Пример конфигурации IPsec между концентратором VPN 3000 и VPN Client 4.x для Windows, с использованием RADIUS для проверки подлинности пользователя и учета сетевых ресурсов

Содержание

Введение

Этот документ описывает, как установить Туннель IPSec между Cisco VPN 3000 Concentrator и Cisco VPN Client 4.x для Microsoft Windows, который использует RADIUS для проверки подлинности пользователя и учета. Этот документ рекомендует серверу Cisco Secure Access Control Server (ACS) для Windows для более легкой Конфигурации RADIUS аутентифицировать пользователей, которые соединяются с VPN 3000 Concentrator. Группа на VPN 3000 Concentrator является набором пользователей, рассматриваемым как единый объект. Конфигурация групп, в противоположность отдельным пользователям, может упростить управление системой и оптимизировать задачи конфигурации.

См. PIX/ASA 7.x и Cisco VPN Client 4.x для Windows с Microsoft Windows 2003 Примера настройки аутентификации RADIUS IAS для устанавливания соединения VPN для удаленного доступа между Cisco VPN Client (4.x для Windows) и устройством защиты PIX 500 Series 7.x, который использует сервер RADIUS Интернет-сервиса проверки подлинности (IAS) Microsoft Windows 2003 года.

См. IPsec Настройки Между маршрутизатором Cisco IOS и Cisco VPN Client 4.x для Windows Using RADIUS для Проверки подлинности пользователя для настройки соединения между маршрутизатором и Cisco VPN Client 4.x, который использует RADIUS для проверки подлинности пользователя.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Secure ACS для Windows RADIUS установлен и работает должным образом с другими устройствами.
- Cisco VPN 3000 Concentrator настроен и может управляться с интерфейсом HTML.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Secure ACS для Windows с версией 4.0
- Концентратор Cisco VPN серии 3000 с графическим файлом 4.7.2. B
- Cisco VPN Client 4. x

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

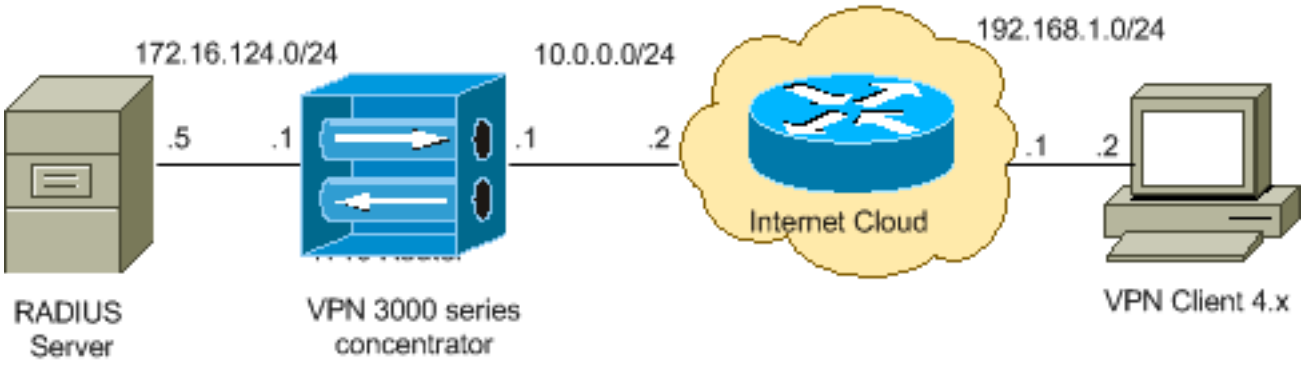
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: Схемы IP-адресации, которые использованы в данной конфигурации, не поддерживаются официальной маршрутизацией в Интернете. Это адреса RFC 1918, используемые в лабораторной среде.

Используйте группы на VPN 3000 Concentrator

Группы могут быть определены и для Cisco Secure ACS для Windows и для VPN 3000 Concentrator, но они используют группы несколько по-другому. Выполните эти задачи для упрощения вещей:

- **Настройте одиночную группу на VPN 3000 Concentrator** для того, когда вы установите начальный туннель. Это обычно называют Туннельная группа, и она используется для того, чтобы установить зашифрованный ключ (IKE) для сессии обмена с VPN 3000 Concentrator при помощи заранее известного ключа (пароль группы). Это - то же имя группы и пароль, который должен быть настроен на всех клиентах Cisco VPN, которые хотят соединиться с Концентратором VPN.
- **Настройте группы на Cisco Secure ACS для Windows Server**, которые используют стандартные атрибуты RADIUS и Определяемые поставщиком Атрибуты (VSA) для управления политиками. VSA, которые должны использоваться с VPN 3000 Concentrator, являются RADIUS (VPN 3000) атрибуты.
- **Настройте пользователей на Cisco Secure ACS для Сервера Windows Radius и назначьте их на одну из групп**, настроенных на том же сервере. Пользователи наследовали атрибуты, определенные для их группы, и Cisco Secure ACS для Windows передает те атрибуты к Концентратору VPN, когда аутентифицируется пользователь.

Как концентратор VPN 3000 использует атрибуты группы и пользователя

После того, как VPN 3000 Concentrator аутентифицирует Туннельную группу с Концентратором VPN и пользователя с RADIUS, это должно организовать атрибуты, которые это получило. Концентратор VPN использует атрибуты в этом заказе предпочтения, сделана ли аутентификация в Концентраторе VPN или с RADIUS:

1. **Атрибуты пользователя** — Эти атрибуты всегда имеют приоритет по любым другим.
2. **Атрибуты Туннельной группы** — Любые атрибуты, не возвращенные, когда пользователь аутентифицировался, заполнены в атрибутами Туннельной группы.
3. **Атрибуты базовой группы** — Любые атрибуты, отсутствующие от пользователя или атрибутов Туннельной группы, заполнены в Атрибутами базовой группы Концентратора VPN.

Конфигурация концентратора серии VPN 3000

Завершите процедуру в этом разделе для настройки Cisco VPN 3000 Concentrator для параметров, требуемых к IP - безопасному соединению, а также клиенту AAA для пользователя VPN для аутентификации с сервером RADIUS.

В этих лабораторных параметрах к Концентратору VPN сначала обращаются через консольный порт, и минимальная настройка добавлена как показано в выходных данных ниже:

```
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 -
>
```

Концентратор VPN появляется в Быстрой настройке, и эти элементы настроены.

- Время/Дата
- Интерфейсы/Маски в **Configuration> Interfaces** (public=10.0.0.1/24, private=172.16.124.1/24)
- Шлюз по умолчанию в **Configuration> System> IP-маршрутизация> Default_Gateway** (10.0.0.2)

На этом этапе Концентратор VPN доступен через HTML от внутренней сети.

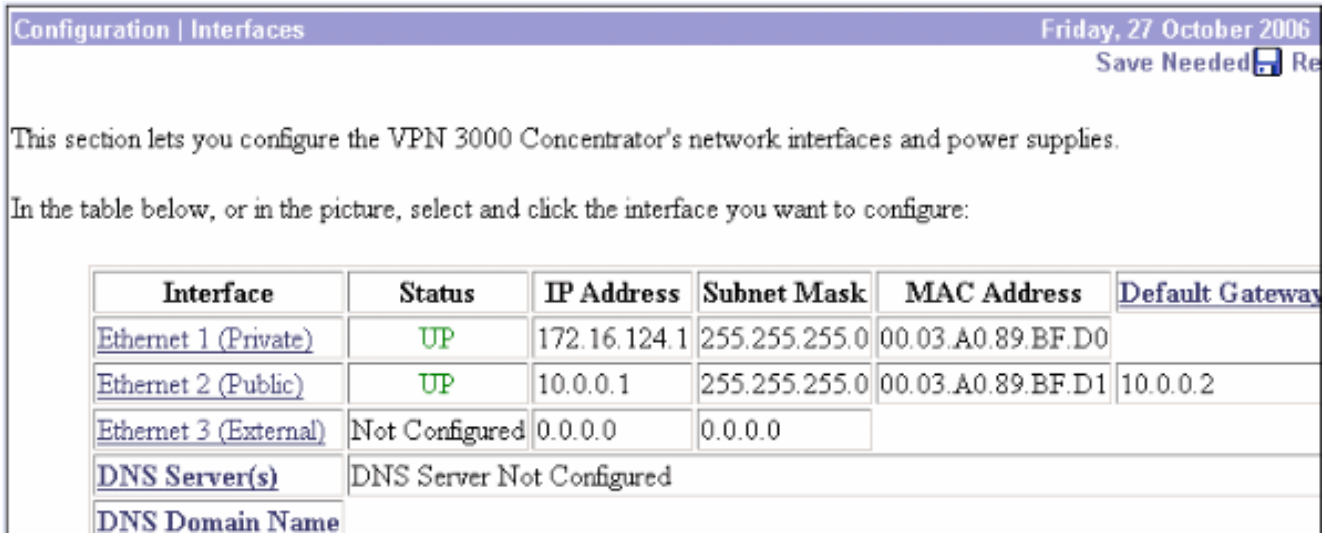
Примечание: Если Концентратором VPN управляют снаружи, вы также выполняете эти шаги:

1. Выберите **Configuration>, 1 интерфейс> C 2 общественностью> 4 - Выбирает IP Filter> 1. Частный (По умолчанию)**.
2. Выберите **Administration> 7 прав доступа> 2 списка контроля доступа> 1 add manager workstation** для добавления IP-адреса внешнего менеджера.

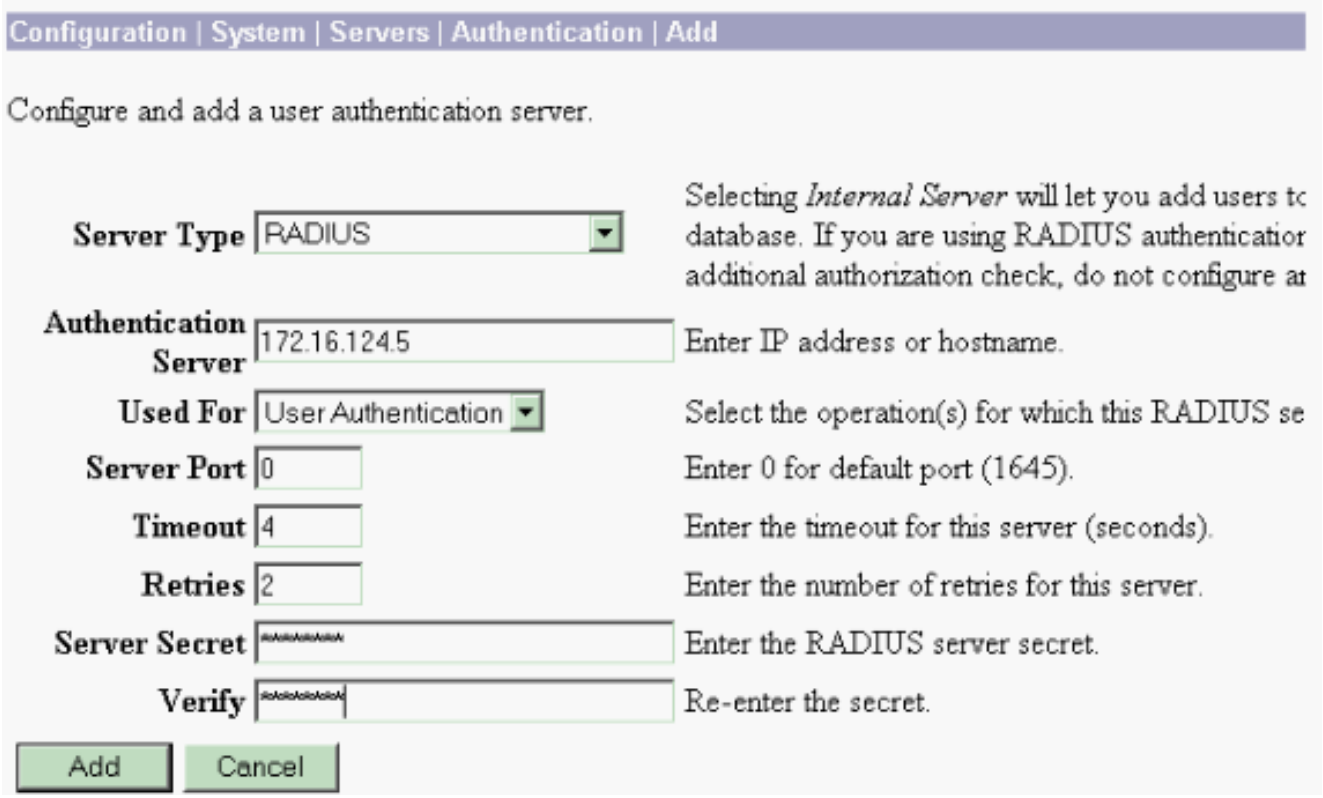
Эти шаги только требуются при управлении Концентратором VPN снаружи.

Как только вы выполнили эти два шага, остаток конфигурации может быть сделан через GUI при помощи web-браузера и соединяющийся с IP интерфейса, который вы просто настроили. В данном примере и на этом этапе, Концентратор VPN доступен через HTML от внутренней сети:

1. Выберите **Configuration> Interfaces** для перепроверки интерфейсов после внедрения GUI.

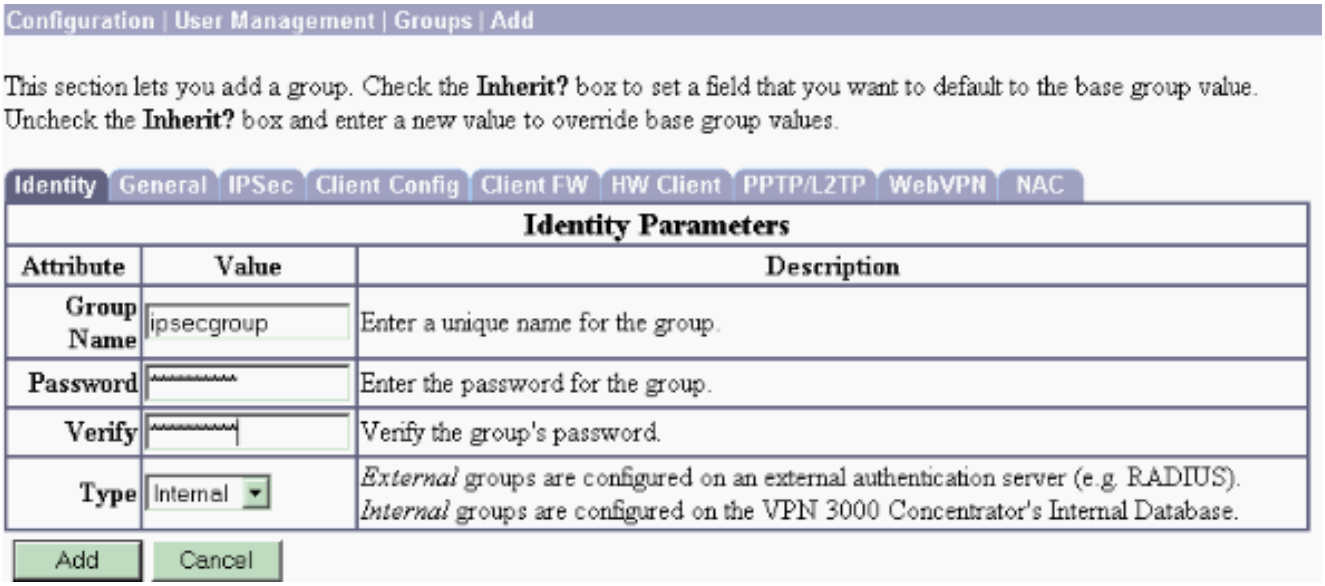


2. Выполните эти шаги для добавления Cisco Secure ACS для Сервера Windows Radius к конфигурации VPN 3000 Concentrator.Выберите **Configuration> System> Servers> Authentication** и **нажмите Add** из левого меню.

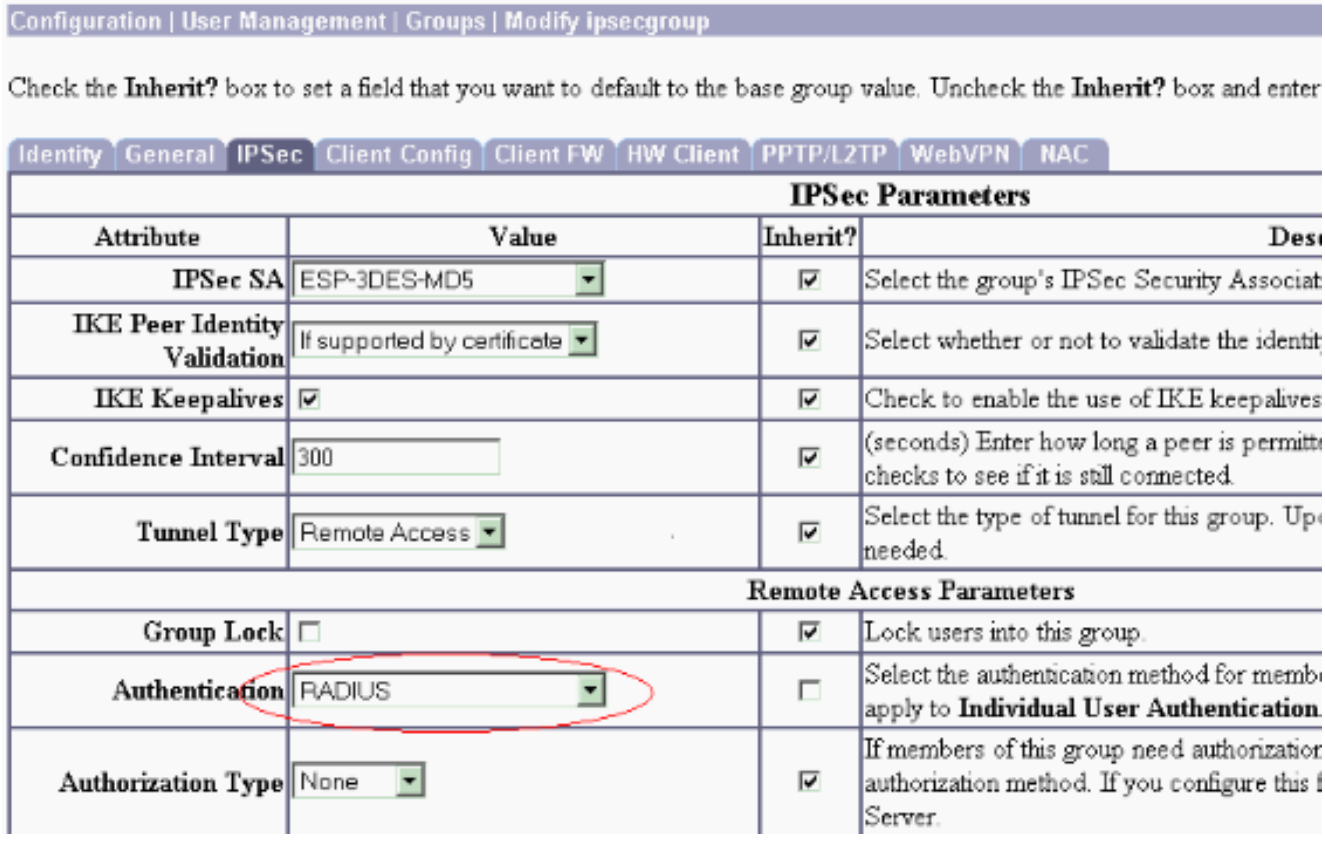


Выберите **тип сервера Radius** и добавьте эти параметры для своего Cisco Secure ACS для Сервера Windows Radius. Оставьте все другие параметры в их состоянии по умолчанию.**Сервер проверки подлинности** — Вводит IP-адрес вашего Cisco Secure ACS для Сервера Windows Radius.**Секретный сервер** — Вводит Секретный пароль сервера RADIUS. Это должно быть той же тайной, которую вы используете при настройке VPN 3000 Concentrator в Cisco Secure ACS для конфигурации Windows.**Проверка** пароль для подтверждения.Это добавляет сервер проверки подлинности в глобальной конфигурации VPN 3000 Concentrator. Этот сервер используется всеми группами за исключением того, когда был в частности определен сервер проверки подлинности. Если сервер проверки подлинности не настроен для группы, он возвращается к серверу глобальной аутентификации.

3. Выполните эти шаги для настройки Туннельной группы на VPN 3000 Concentrator.**Choose Configuration> User Management> Groups** из левого меню и **нажмите Add**.Измените или добавьте эти параметры во Вкладках конфигурация. Не нажимайте Apply, пока вы не измените все эти параметры:**Примечание:** Эти параметры являются минимумом, необходимым для соединений VPN для удаленного доступа. Эти параметры также предполагают, что не были изменены настройки по умолчанию в Базовой группе на VPN 3000 Concentrator.**Identity**

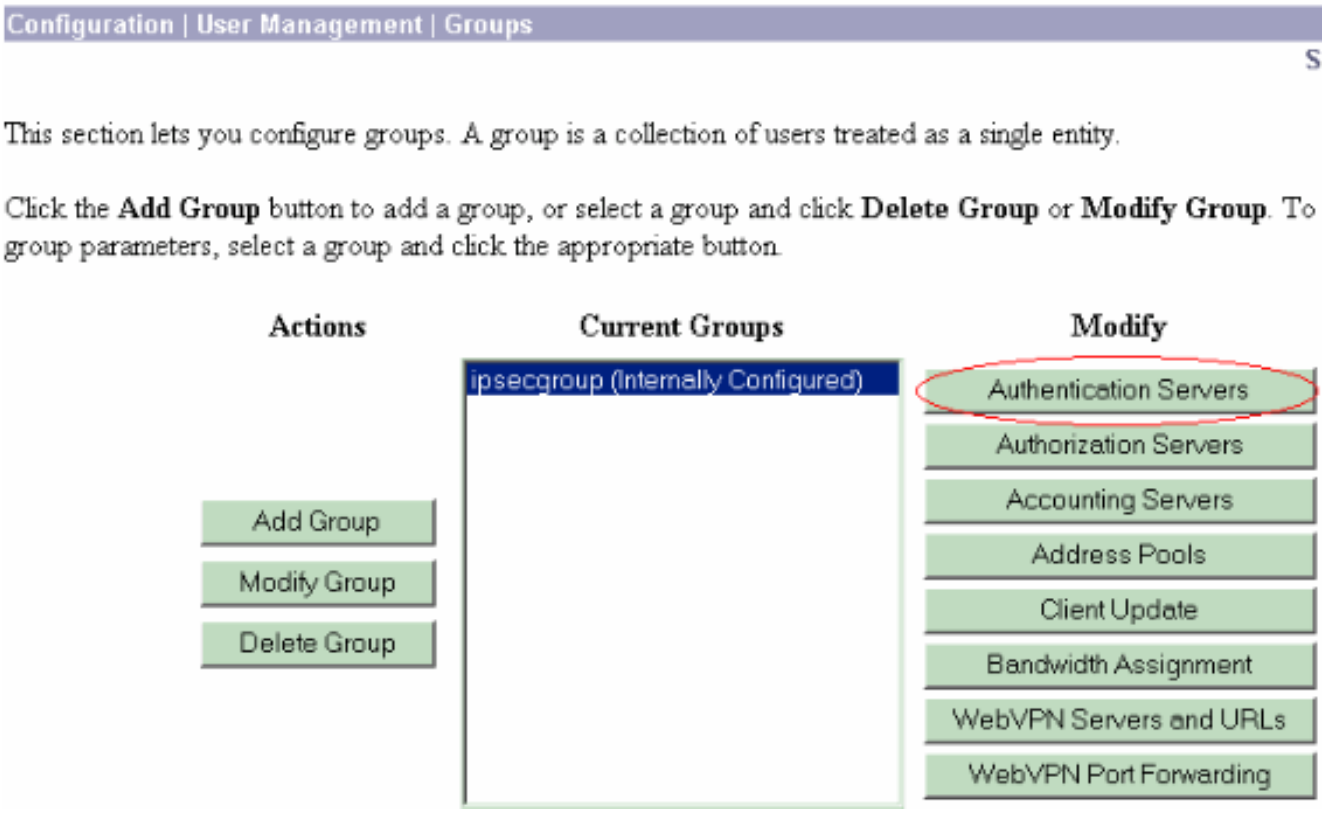


Имя группы — Тип имя группы. Например, IPsecUsers.**Пароль** — Вводит пароль для группы. Это - предварительный общий ключ для сеанса IKE.**Проверка** пароль для подтверждения.**Введите** — Выход это как по умолчанию: Внутренний.**IPSec**



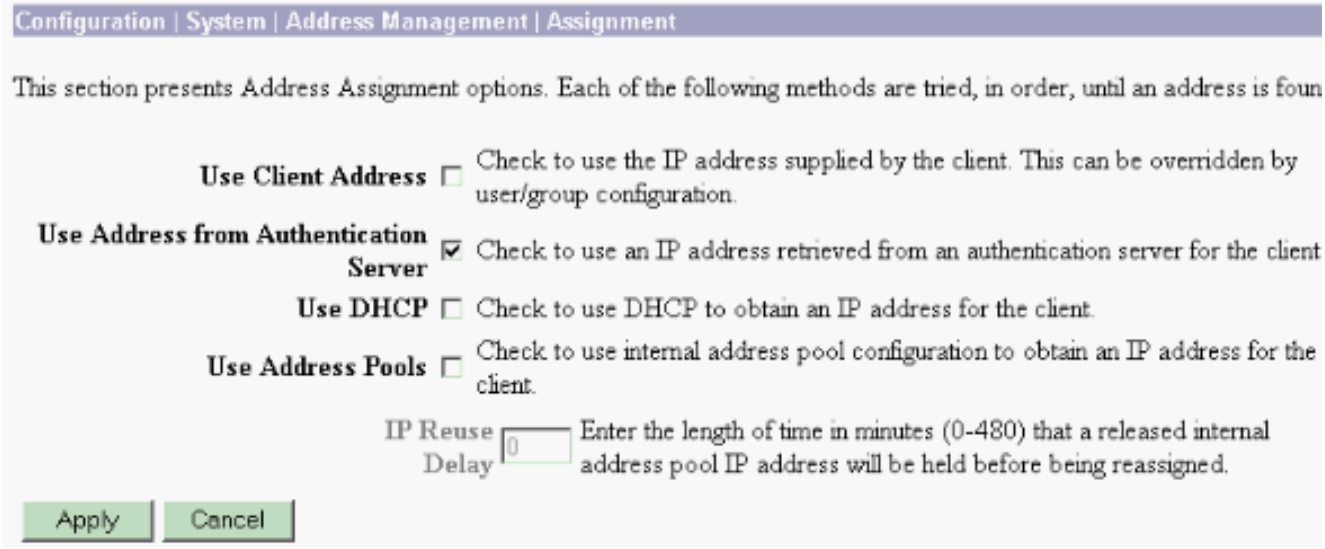
Тип туннеля — выбирает **удаленный доступ**.**Аутентификация** — RADIUS. Это говорит концентратору VPN, какой метод нужно использовать для того чтобы опознать пользователя.**Настройка режима** — проверяет **настройку режима**.**Щелкните "Применить".**

4. Выполните эти шаги для настройки серверов несколько серверов проверок подлинности на VPN 3000 Concentrator.Как только группа определена, выделите ту группу и нажмите **Authentication Servers** под столбцом Modify. Даже если эти серверы не существуют в глобальных серверах, отдельные серверы проверки подлинности могут быть определены для каждой группы.



Выберите **тип сервера Radius** и добавьте эти параметры для своего Cisco Secure ACS для Сервера Windows Radius. Оставьте все другие параметры в их состоянии по умолчанию.**Сервер проверки подлинности** — Вводит IP-адрес вашего Cisco Secure ACS для Сервера Windows Radius.**Секретный сервер** — Вводит Секретный пароль сервера RADIUS. Это должно быть той же тайной, которую вы используете при настройке VPN 3000 Concentrator в Cisco Secure ACS для конфигурации Windows.**Проверка** пароль для подтверждения.

5. Выберите **Configuration> System> Address Management> Assignment** и проверьте **Адрес Использования от Сервера проверки подлинности** для присвоения IP-адреса на Клиенты VPN от пула IP, созданного в сервере RADIUS, как только аутентифицируется клиент.



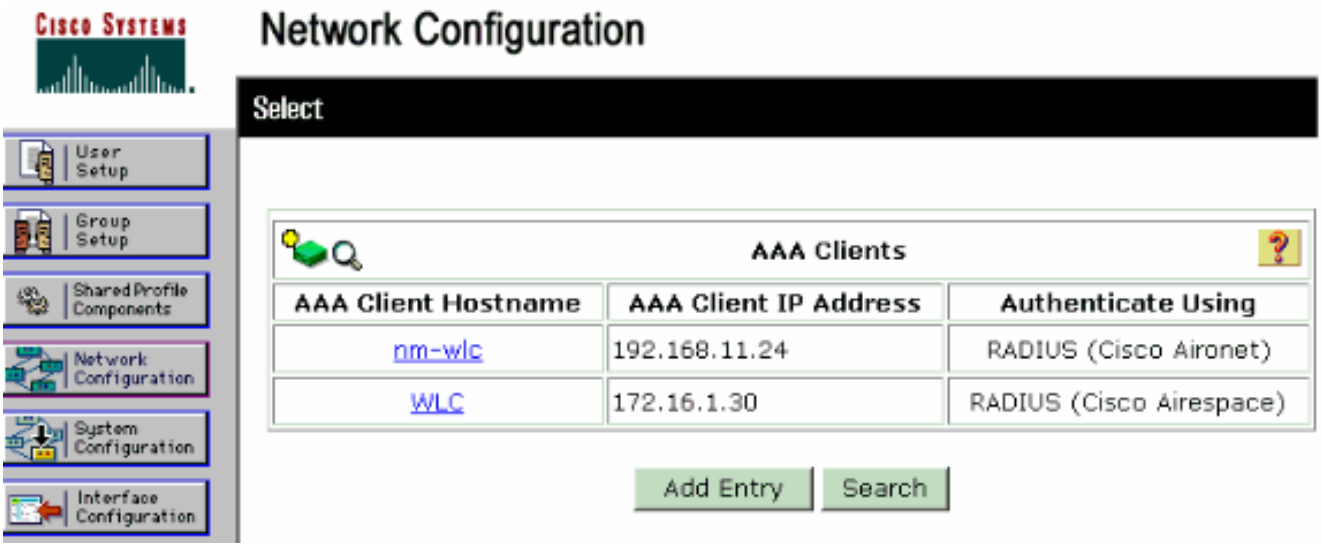
Конфигурация сервера RADIUS

Этот раздел документа описывает процедуру, требуемую настраивать Cisco Secure ACS как сервер RADIUS для аутентификации Пользователя VPN-клиента, переданной

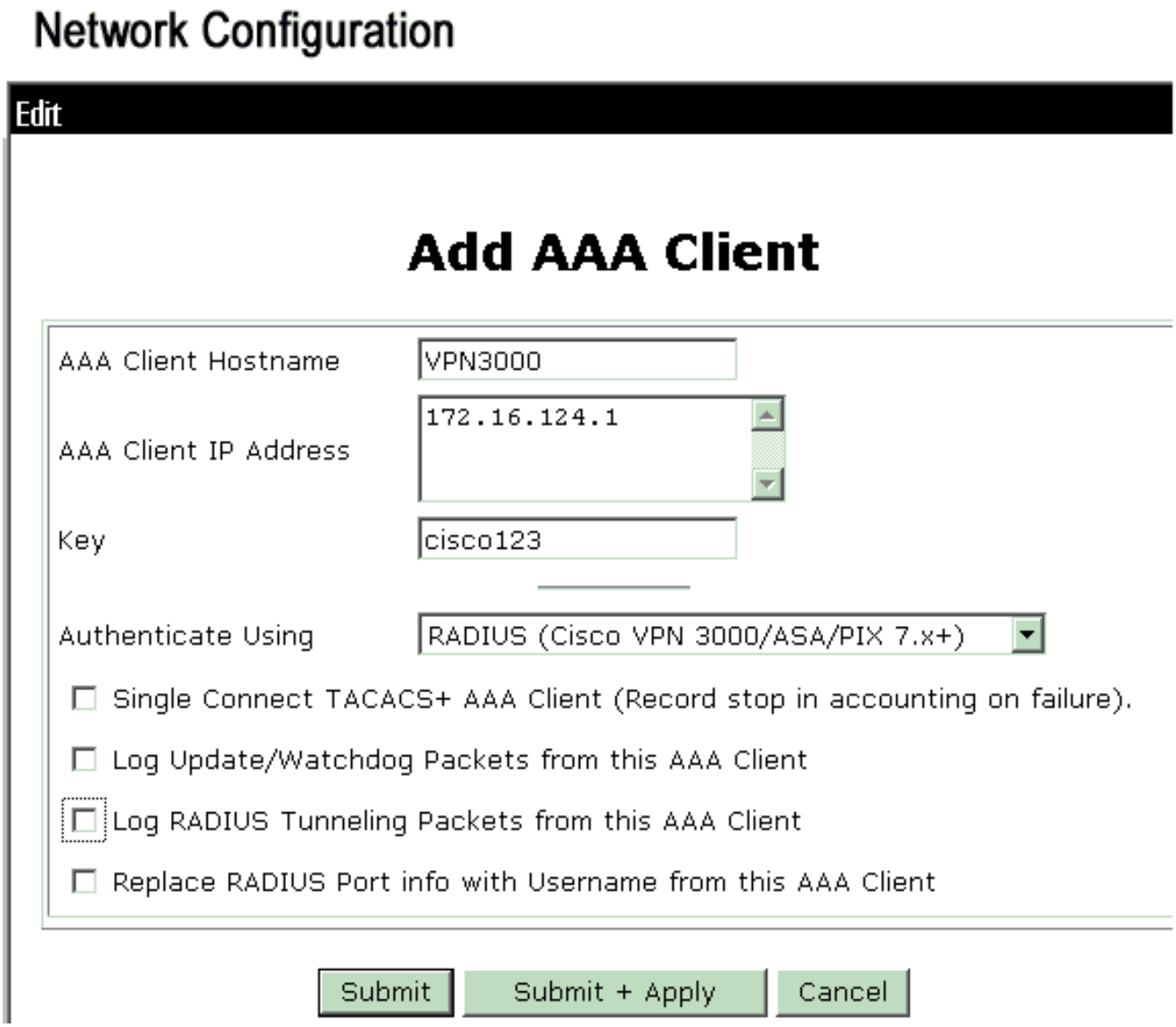
концентратором Cisco VPN серии 3000 - клиент AAA.

Дважды нажмите **значок ACS Admin** для начала сеанса admin на ПК, который выполняет Cisco Secure ACS для Сервера Windows Radius. Войдите с правильным именем пользователя и паролем при необходимости.

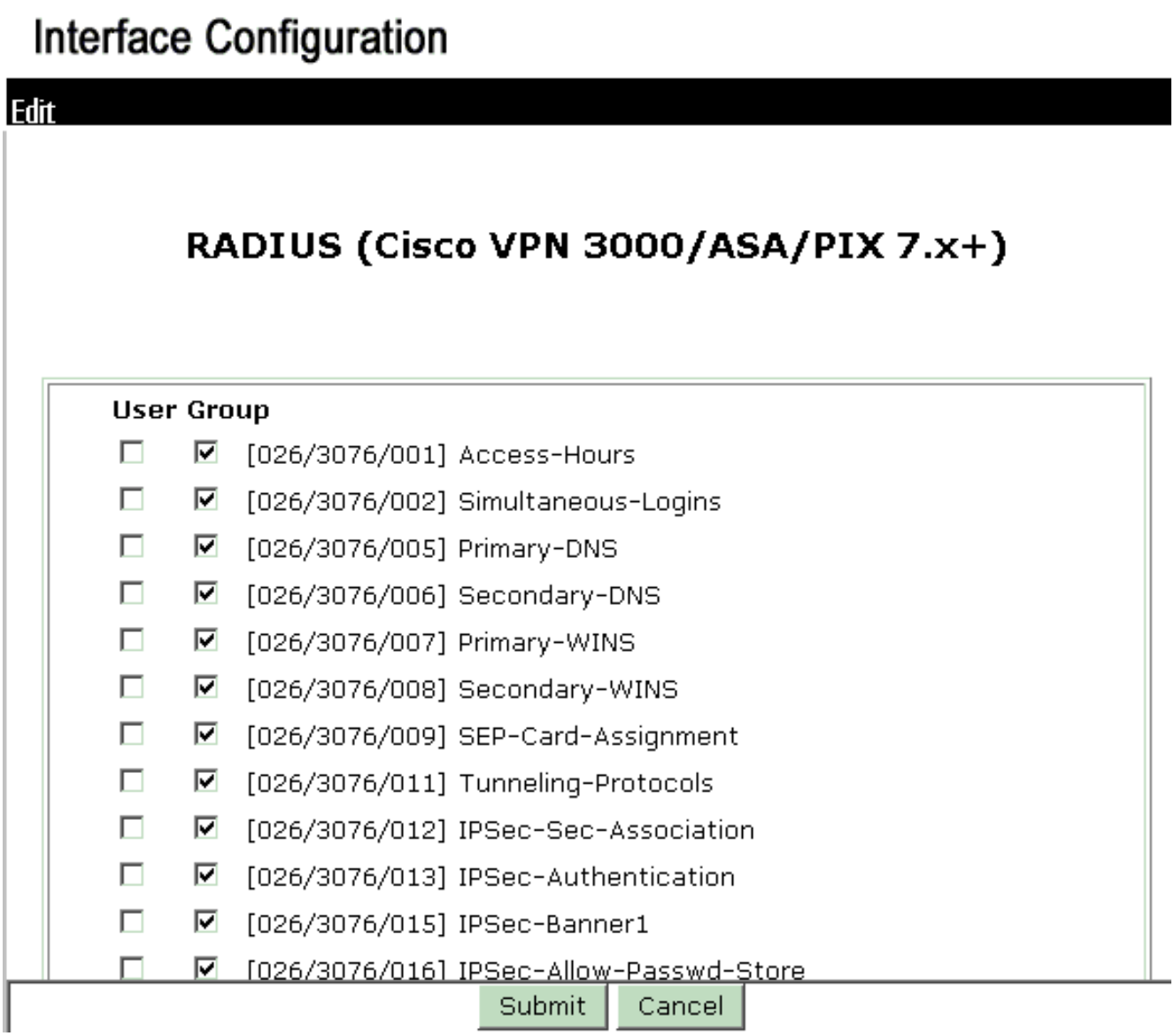
1. Выполните эти шаги для добавления VPN 3000 Concentrator к Cisco Secure ACS для конфигурации Windows Server.Выберите **Network Configuration** и **нажмите Add Запись** для добавления клиента AAA к серверу RADIUS.



Добавьте эти параметры для своего VPN 3000 Concentrator:

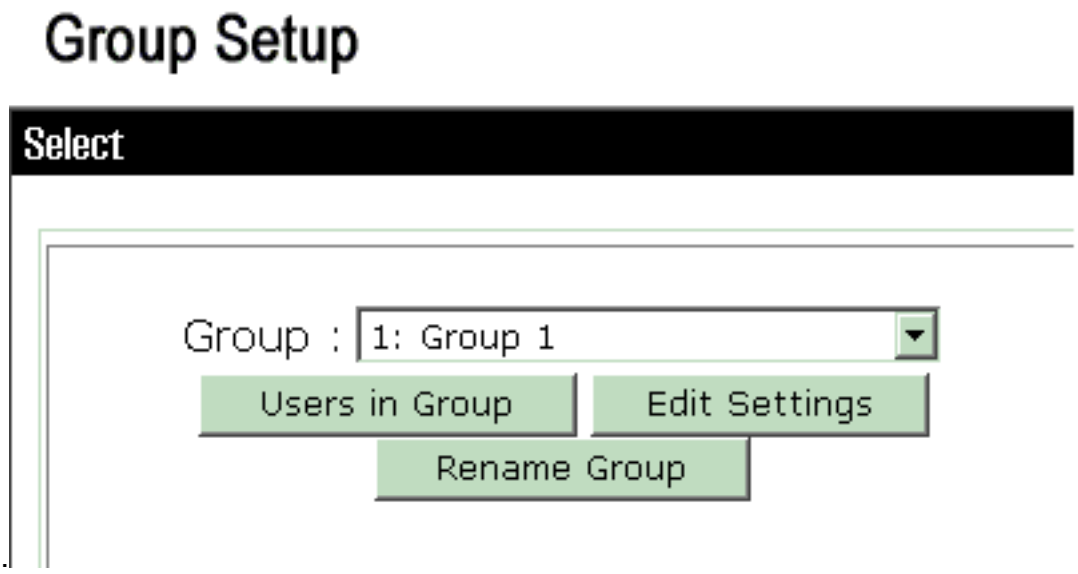


Имя хоста для клиента AAA — Вводит имя хоста вашего VPN 3000 Concentrator (для Разрешения DNS).**IP-адрес клиента AAA** — Вводит IP-адрес вашего VPN 3000 Concentrator.**Ключ** — Вводит Секретный пароль сервера RADIUS. Это должно быть той же тайной, которую вы настроили, когда вы добавили Сервер проверки подлинности на Концентраторе VPN.**Используемая аутентификация** — Выбирает **RADIUS (Cisco VPN 3000/ASA/PIX 7.x +)**. Это позволяет VSA VPN 3000 отображаться в окне Конфигурации группы.**Нажмите кнопку Submit (Отправить).**Выберите **Interface Configuration**, нажмите **RADIUS (Cisco VPN 3000/ASA/PIX 7.x +)** и проверьте **Группу [26] Определяемый поставщиком**.

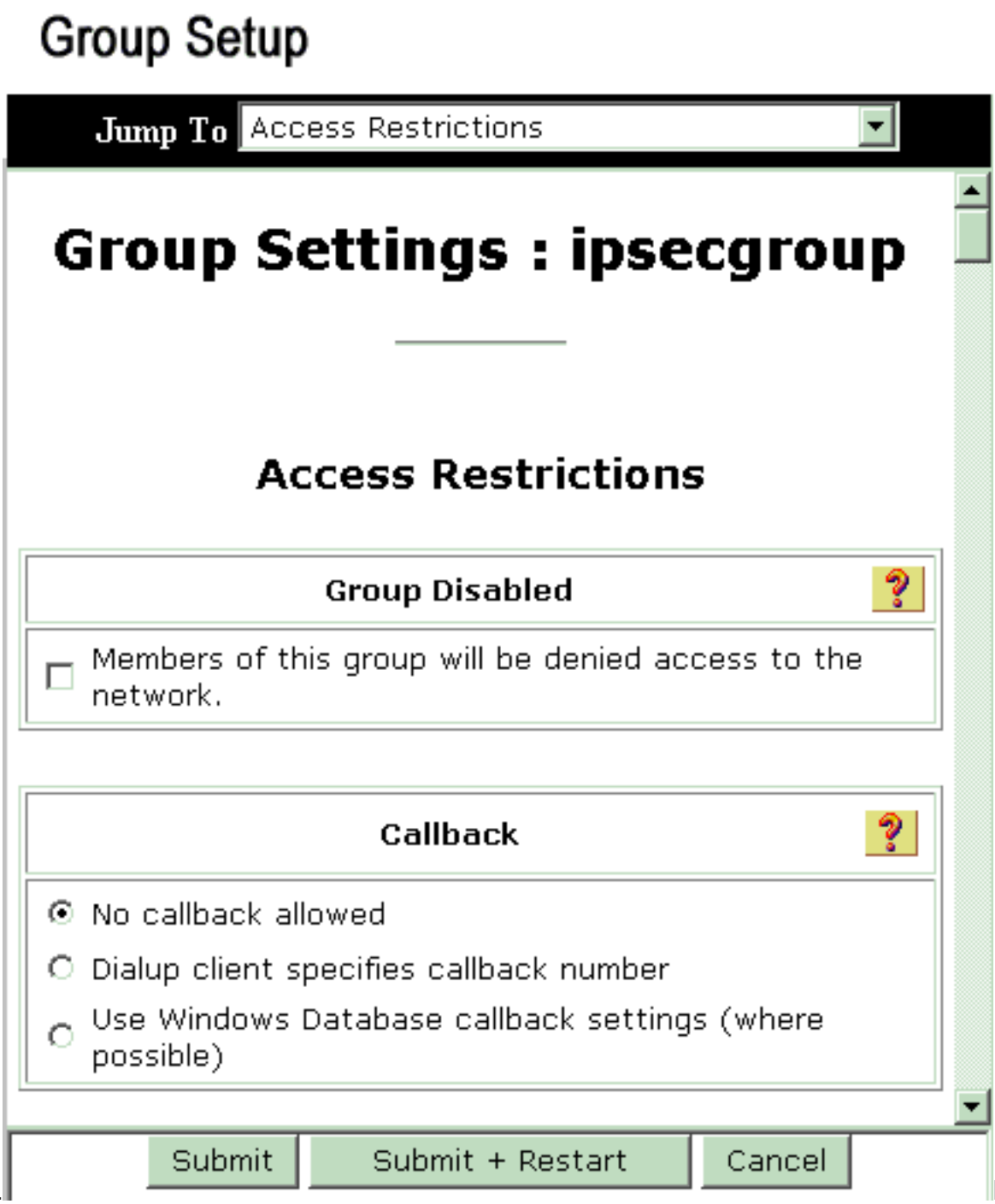


Примечание: 'Атрибут RADIUS 26' обращается ко всем определяемым поставщиком атрибутам. Например, выберите **Interface Configuration> RADIUS (Cisco VPN 3000)** и посмотрите, что все доступные атрибуты запускаются с 026. Это показывает, что все эти определяемые поставщиком атрибуты подпадают под РАДИУС IETF 26 стандартов. Эти атрибуты не обнаруживаются в Пользователе или Настройке групп по умолчанию. Для разоблачения в Настройке групп создайте клиента AAA (в этом VPN 3000 Concentrator случая), который аутентифицируется с RADIUS в конфигурации сети. Затем проверьте атрибуты, которые должны появиться в Настройке пользователя, Настройке групп или обоих от Конфигурации интерфейса.См. атрибуты RADIUS для получения дополнительной информации о доступных атрибутах и их использовании.**Нажмите кнопку Submit (Отправить).**

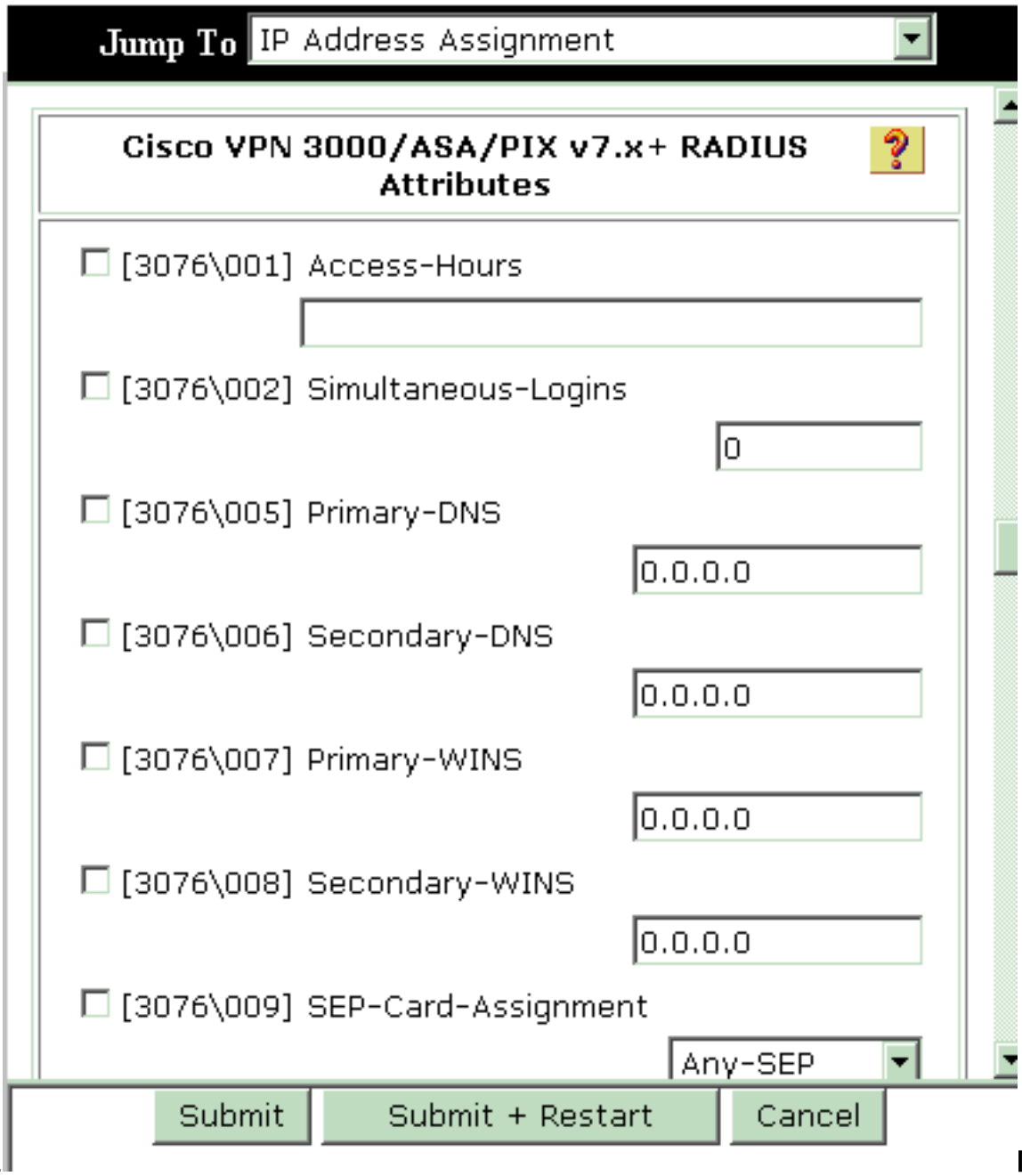
2. Выполните эти шаги для добавления групп к Cisco Secure ACS для конфигурации Windows.Выберите **Group Setup**, затем выберите одну из групп шаблона, например, Группы 1, и нажмите **Rename**



Group. Помен
яйте имя на что-то соответствующее вашей организации., например, ipsecgroup. Так как пользователи добавлены к этим группам, заставьте имя группы отразить фактическую цель той группы. Если все пользователи помещены в ту же группу, можно назвать ее VPN Users Group.Нажмите **Edit Settings** для редактирования параметров в недавно переименованной



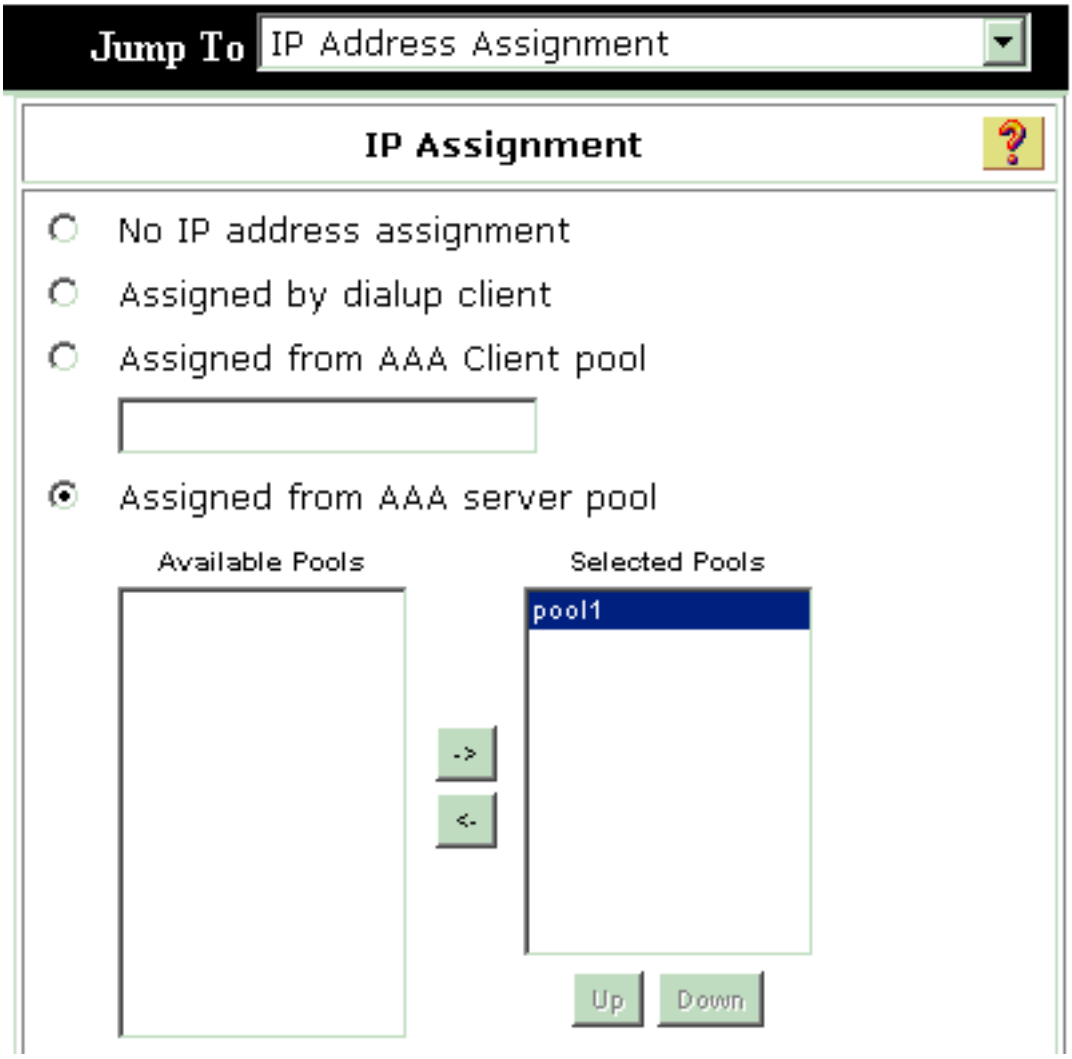
группе. На жмите **Cisco VPN 3000 RADIUS** и настройте эти рекомендуемые атрибуты. Это позволяет пользователям, назначенным на эту группу наследовать атрибуты RADIUS Cisco VPN 3000, который позволяет вам централизовать политику для всех пользователей в Cisco Secure ACS для



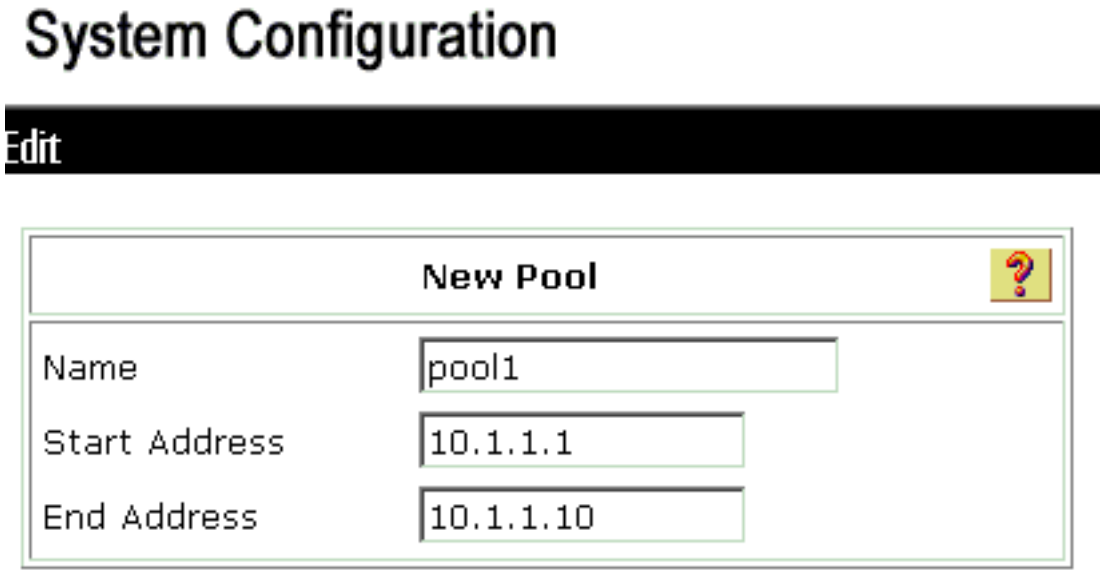
Windows. **Пр**

имечание: Технически, атрибуты RADIUS VPN 3000 не требуются, чтобы быть настроенными, пока Туннельная группа установлена в шаге 3 Конфигурации Концентратора серии VPN 3000, и Базовая группа в Концентраторе VPN не изменяется от исходных настроек по умолчанию.**Рекомендуемые атрибуты VPN 3000:Основной DNS** — Вводит IP-адрес вашего Основного сервера DNS.**Вторичный DNS** — Вводит IP-адрес вашего Дополнительного DNS - сервера.**Основной WINS** — Вводит IP-адрес вашего Основного сервера WINS.**Вторичный WINS** — Вводит IP-адрес вашего дополнительного сервера WINS.**Протоколы туннелирования** — Выбирают **IPsec**. Это позволяет *только* соединения Клиента IPSEC. PPTP или L2TP не позволены.**АССОЦИАЦИЯ СЕК. IPSEC** — Введите **ESP-3DES-MD5**. Это гарантирует все ваше подключение Клиентов IPSEC доступным шифрованием с наивысшей стойкостью.**IPsec-Allow-Password-Store** — Выберите **Disallow**, таким образом, пользователям *не* разрешают сохранить их пароль в Клиенте VPN.**IPsec-Banner** — Введите заголовок с приветственным сообщением, который будет представлен пользователю на соединение. Например, "Добро пожаловать в доступ VPN сотрудника

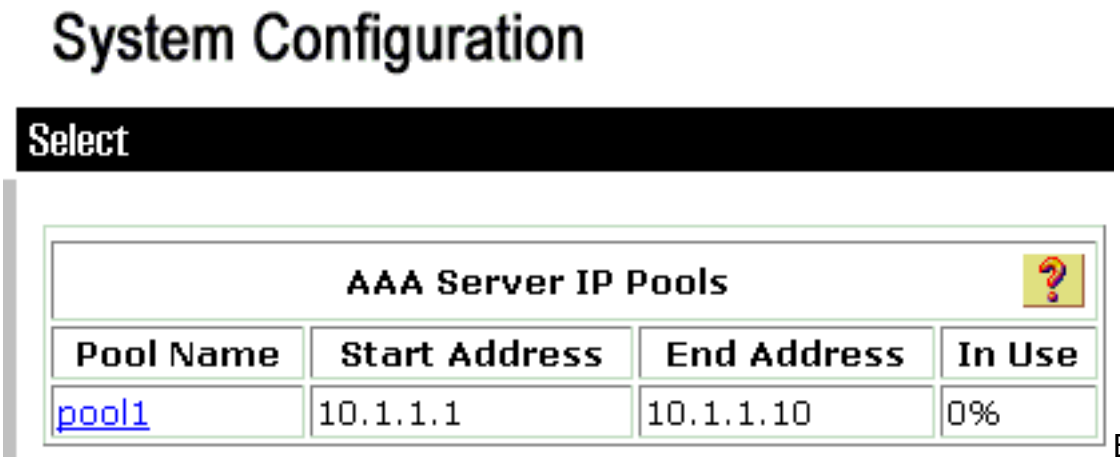
MyCompany!"**Домен по умолчанию ipsec —** Вводит доменное имя вашей компании. Например, "mycompany.com".Этот набор атрибутов не необходим. Но если вы не уверены, если Атрибуты базовой группы VPN 3000 Concentrator изменились, то Cisco рекомендует настроить эти атрибуты:**Одновременные входы в систему** — Вводят число раз, в которое вы позволяете пользователю одновременно входить с том же имя пользователя. Рекомендация равняется 1 или 2.**Назначение карты SEP** — выбирает **Any-SEP**.**Mode-Config ipsec** — выбирает **ON**.**IPsec по UDP** — Выбирает **OFF**, пока вы не хотите, чтобы пользователи в этой группе подключили IPsec использования по протоколу UDP. При выборе ON VPN Client все еще имеет способность локально отключить IPsec по UDP и подключению обычно.**IPsec по порту UDP** — Выбирает Номер порта UDP в диапазоне 4001 - 49151. Это используется, только если идет IPsec по UDP.Следующий набор атрибутов требует, чтобы вы настроили что-то на Концентраторе VPN сначала, прежде чем можно будет использовать их. Это только рекомендуется для опытных пользователей.**Пункты меню Access Hours (Часы доступа)** — Это требует, чтобы вы установили диапазон Пунктов меню Access Hours (Часы доступа) на VPN 3000 Concentrator под **Configuration> Policy Management**. Вместо этого используйте Пункты меню Access Hours (Часы доступа), доступные в Cisco Secure ACS для Windows для управления этим атрибутом.**IPsec-Split-Tunnel-List** — Это требует, чтобы вы установили Список сети на Концентраторе VPN под **Configuration> Policy Management> Traffic Management**. Это - список сетей, передаваемых вниз клиенту, которые говорят клиенту шифровать данные к только тем сетям в списке.Выберите **присвоение IP в Настройке групп** и проверьте **Назначенный от Пула AAA-сервера** для присвоения IP-адресов на Пользователей VPN-клиента, как только они, аутентифицируются.



Выберите **Конфигурацию системы> пулы IP**, чтобы создать пул IP для Пользователей VPN-клиента и нажать

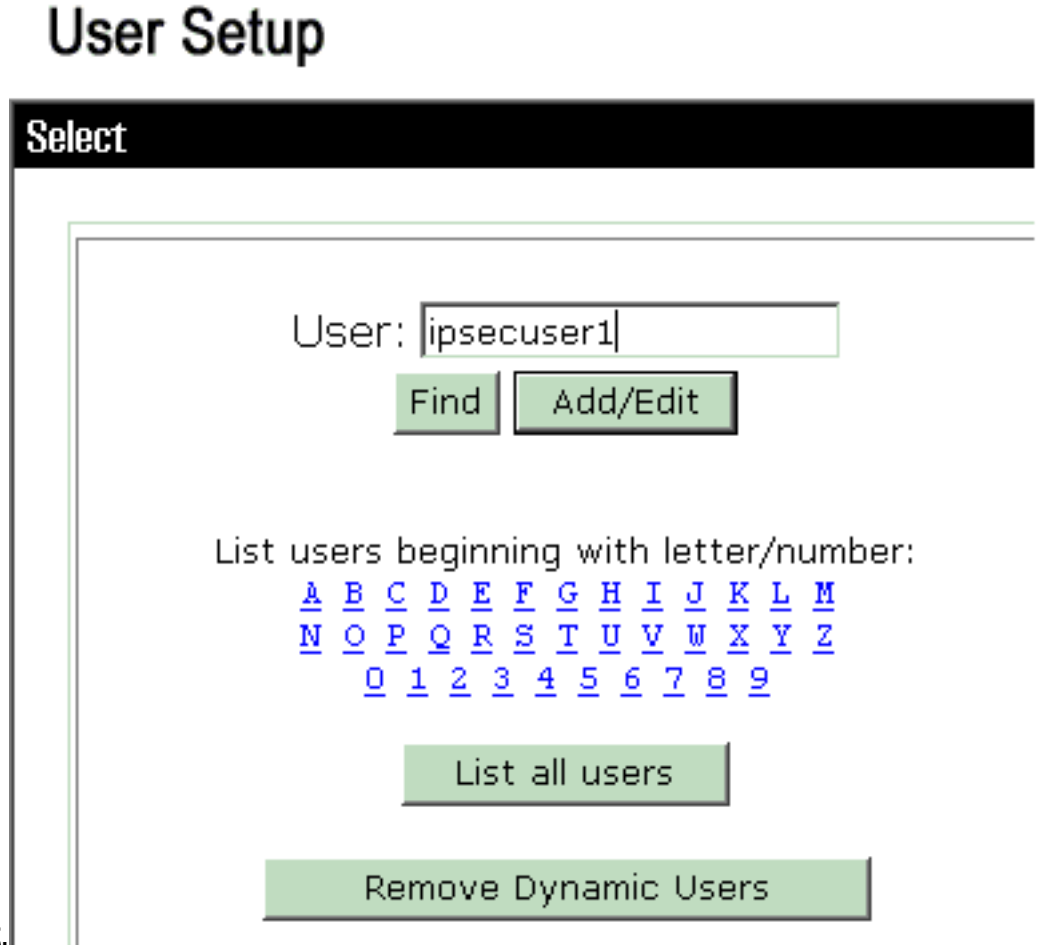


Submit.

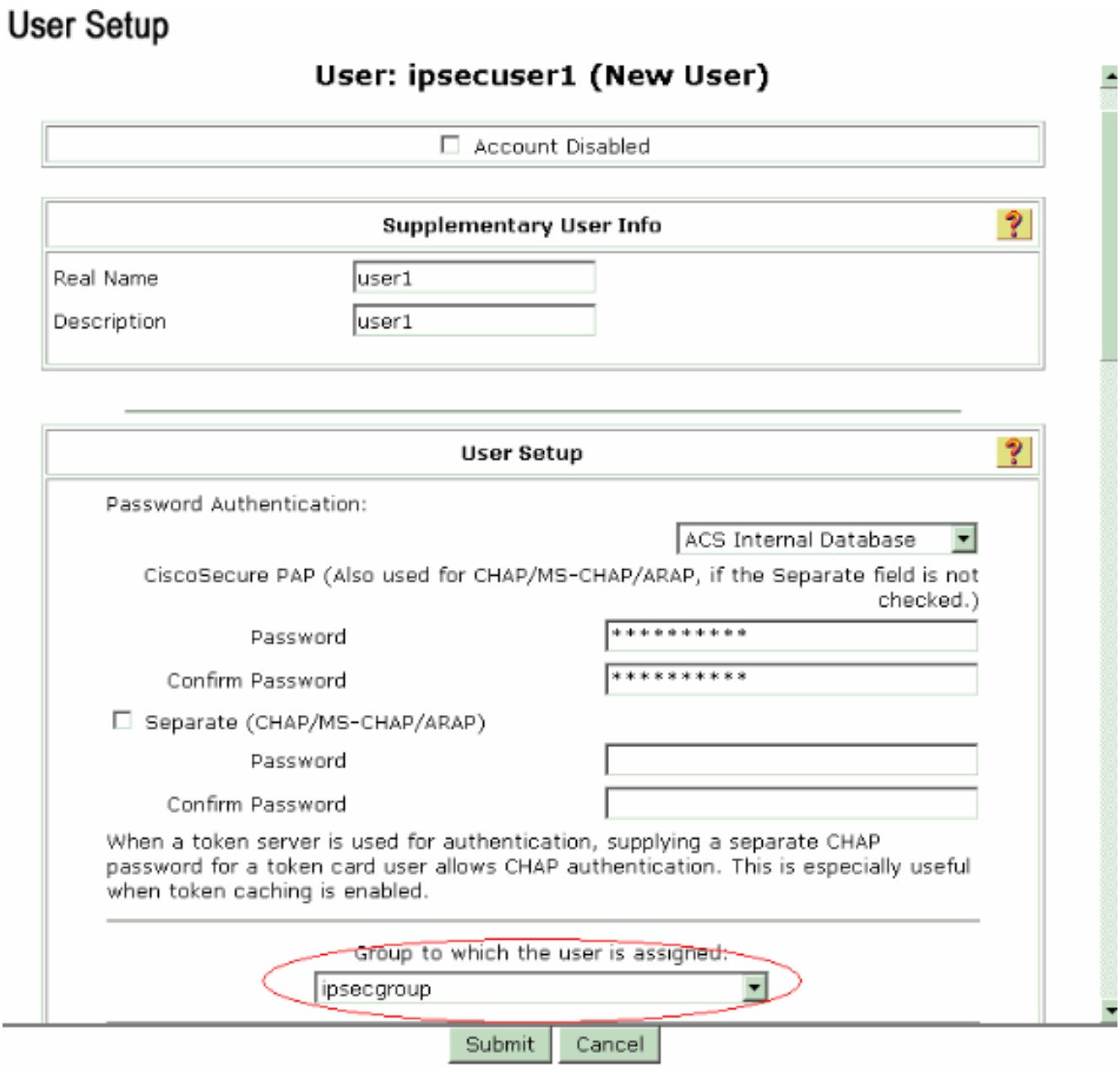


Выберите **Submit> Restart**, чтобы сохранить конфигурацию и активировать новую группу.Повторите эти шаги для добавления больших групп.

3. **Настройте пользователей на Cisco Secure ACS для Windows.**Выберите **User Setup**, введите имя пользователя и нажмите



Add/Edit. Настройте эти параметры под разделом настройки пользователя:

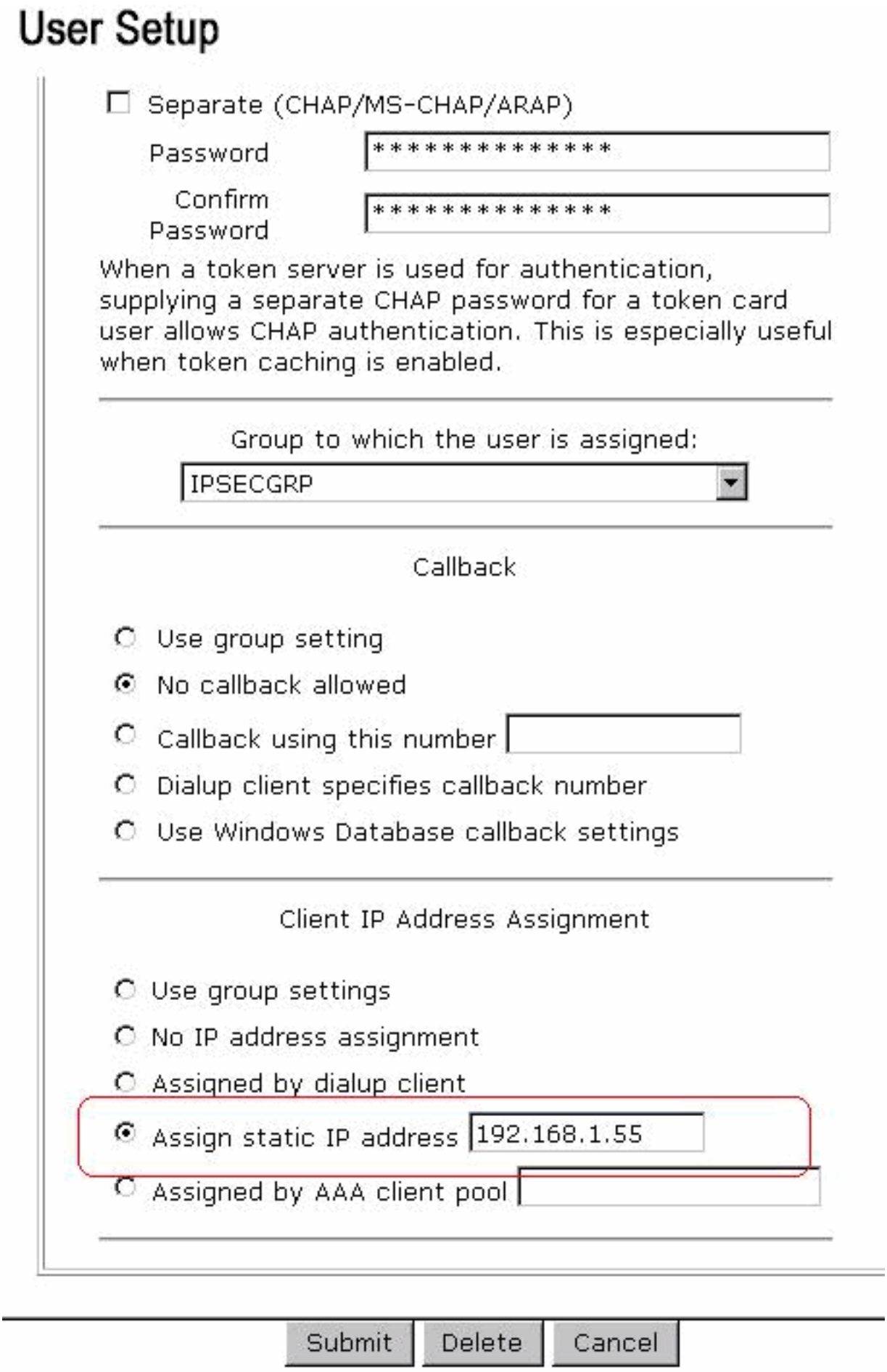


Проверка подлинности с помощью пароля — выбирает **внутреннюю базу данных ACS**.**PAP Cisco Secure - Пароль** — Вводит пароль для пользователя.**PAP Cisco Secure - Подтверждает, что Пароль** — Повторно вводит пароль для нового пользователя.**Группа, на которую пользователю назначают** — Выбирает название группы, которую вы создали в предыдущем шаге.Нажмите **Submit**, чтобы сохранить и активировать параметры пользователя.Повторите эти шаги для добавления дополнительных пользователей.

Назначьте Статический IP - адрес на Пользователя VPN-клиента

Выполните следующие действия:

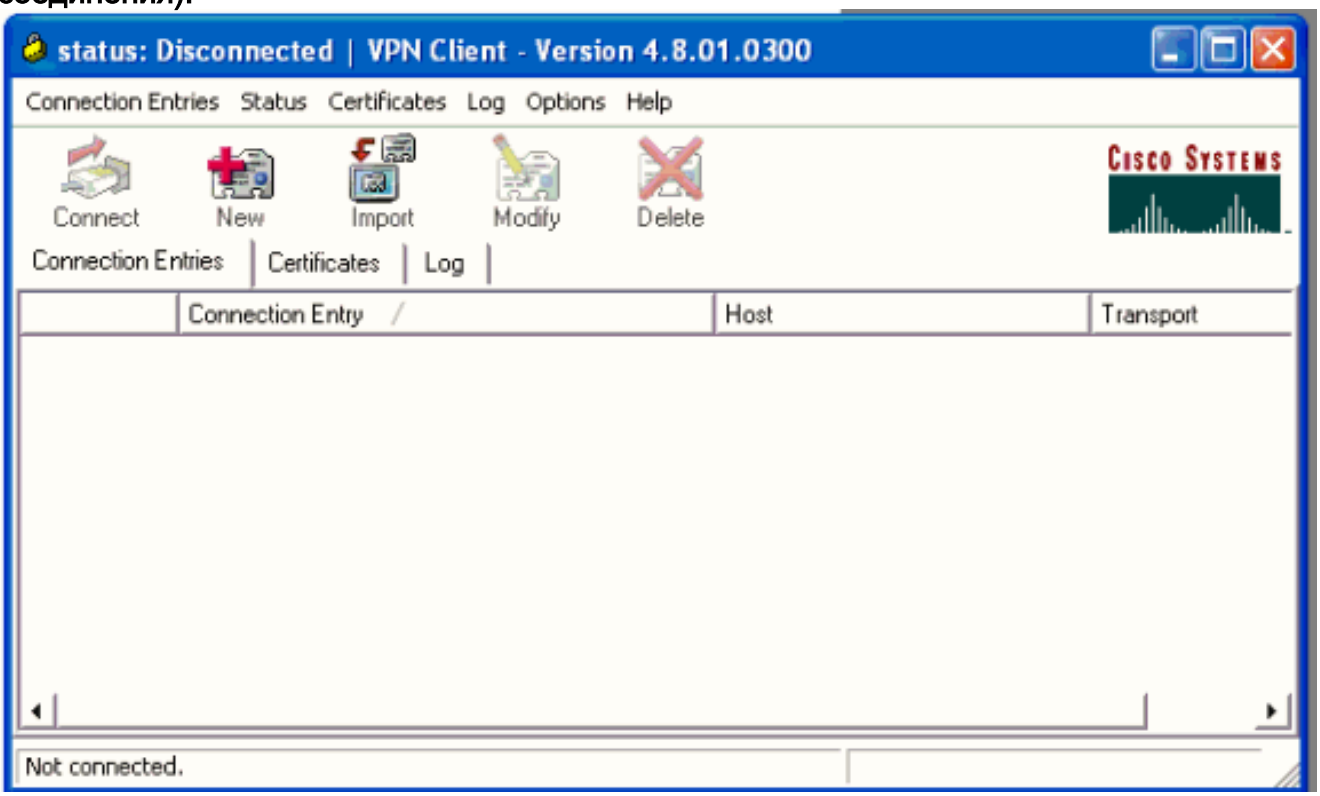
1. Создайте новую группу VPN IPSECGRP.
2. Создайте пользователя, который хочет получить статическое ip и выбрать **IPSECGRP**. Выберите **статический IP - адрес Assign** со статическим IP - адресом, который назначен под Присвоением IP-адреса
клиента.



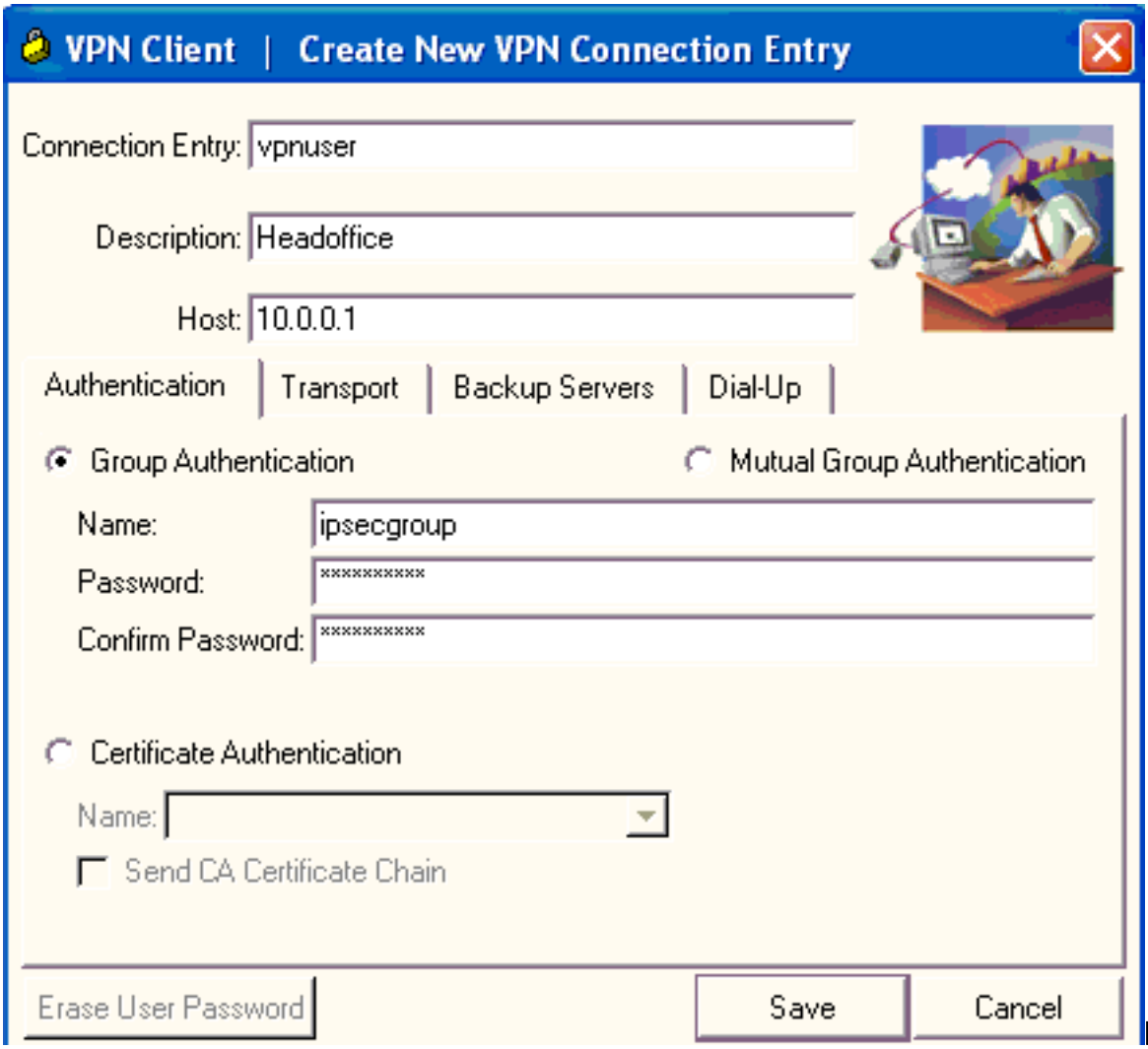
[Конфигурация клиента VPN]

В этом разделе описываются конфигурацию стороны Клиента VPN.

1. **Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client.**
2. **Нажмите New, чтобы открыть окно "Create New VPN Connection Entry" (Создание новой записи VPN-соединения).**



3. Получив соответствующий запрос, присвойте имя новому элементу. При необходимости можно также ввести описание. Задайте IP-адрес открытого интерфейса VPN 3000 Concentrator в столбце Host и выберите **Group Authentication**. Затем предоставьте имя группы и пароль. Нажмите **Save** для завершения новой записи VPN-подключения.

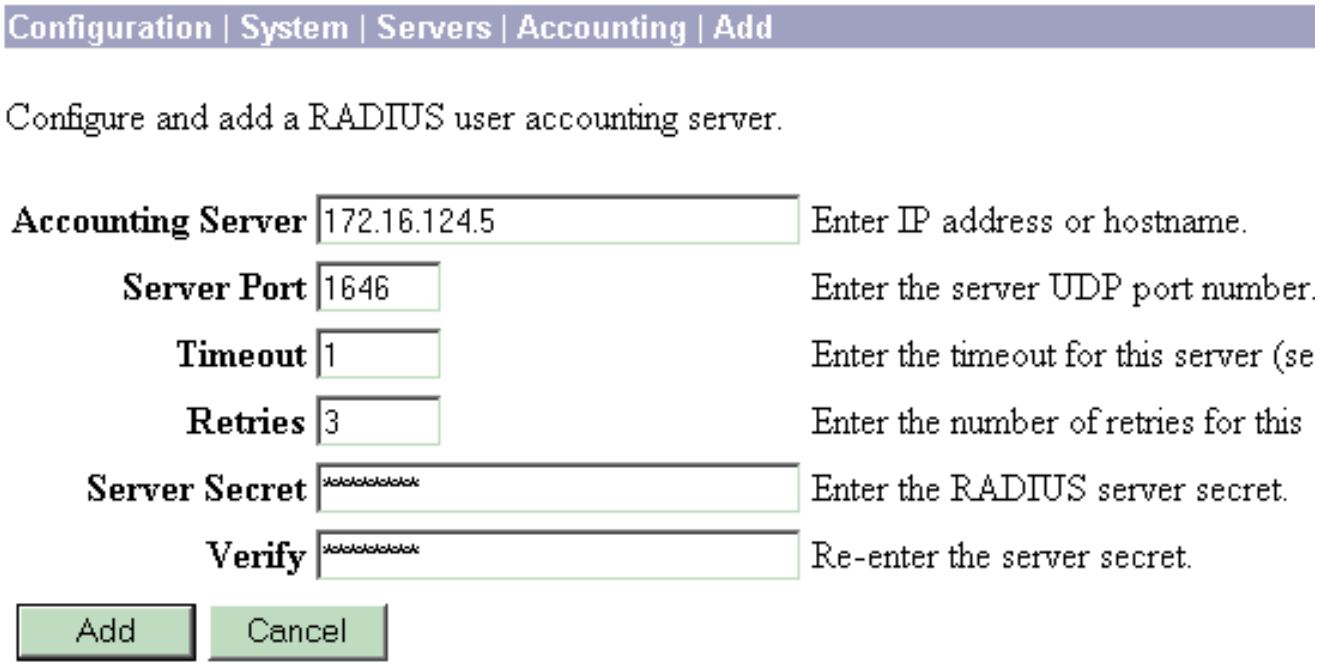


Примечание: Убедитесь, что Клиент VPN настроен для использования того же имени группы и пароля, настроенного в концентраторе Cisco VPN серии 3000.

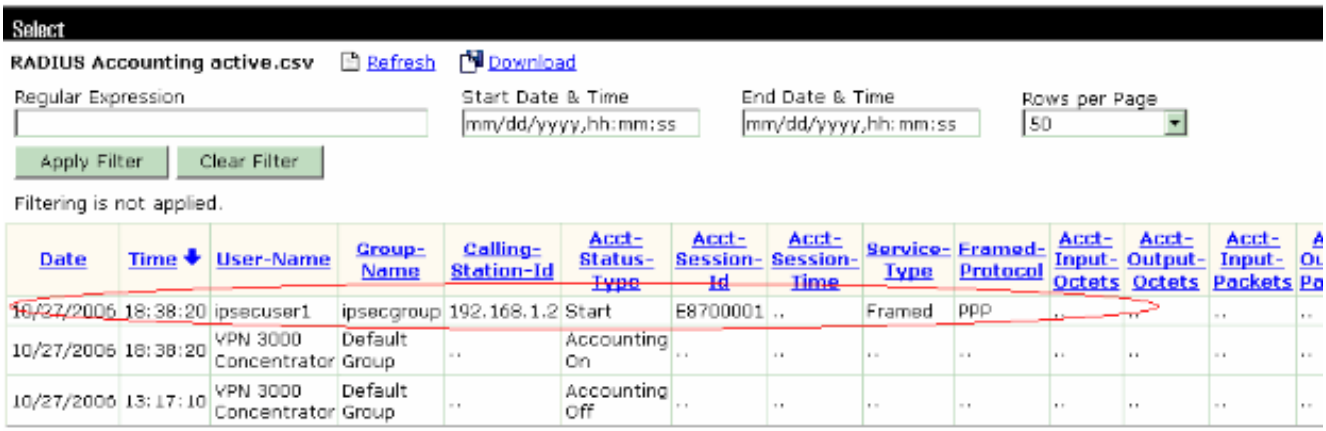
Добавление учета

После того, как аутентификация работает, можно добавить учет.

1. На VPN 3000 выберите **Configuration> System> Servers> Accounting Servers** и добавьте **Cisco Secure ACS для Windows Server**.
2. Можно добавить отдельные учетные серверы к каждой группе при выборе **Configuration> User Management> Groups** выделите группу и нажмите **Modify Acct. Серверы**. Затем введите IP-адрес учетного сервера с секретным сервером.



В Cisco Secure ACS для Windows учетные записи появляются как показано в выходных данных
ниже:



Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Проверьте концентратор VPN

На стороне VPN 3000 Concentrator выберите **Administration> Administer Sessions** для проверки удаленного установления VPN-туннеля.

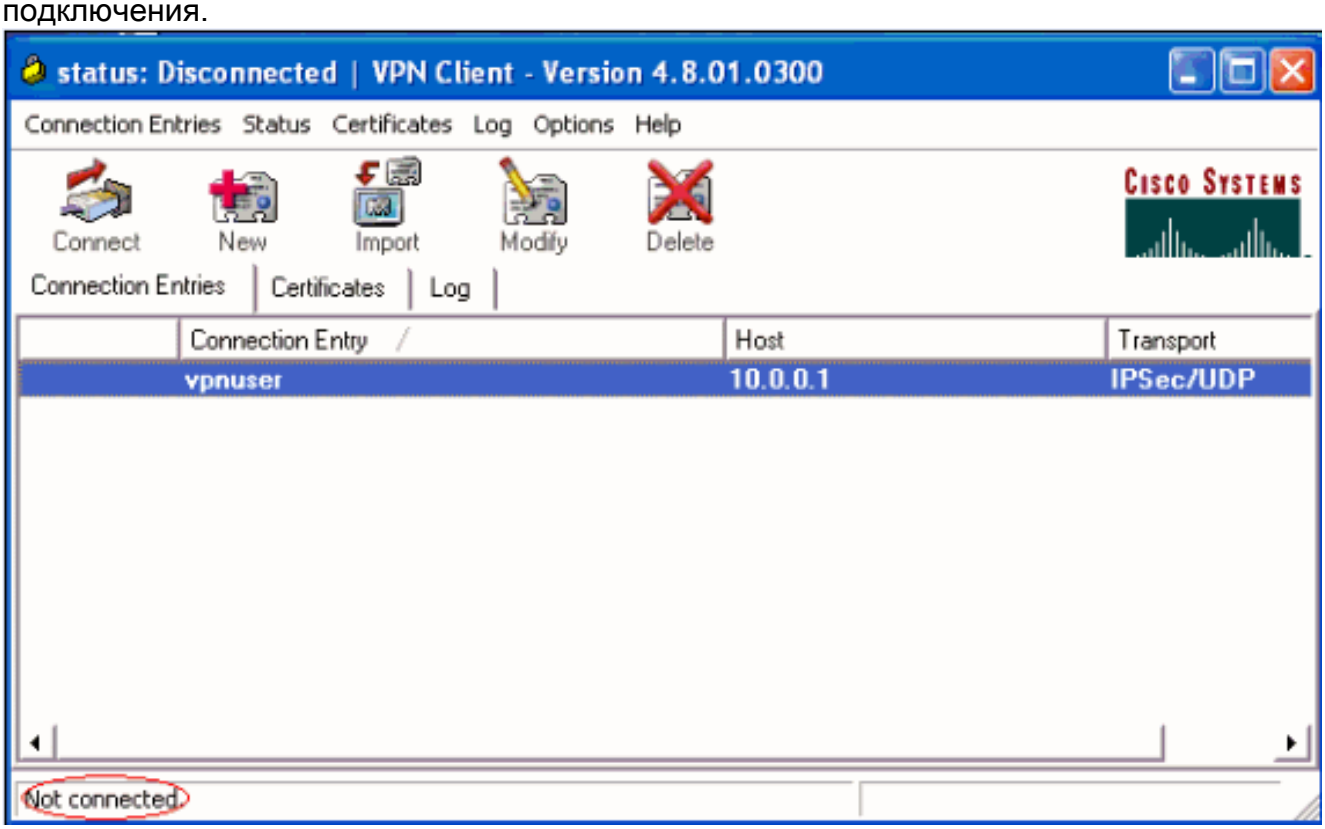
Remote Access Sessions [LAN-to-LAN Sessions | Management Sessions]

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]

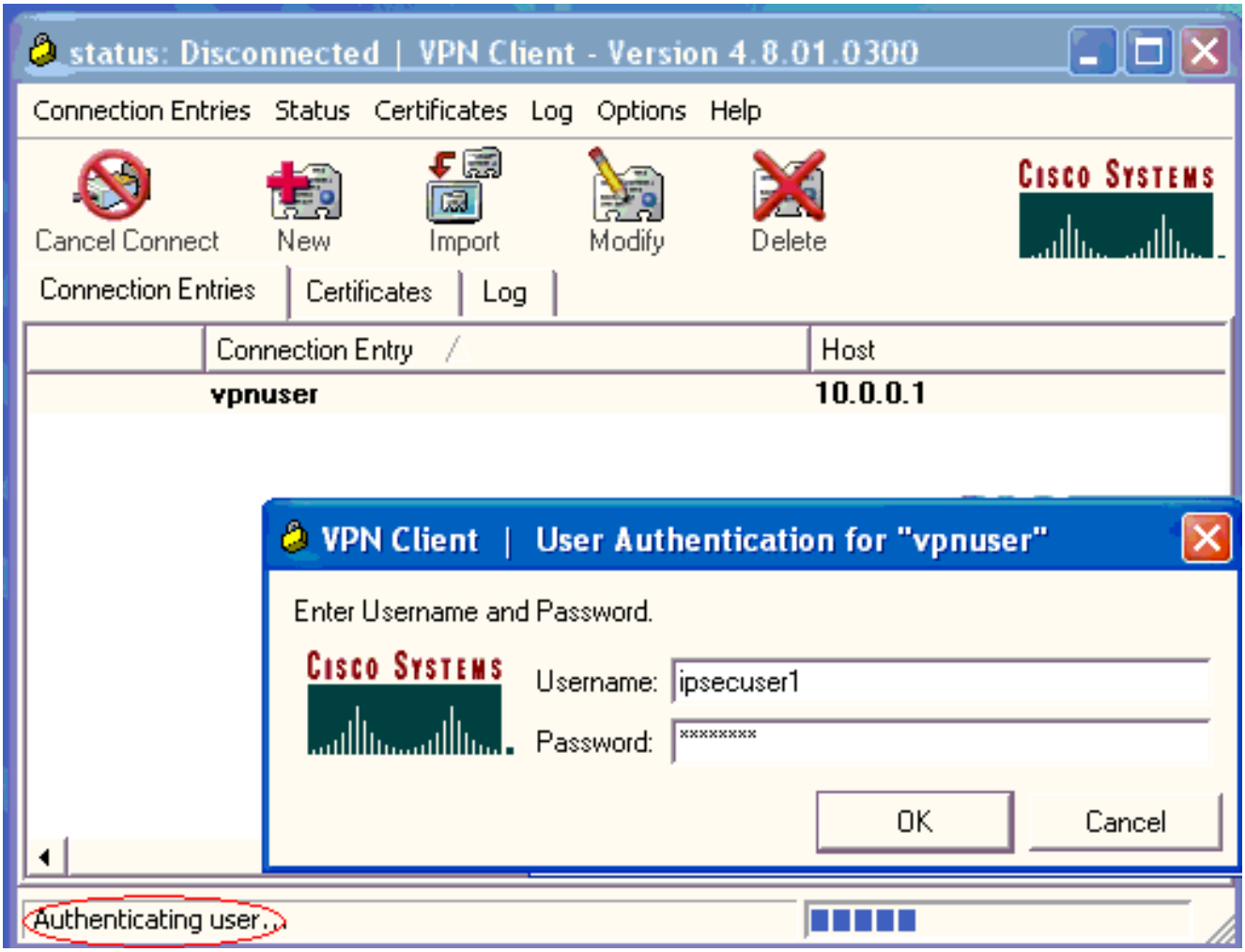
Проверьте клиент VPN

Выполните эти шаги для проверки Клиента VPN.

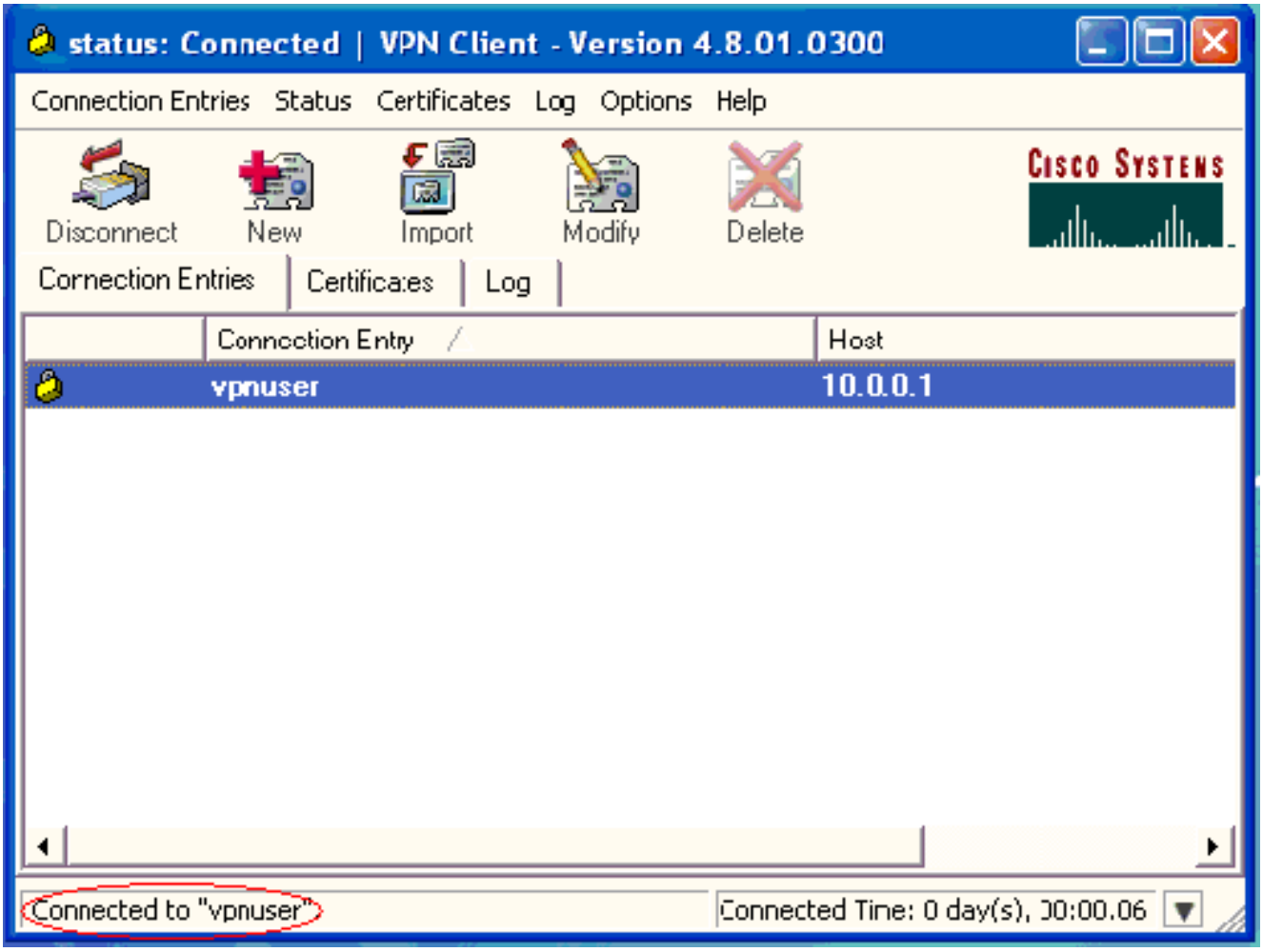
1. Нажмите **Connect** для инициирования VPN-подключения.



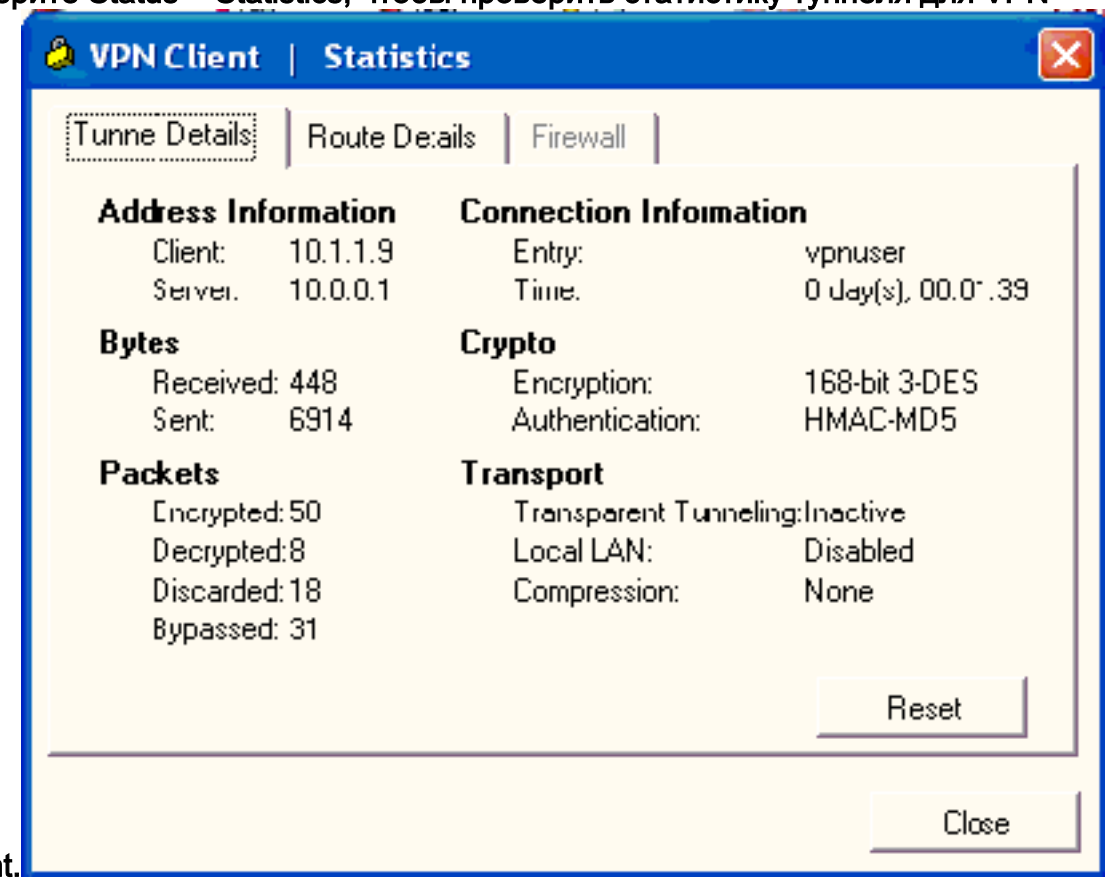
2. Это окно появляется для проверки подлинности пользователя. Введите допустимое имя пользователя и Пароль для установления VPN-подключения.



3. Клиент VPN связан с VPN 3000 Concentrator в центральном узле.



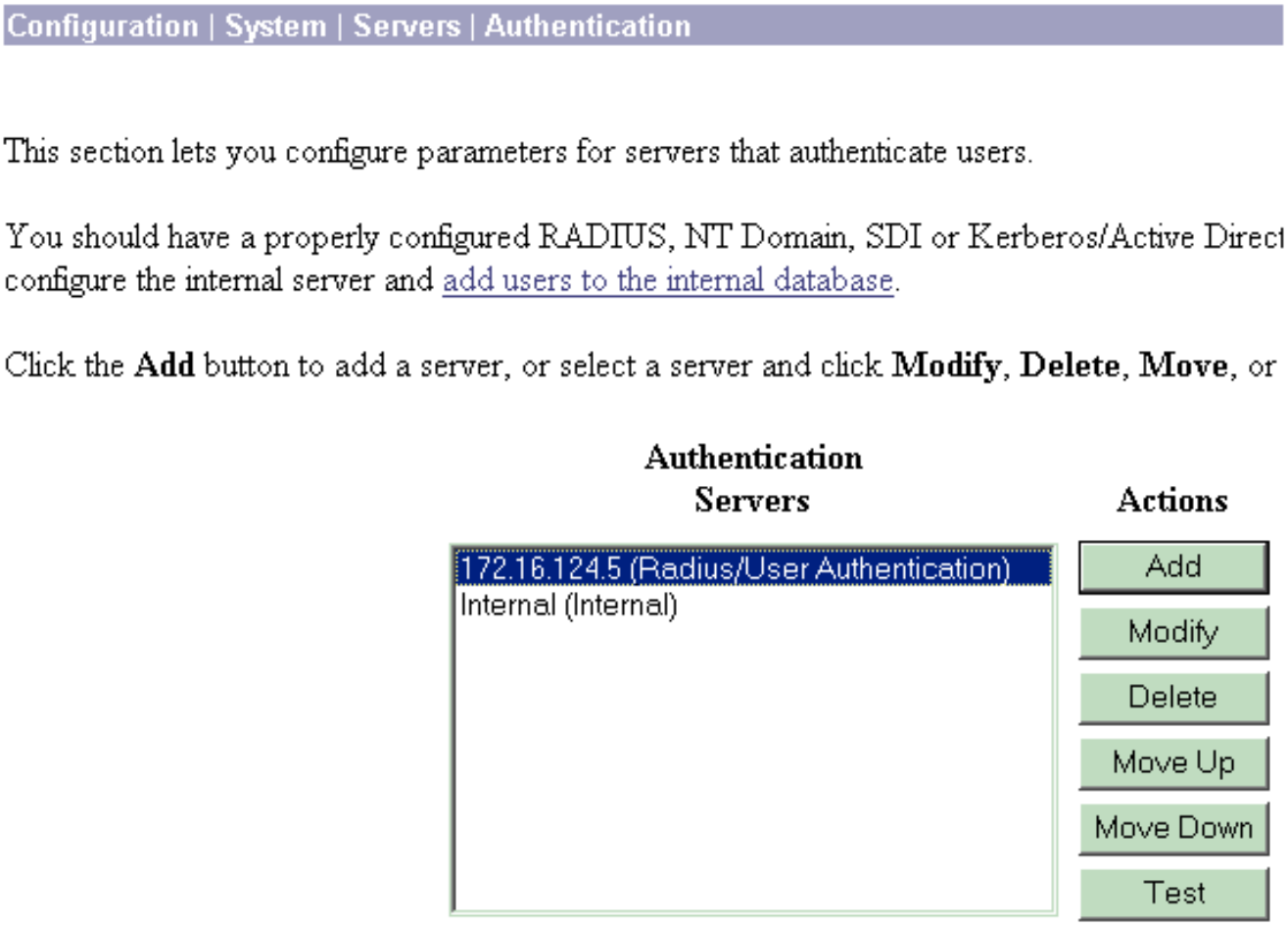
4. Выберите Status > Statistics, чтобы проверить статистику туннеля для VPN Client.



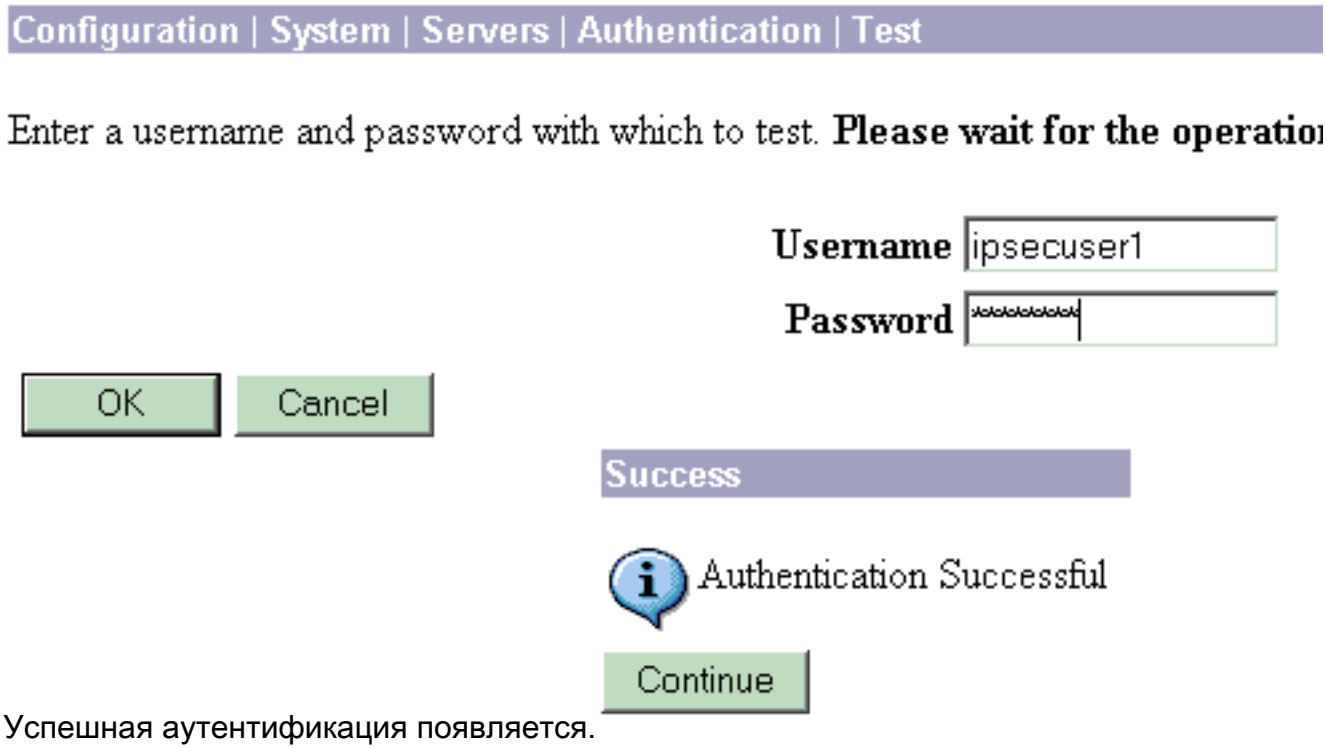
Устранение неполадок

Выполните следующие шаги для устранения неполадки в вашей настройке.

1. Выберите **Configuration> System> Servers> Authentication** и выполните эти шаги для тестирования подключения между сервером RADIUS и VPN 3000 Concentrator.Выберите свой сервер, и затем нажмите **Test**.

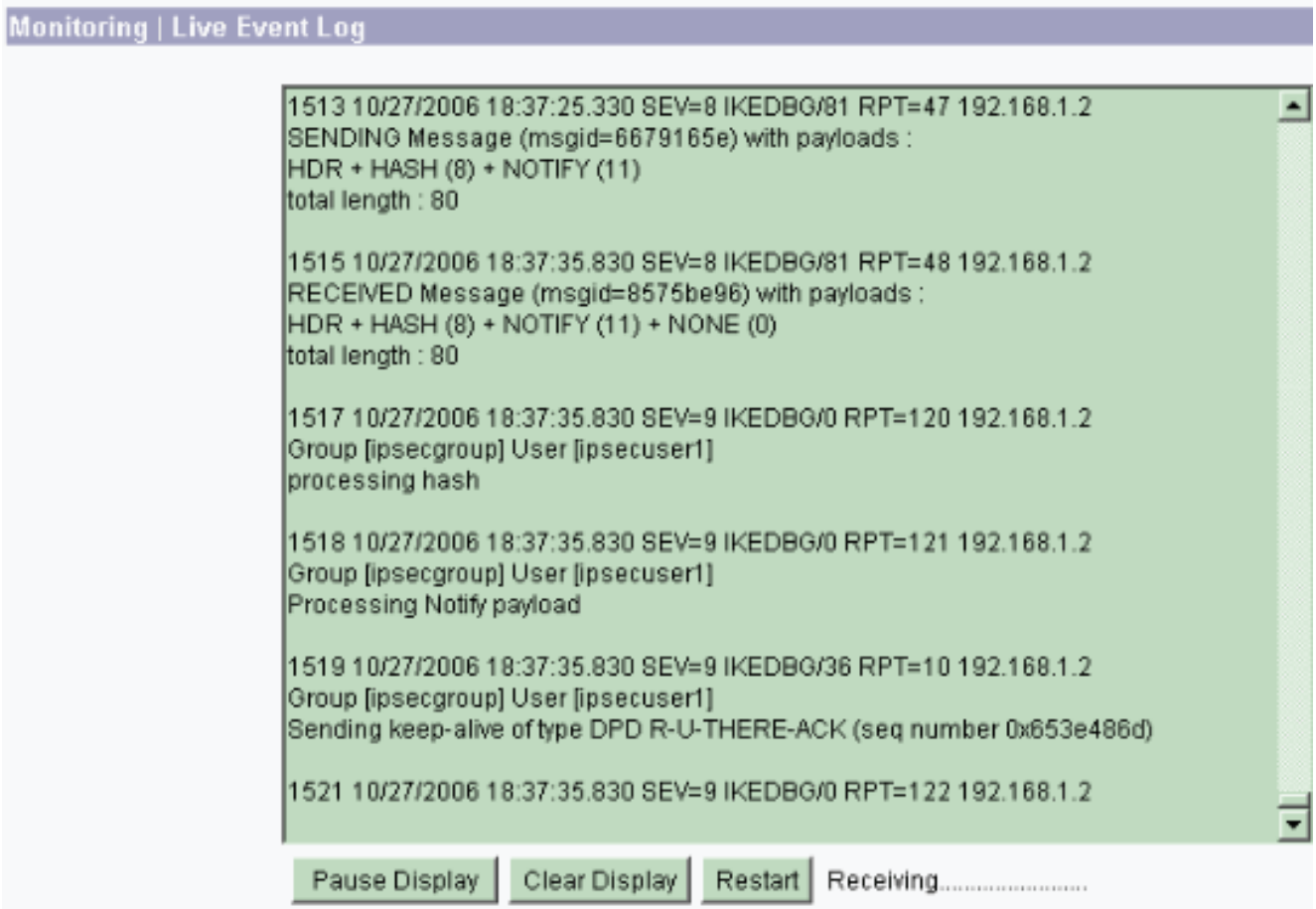


Введите Имя пользователя RADIUS и пароль и нажмите **OK**.



Успешная аутентификация появляется.

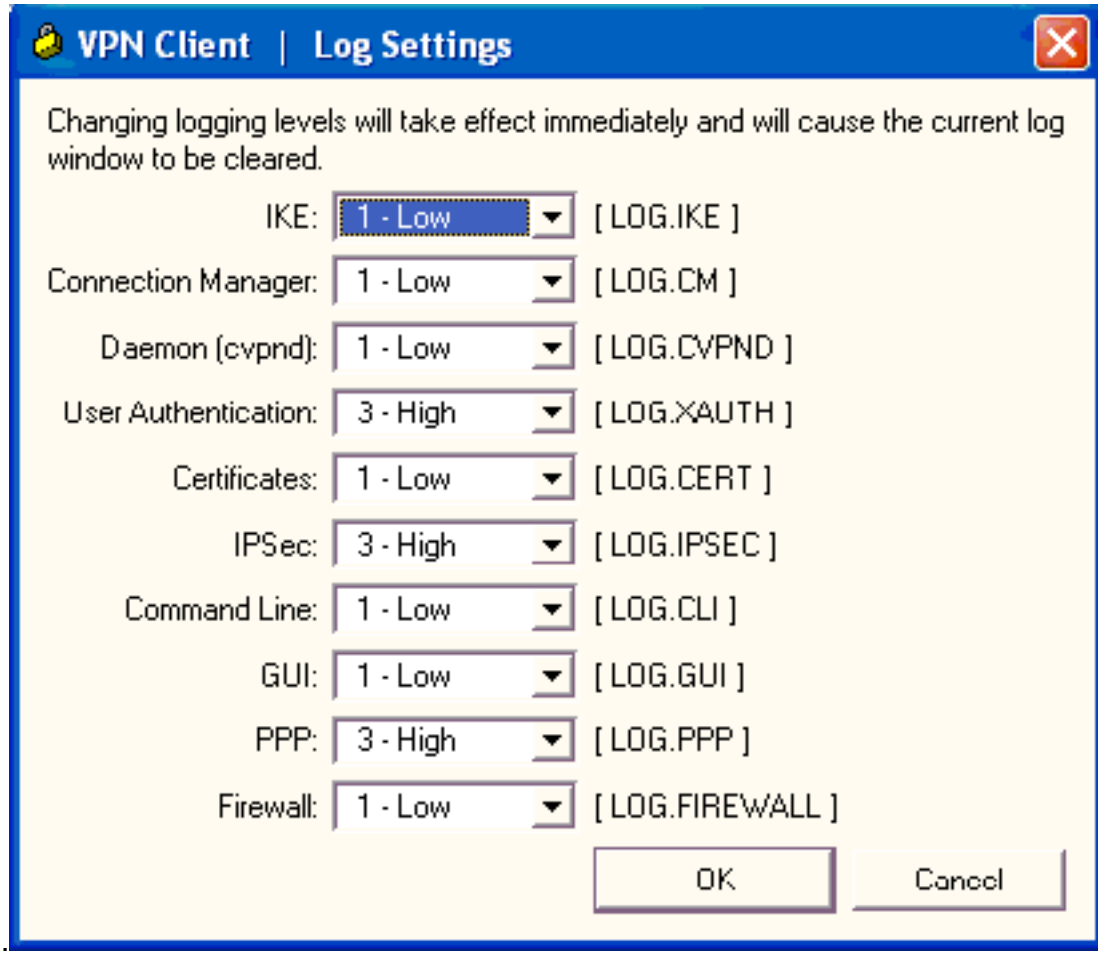
2. Если это отказывает, существует или проблема конфигурации или невозможность IP-подключения. Проверьте Вход в систему Неудачных попыток сервера ACS для сообщений, отнесенных к сбою.Если никакие сообщения не появляются в этом журнале тогда существует, вероятно, невозможность IP-подключения. Запрос RADIUS не достигает сервера RADIUS. Проверьте, что фильтры применились к соответствующему интерфейсу VPN 3000 Concentrator, позволяет RADIUS (1645) пакеты в и.Если тестовая аутентификация успешна, но входит к VPN 3000 Concentrator, продолжают отказывать, проверять Журнал событий с фильтрацией через консольный порт.Если соединения не работают, можно добавить AUTH, IKE и классы События IPSec к Концентратору VPN при выборе **Configuration> System> Events> Classes> Modify (Severity to Log=1-9, Severity to Console=1-3)**. AUTHDBG, AUTHDECODE, IKEDBG, IKEDECODE, IPSECDBG и IPSECDECODE также доступны, но могут предоставить слишком много информации. Если подробные сведения необходимы на атрибутах, которые переданы от сервера RADIUS, AUTHDECODE, IKEDECODE, и IPSECDECODE предоставляет это при Степенях серьезности ошибки к Log=1-13 уровню.
3. Получите журнал событий из **Monitoring> Event Log**.



Устраните неполадки клиента VPN 4.8 для Windows

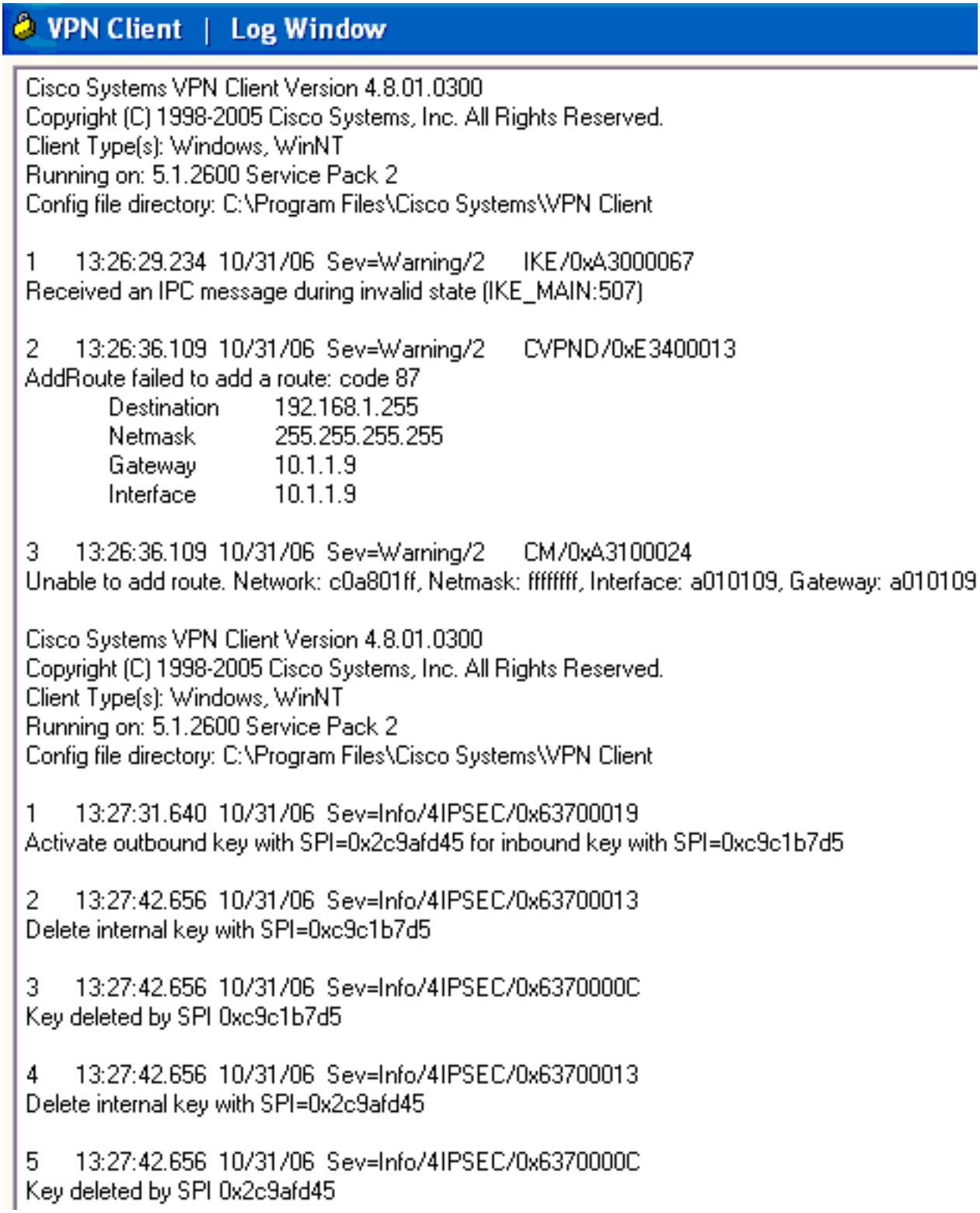
Выполните эти шаги для устранения проблем Клиента VPN 4.8 для Windows.

1. Выберите **Log> Настройки журнала** для включения регистрационных уровней в



Клиенте VPN.

2. Выберите **Log> Log Window** для просмотра записей журнала в Клиенте VPN.



Дополнительные сведения

- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN Client
- Согласование IPsec/Протоколы IKE
- Страница поддержки Cisco Secure ACS для Windows
- Динамические фильтры Настройки на сервере RADIUS
- Cisco Systems – техническая поддержка и документация