wiederholen Sie diese Schritte, um weitere Benutzer hinzuzufügen.

Zuweisen einer statischen IP-Adresse zum VPN-Client-Benutzer

Gehen Sie wie folgt vor:

1. Erstellen Sie eine neue VPN-Gruppe IPSECGRP.
2. Erstellen Sie einen Benutzer, der die statische IP empfangen möchte, und wählen Sie **IPSECGRP aus**. Wählen Sie **Statische IP-Adresse** mit der statischen IP-Adresse **zuweisen**, die unter der Client-IP-Adressenzuweisung zugewiesen

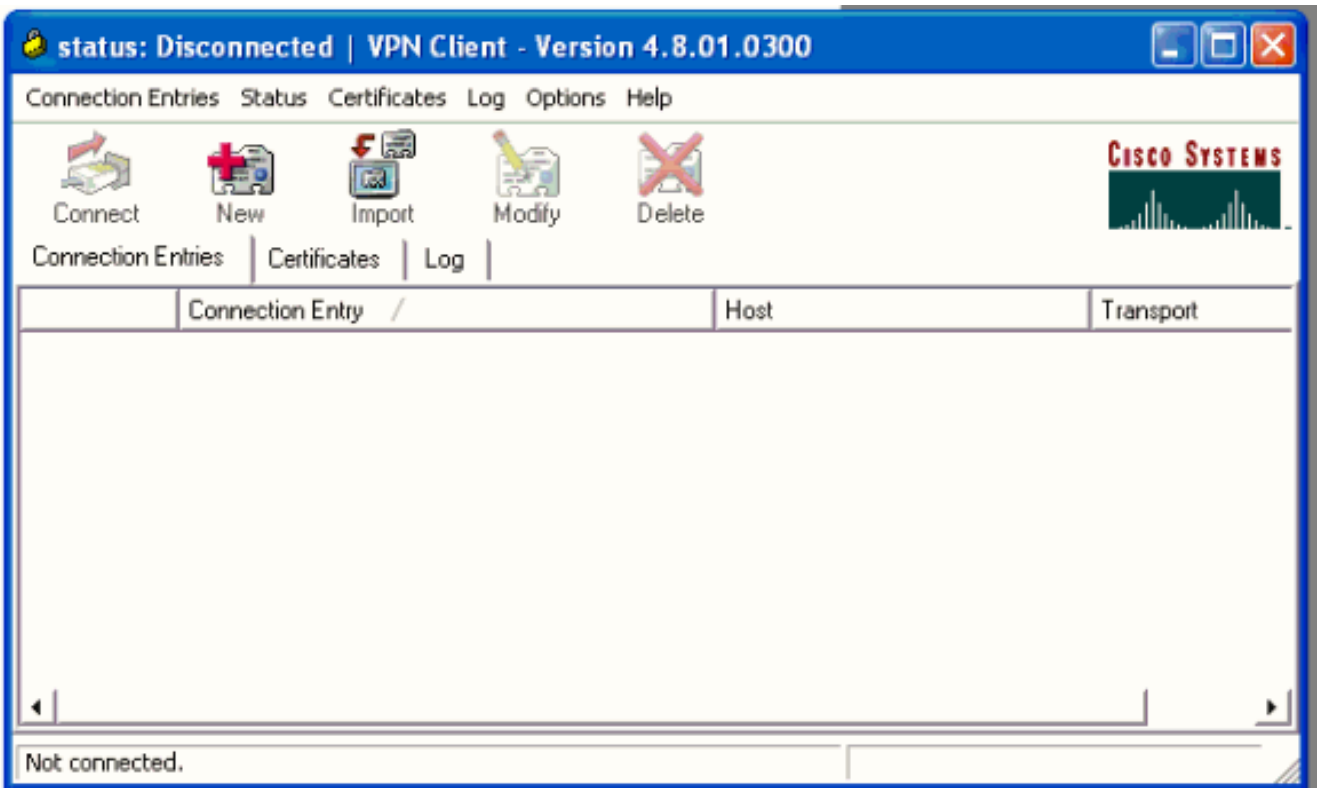


wird.

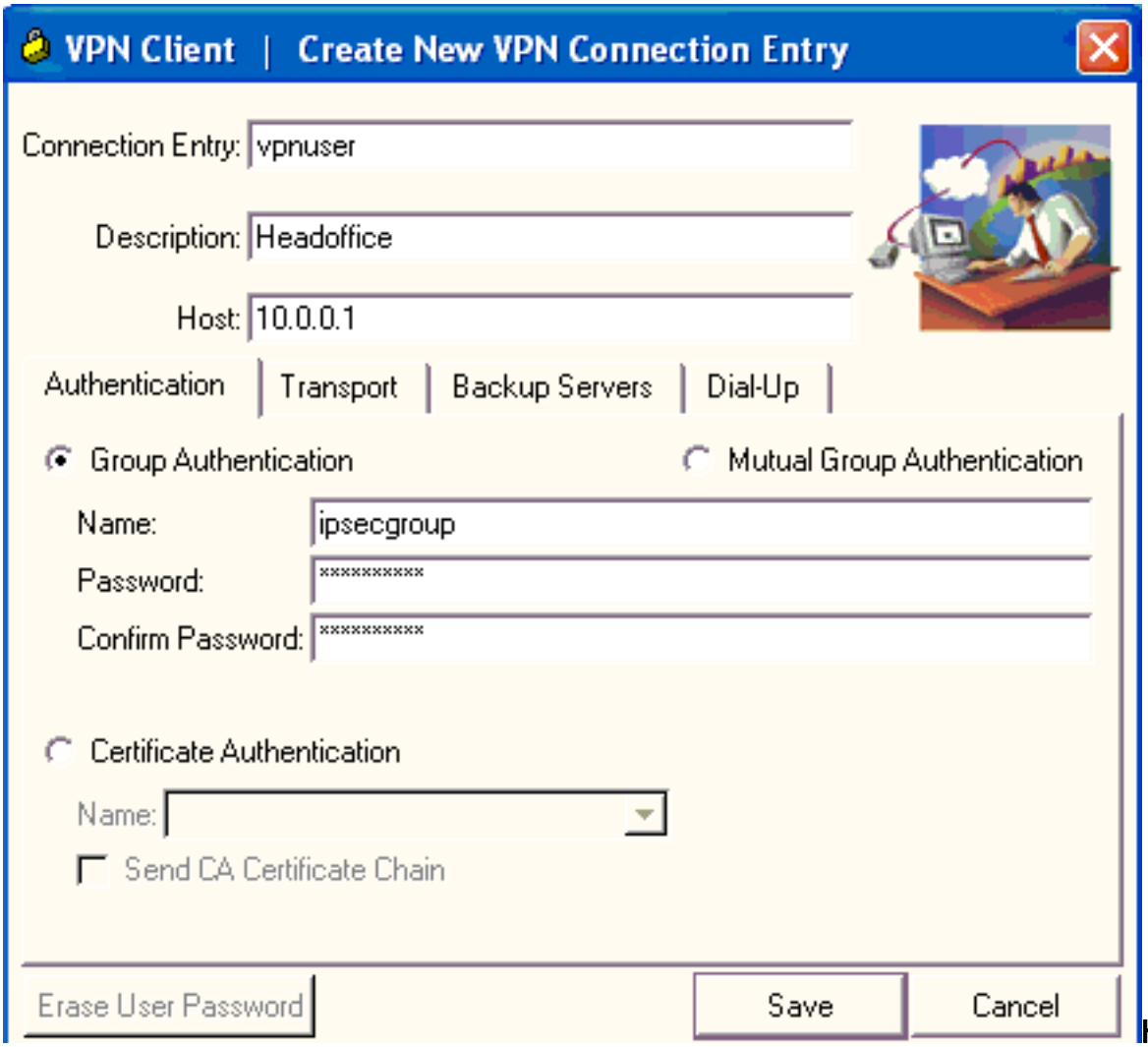
[VPN-Client-Konfiguration]

In diesem Abschnitt wird die Konfiguration der VPN-Client-Seite beschrieben.

1. Wählen Sie **Start > Programme > Cisco Systems VPN Client > VPN Client aus**.
2. Klicken Sie auf **Neu**, um das Fenster Create New VPN Connection Entry (Neue VPN-Verbindung erstellen) zu
   öffnen.



3. Weisen Sie Ihrem Eintrag bei Aufforderung einen Namen zu. Sie können auch eine Beschreibung eingeben, wenn Sie möchten. Geben Sie die IP-Adresse der öffentlichen Schnittstelle des VPN 3000 Concentrator in der Spalte Host an, und wählen Sie **Gruppenauthentifizierung** aus. Geben Sie dann den Gruppennamen und das Kennwort ein. Klicken Sie auf **Speichern**, um den neuen VPN-Verbindungseintrag abzuschließen.

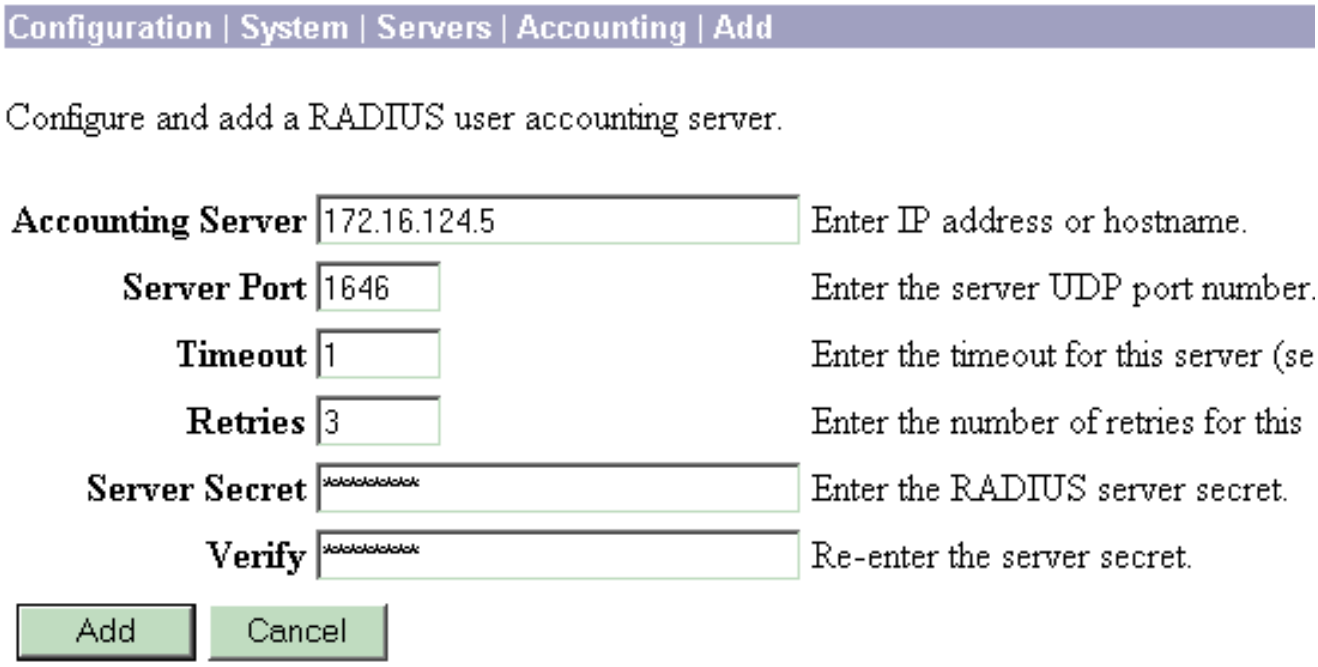


Hinweis: Stellen Sie sicher, dass der VPN-Client so konfiguriert ist, dass er denselben Gruppennamen und dasselbe Kennwort verwendet, der im Cisco VPN-Konzentrator der Serie 3000 konfiguriert wurde.

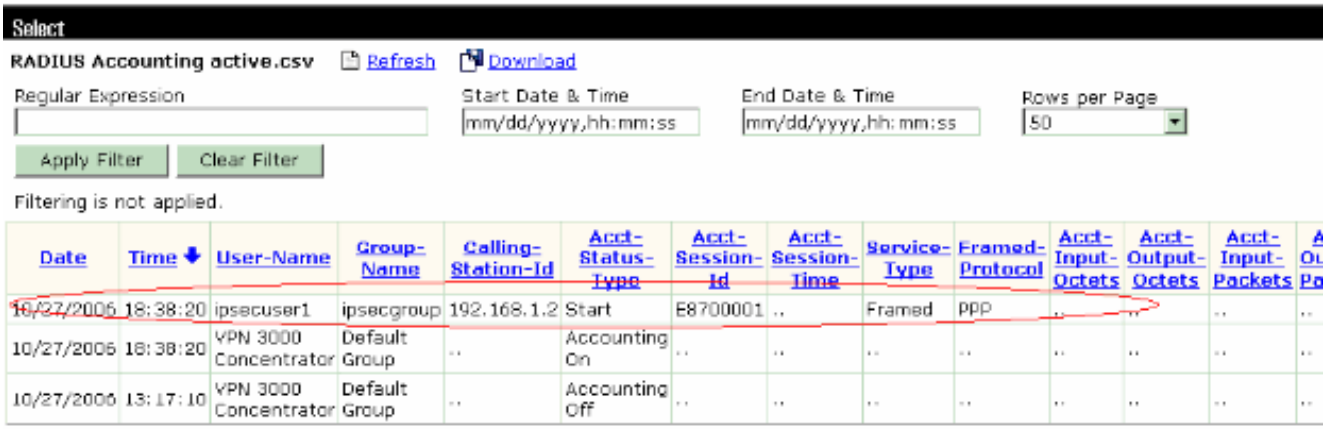
Accounting hinzufügen

Nach der Authentifizierung können Sie Accounting hinzufügen.

1. Wählen Sie auf dem VPN 300 **Configuration > System > Servers > Accounting Servers aus**, und fügen Sie den **Cisco Secure ACS für Windows-**Server hinzu.
2. Sie können jeder Gruppe individuelle Accounting-Server hinzufügen, wenn Sie **Konfiguration > Benutzerverwaltung > Gruppen** auswählen, eine Gruppe markieren und auf **Konto ändern** klicken**. Server**. Geben Sie dann die IP-Adresse des Accounting-Servers mit dem Servergeheimnis
ein.



In Cisco Secure ACS für Windows werden die Accounting-Datensätze wie folgt angezeigt:



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Überprüfen des VPN-Konzentrators

Wählen Sie auf der Seite VPN 3000 Concentrator (VPN-Konzentrator) **Administration > Administration (Administration > Sitzungen verwalten)**, um die Einrichtung des Remote-VPN-Tunnels zu überprüfen.

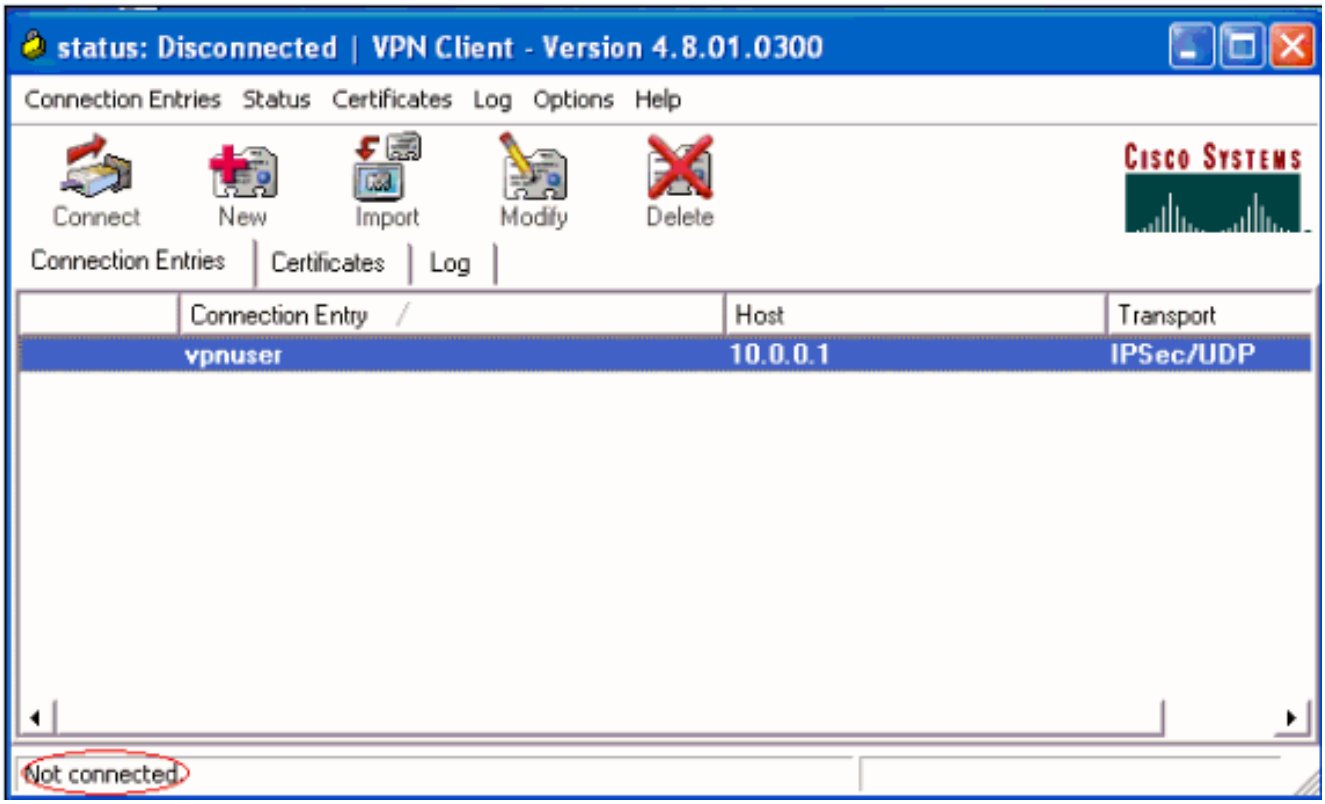
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

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]

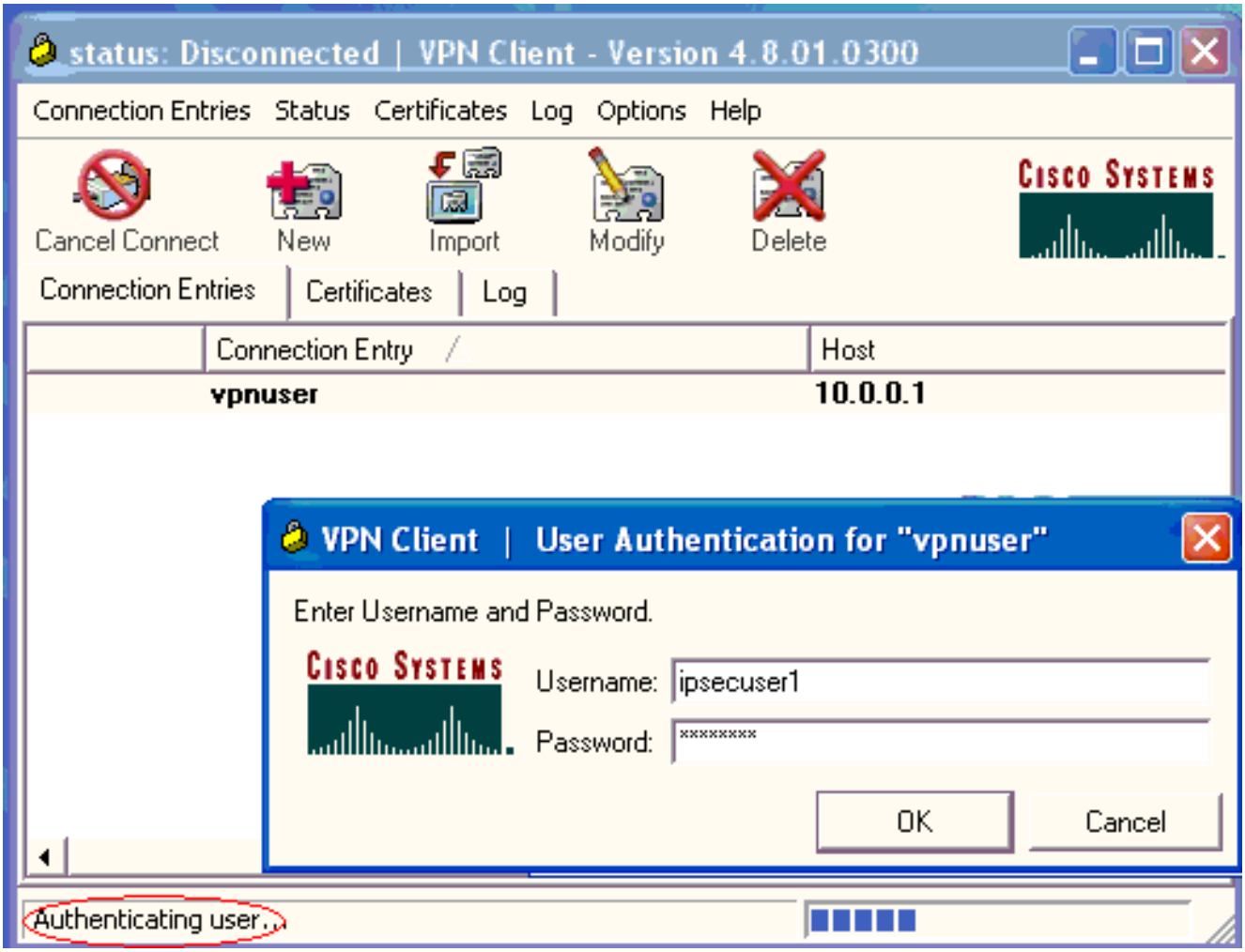
Überprüfen des VPN-Clients

Führen Sie diese Schritte aus, um den VPN-Client zu überprüfen.

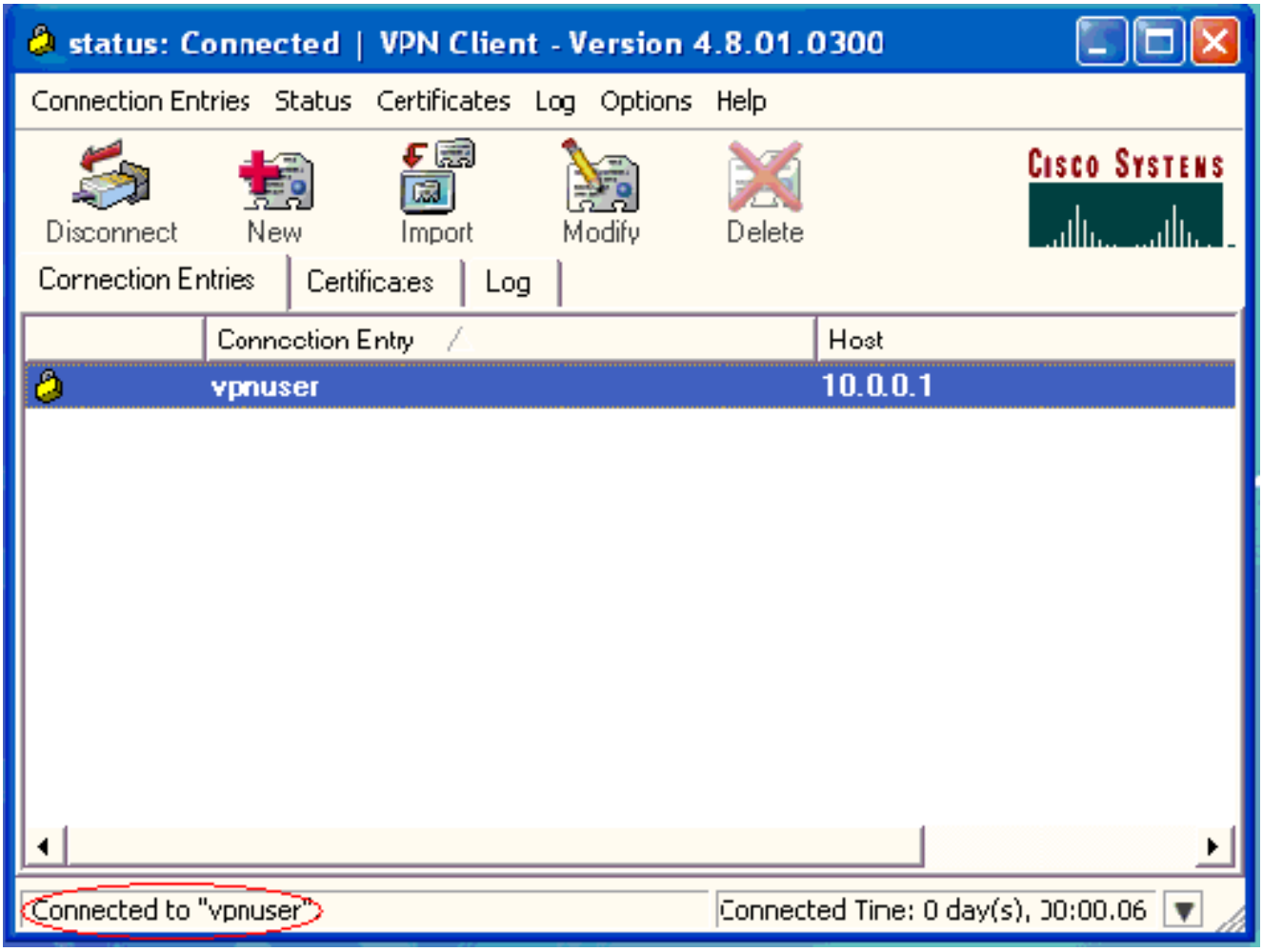
1. Klicken Sie auf **Verbinden**, um eine VPN-Verbindung zu initiieren.



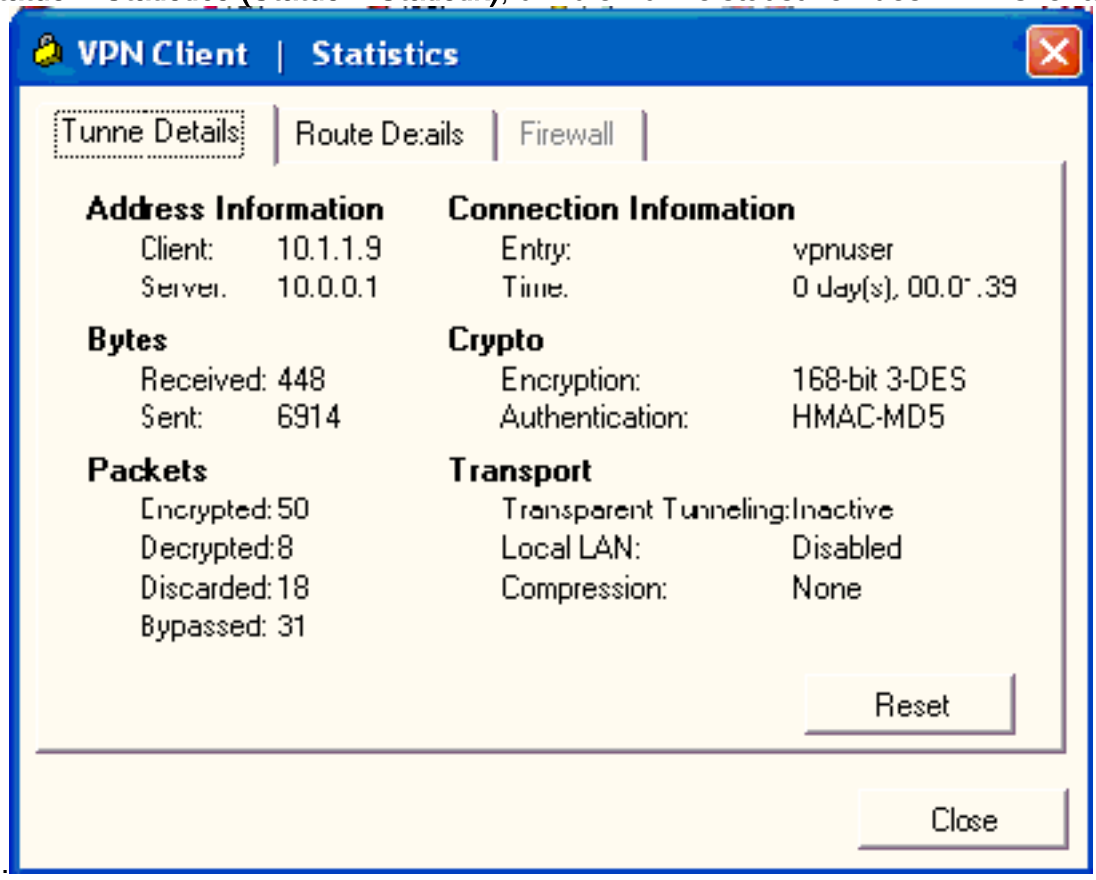
2. Dieses Fenster wird für die Benutzerauthentifizierung angezeigt. Geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort ein, um die VPN-Verbindung herzustellen.



3. Der VPN-Client wird in der Zentrale mit dem VPN 3000-Konzentrator verbunden.



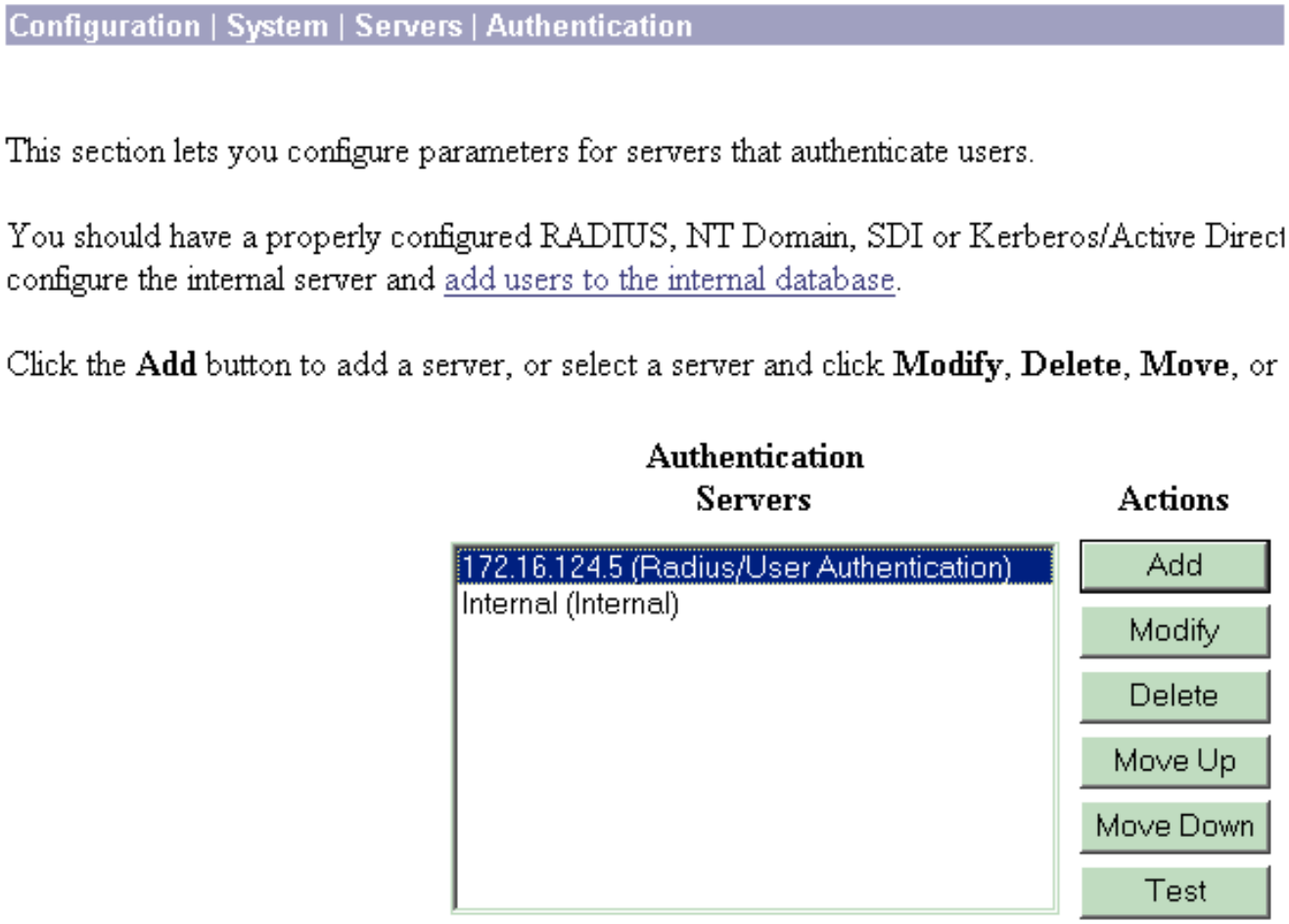
4. Wählen Sie **Status > Statistics (Status > Statistik)**, um die Tunnelstatistiken des VPN-Clients zu überprüfen.



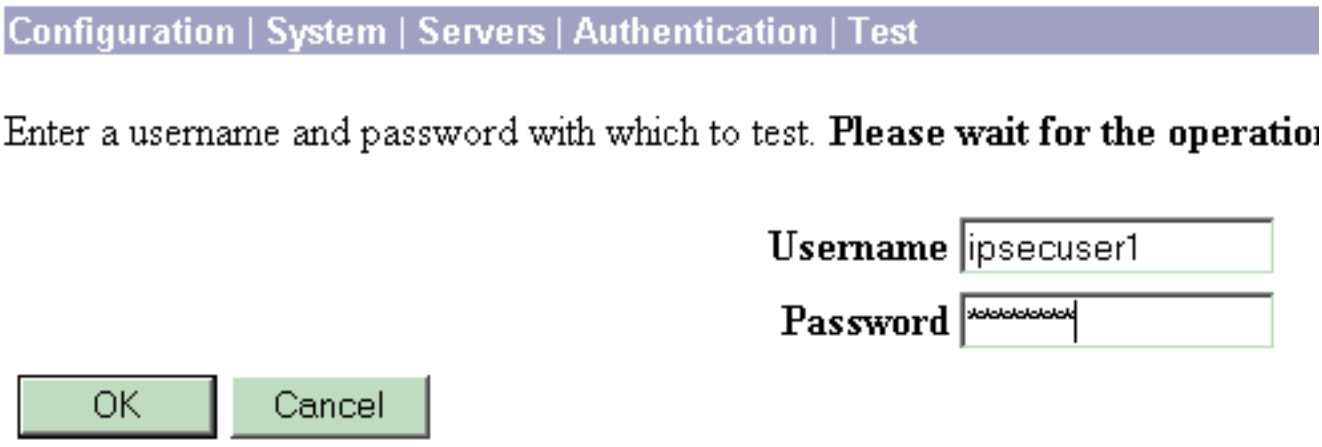
Fehlerbehebung

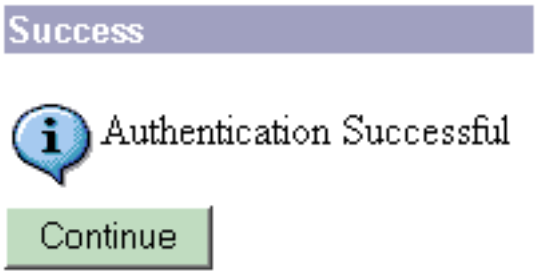
Führen Sie diese Schritte aus, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

1. Wählen Sie **Configuration > System > Servers > Authentication (Konfiguration > System > Server > Authentifizierung) aus,** und führen Sie diese Schritte aus, um die Verbindung zwischen dem RADIUS-Server und dem VPN 3000-Konzentrator zu testen.Wählen Sie den Server aus, und klicken Sie dann auf **Test**.



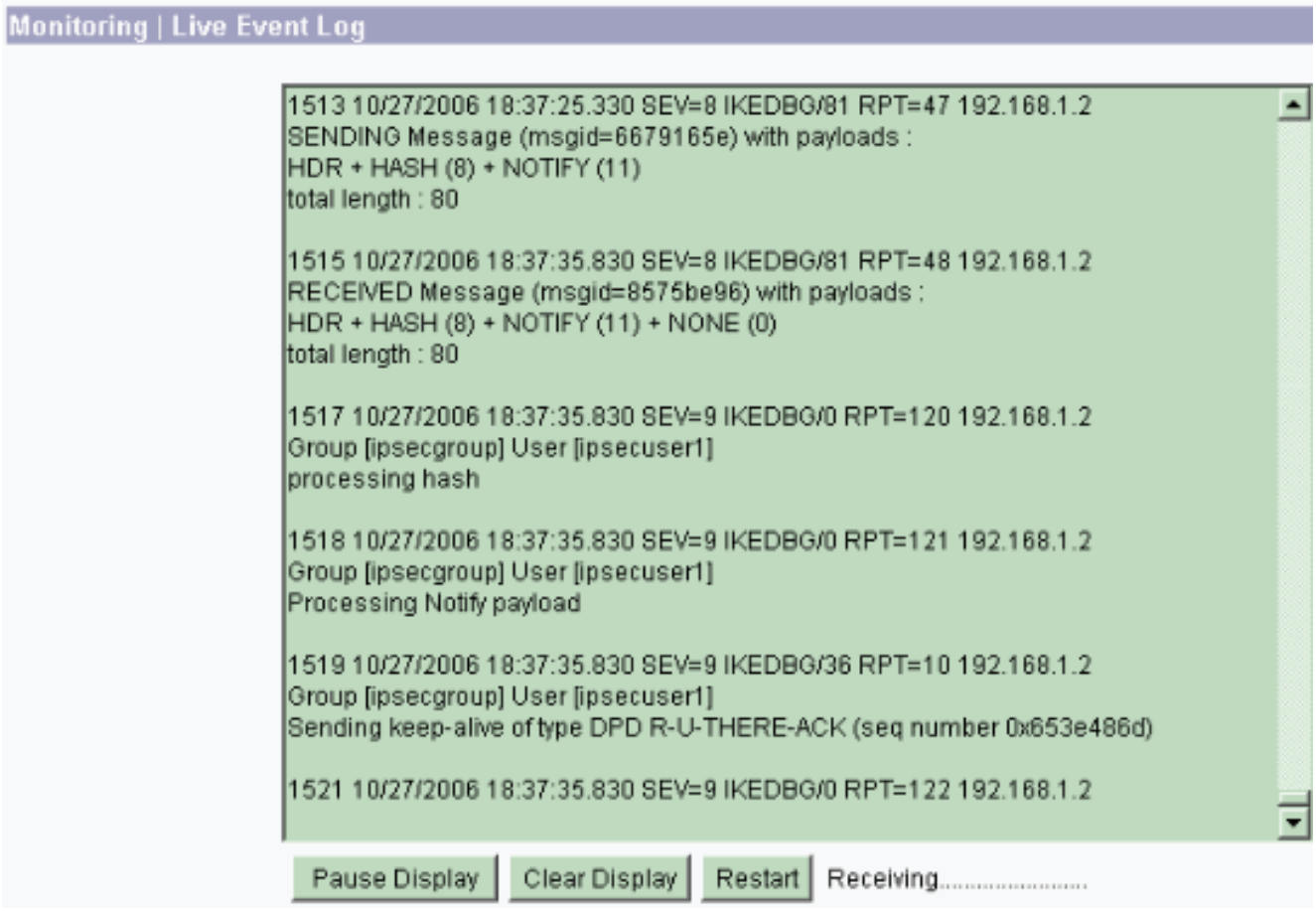
Geben Sie den RADIUS-Benutzernamen und das RADIUS-Kennwort ein, und klicken Sie auf **OK**.





Eine erfolgreiche Authentifizierung wird angezeigt.

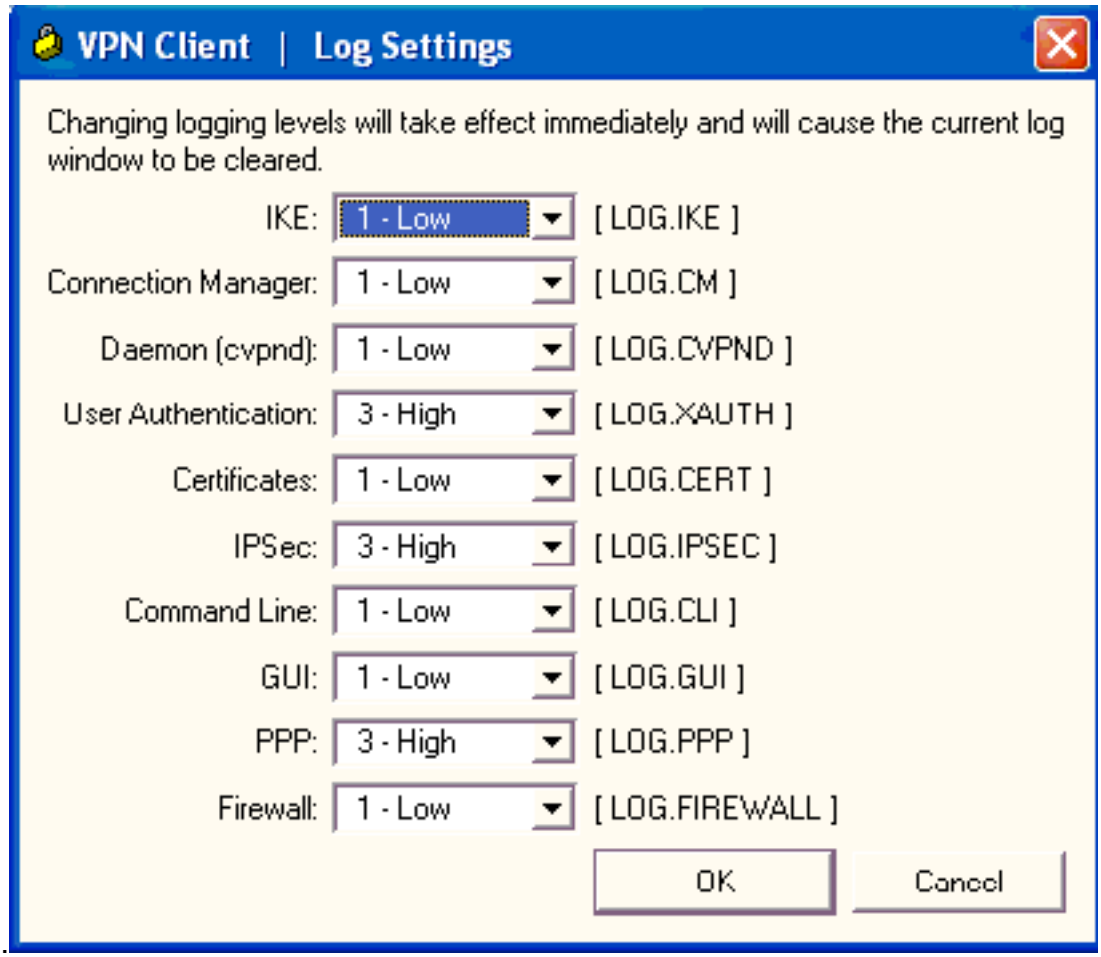
2. Wenn es fehlschlägt, liegt entweder ein Konfigurationsproblem oder ein IP-Verbindungsproblem vor. Überprüfen Sie, ob im ACS-Server bei fehlgeschlagenen Versuchen Meldungen zu dem Fehler eingehen.Wenn in diesem Protokoll keine Meldungen angezeigt werden, liegt wahrscheinlich ein Problem mit der IP-Verbindung vor. Die RADIUS-Anforderung erreicht den RADIUS-Server nicht. Überprüfen Sie, ob die auf die entsprechende VPN 300 Concentrator-Schnittstelle angewendeten Filter RADIUS (1645)-Pakete ein- und auslassen.Wenn die Testauthentifizierung erfolgreich ist, die Anmeldung beim VPN 3000-Konzentrator jedoch weiterhin fehlschlägt, überprüfen Sie das Filterbare Ereignisprotokoll über den Konsolenport.Wenn Verbindungen nicht funktionieren, können Sie dem VPN-Konzentrator AUTH-, IKE- und IPsec-Ereignisklassen hinzufügen, wenn Sie **Configuration > System > Events > Classes > Modify (Severity to Log=1-9, Severity to Console=1-3)** auswählen. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG und IPSECDECODE sind ebenfalls verfügbar, können aber zu viele Informationen bereitstellen. Wenn detaillierte Informationen zu den Attributen benötigt werden, die vom RADIUS-Server, AUTHDECODE, IKEDECODE und IPSECDECODE weitergeleitet werden, stellen Sie diese auf der Ebene Severity to Log=1-13 bereit.
3. Rufen Sie das Ereignisprotokoll von **Überwachung > Ereignisprotokoll ab**.



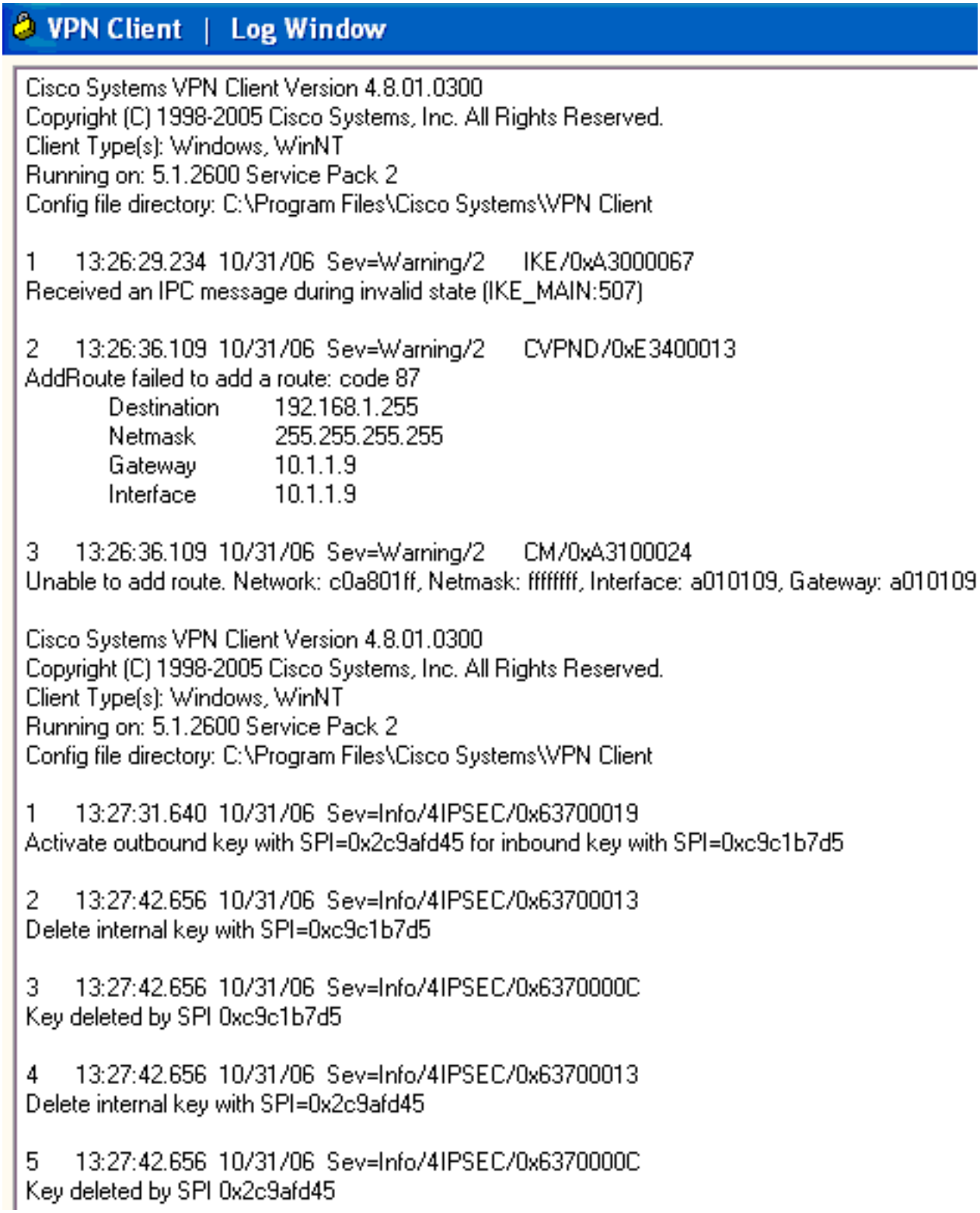
Fehlerbehebung beim VPN Client 4.8 für Windows

Führen Sie diese Schritte aus, um eine Fehlerbehebung für VPN Client 4.8 für Windows durchzuführen.

1. Wählen Sie **Log > Log settings** (Protokoll > Protokolleinstellungen), um die Protokollstufen im VPN-Client zu aktivieren.



2. Wählen Sie **Log > Log Window (Protokoll > Protokollfenster)**, um die Protokolleinträge im VPN-Client anzuzeigen.



Zugehörige Informationen

- Support-Seite für Cisco VPN Concentrator der Serie 3000
- Support-Seite für Cisco VPN-Clients
- IPsec-Aushandlung/IKE-Protokolle
- Support-Seite für Cisco Secure ACS für Windows
- Konfigurieren dynamischer Filter auf einem RADIUS-Server
- Technischer Support und Dokumentation - Cisco Systems