Настройка концентраторов серии Cisco VPN 3000 на поддержку функции истечения срока действия пароля NT с RADIUS Server

Содержание

Введение

Этот документ включает пошаговые инструкции о том, как настроить концентраторы Cisco VPN серии 3000 для поддержки Характеристики истечение срока действия пароля NT с помощью сервера RADIUS.

См. RADIUS VPN 3000 с Характеристикой проверки срока действия Использование Сервера аутентификации Microsoft Internet Authentication Server для узнавания больше о том же сценарии с Internet Authentication Server (IAS).

Предварительные условия

Требования

- Если ваш сервер RADIUS и сервер Аутентификации в домене NT находятся на двух отдельных компьютерах, удостоверьтесь, что вы установили возможность подключения с помощью IP-адреса между этими двумя машинами.

- Удостоверьтесь, что вы установили возможность подключения с помощью IP-адреса от концентратора до сервера RADIUS. Если сервер RADIUS находится к открытому интерфейсу, не забывайте открывать ПОРТ RADIUS на Общем фильтре.
- Гарантируйте, что можно соединиться с концентратором от клиента VPN, использующего Базу данных Внутреннего пользователя. Если это не настроено см. IPSec Настройки - Клиент VPN Cisco 3000 к VPN 3000 Concentrator.

Примечание: Характеристика истечение срока действия пароля не может использоваться с веб-VPN или VPN-клиентами SSL (SVC).

Используемые компоненты

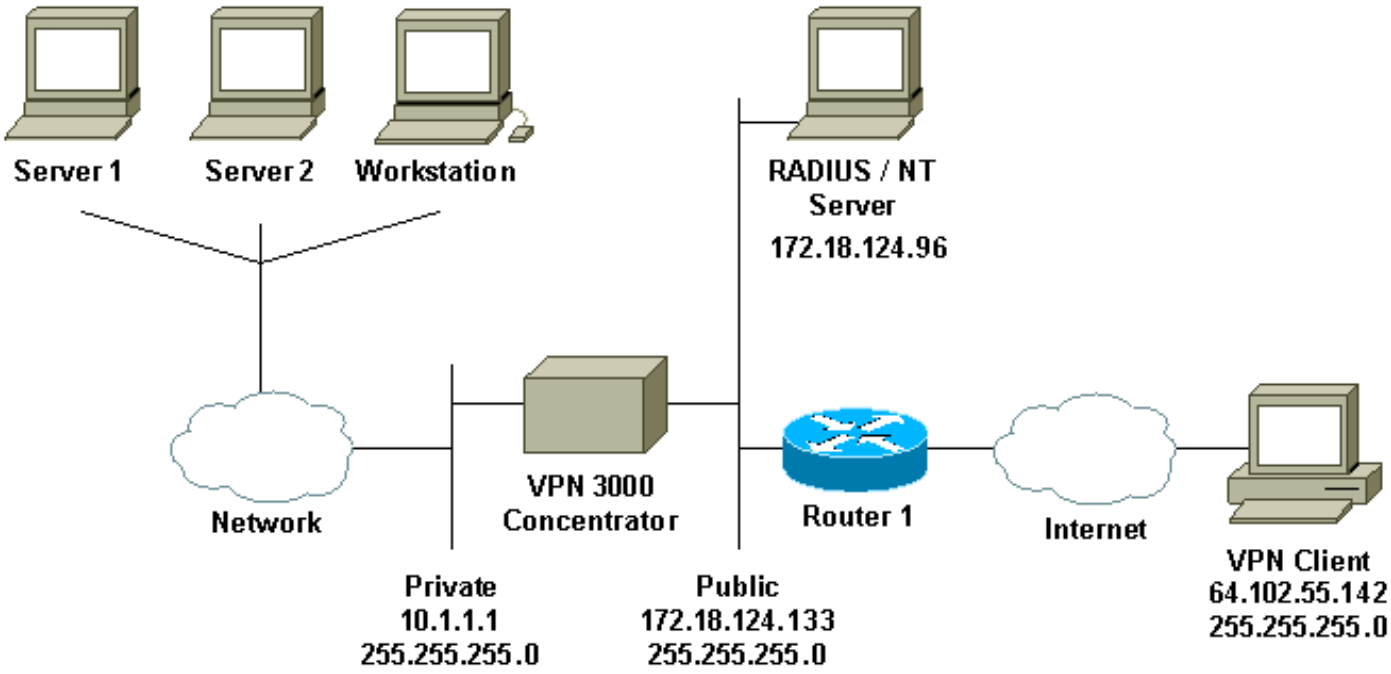
При разработке и тестировании этой конфигурации использовались следующие версии программного и аппаратного обеспечения.

- Версия программного обеспечения 4.7 VPN 3000 Concentrator
- Выпуск 3.5 клиента VPN
- Cisco Secure для NT (CSNT) Сервер Active Directory Microsoft Windows 2000 версии 3.0 для Проверки подлинности пользователя

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.

Схема сети

В настоящем документе используется следующая схема сети:



Примечания к диаграмме

1. Сервер RADIUS в этой конфигурации находится на открытом интерфейсе. Если это верно, с вашей определенной настройкой, создайте два правила в своем общем фильтре, чтобы позволить Трафику сервера RADIUS вводить и оставлять

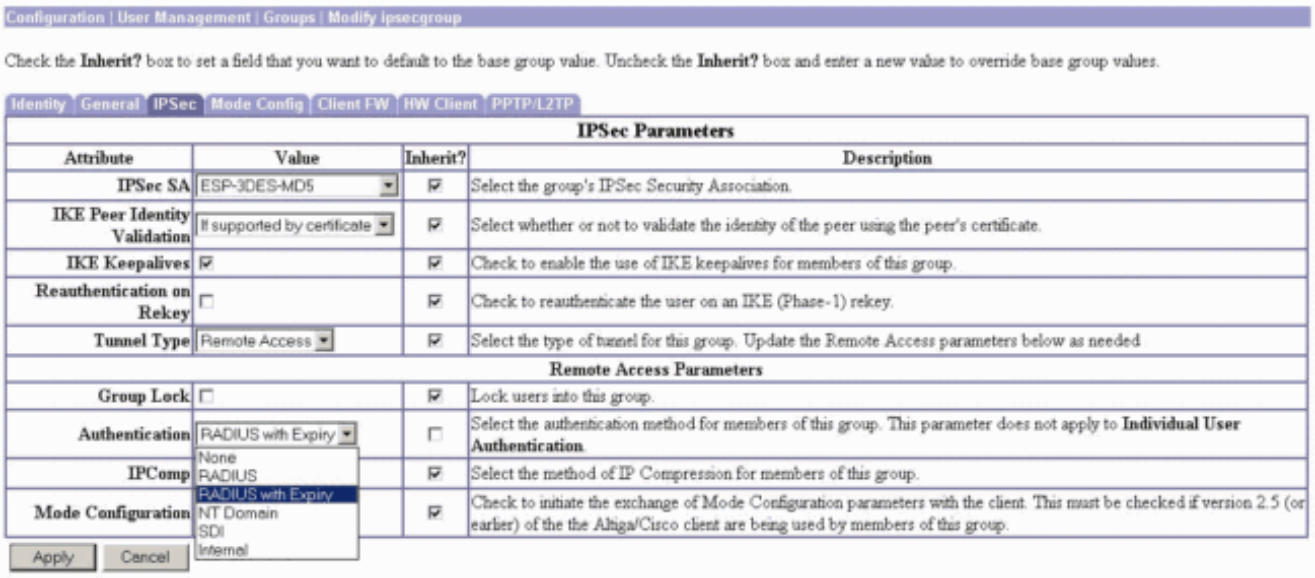
концентратор.
2. Эта конфигурация показывает программное обеспечение CSNT и NT Domain Authentication Services, работающая на той же машине. Эти элементы могут быть выполнены на двух отдельных компьютерах при необходимости вашей конфигурацией.

Настройка концентратора VPN 3000

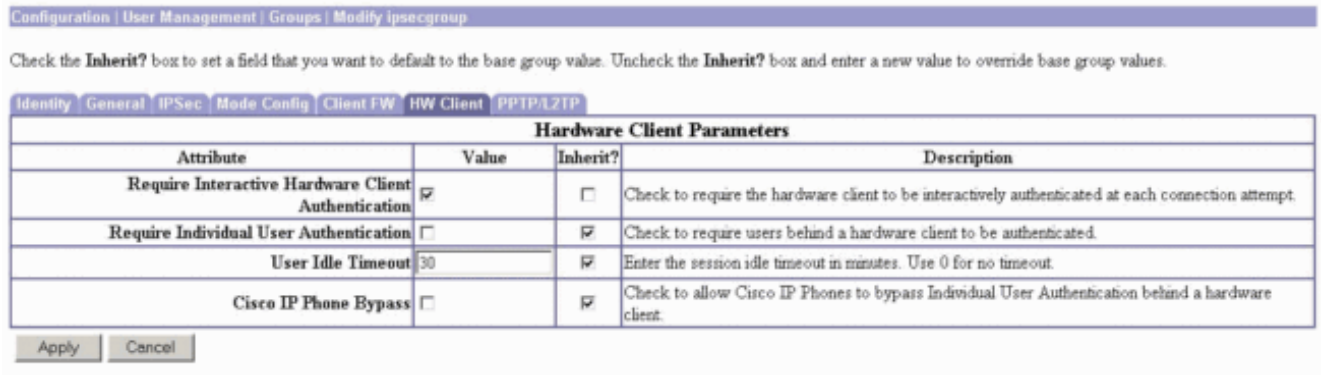
Конфигурация группы

1. Для настройки группы для принятия Параметров Истечения срока действия пароля NT от сервера RADIUS перейдите **к Configuration> User Management> Groups**, выберите группу из списка и нажмите **Modify Group**. Пример ниже показов, как модифицировать группу, названную "ipsecgroup".

2. Перейдите к вкладке **IPSec**, удостоверьтесь, что **RADIUS с Истечением** выбран для **Опознавательного** атрибута.

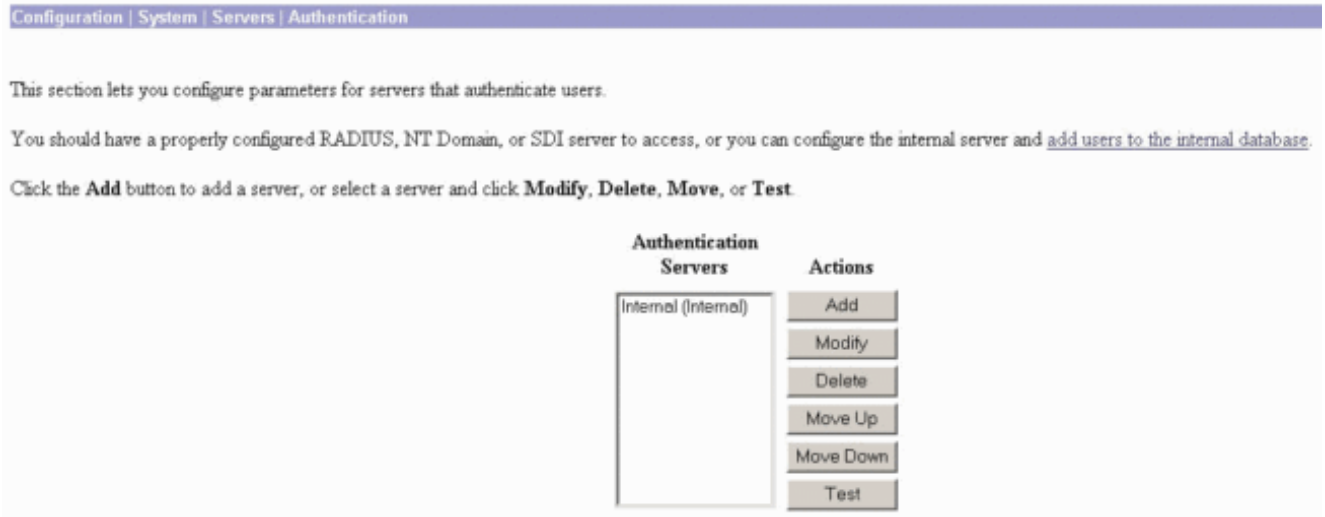


3. Если вы хотите, чтобы эта функция была включена на аппаратных клиентах VPN 3002, перешла к вкладке **HW Client**, удостоверьтесь, что **Require Interactive Hardware Client Authentication**, включен, то нажмите **Apply**.



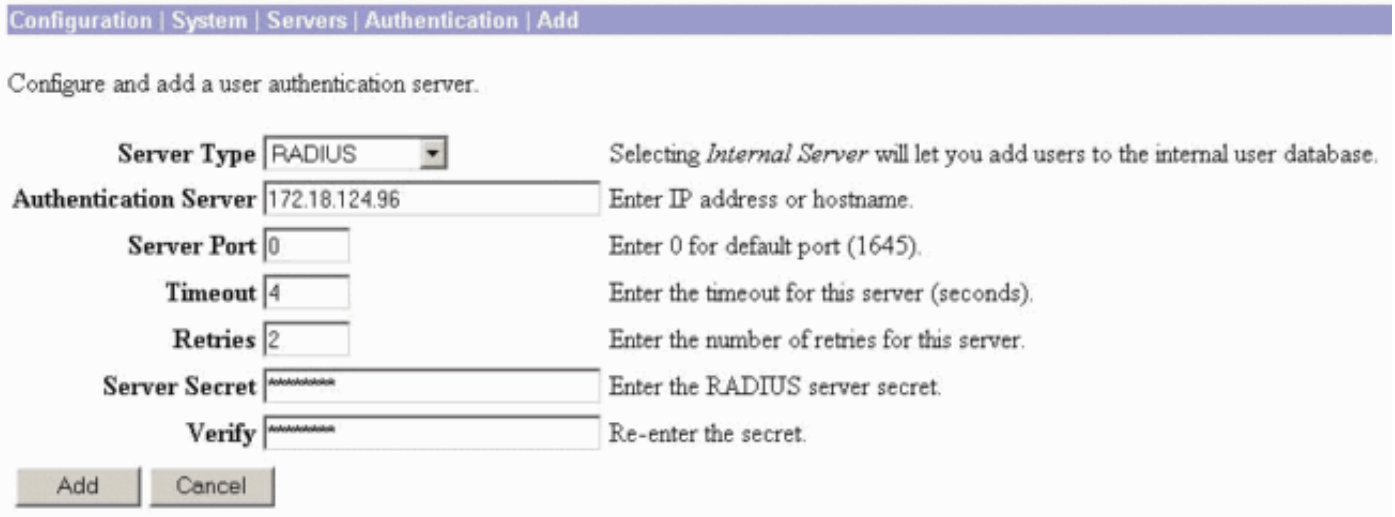
Конфигурация RADIUS

1. Для настройки параметров настройки сервера RADIUS на концентраторе перейдите **к Configuration> System> Servers> Authentication>, Добавляют**.



2. На **экране Add** введите в значениях, которые соответствуют серверу RADIUS и **нажмите Add**.Пример ниже использует следующие значения.`Server Type:` **`RADIUS`**

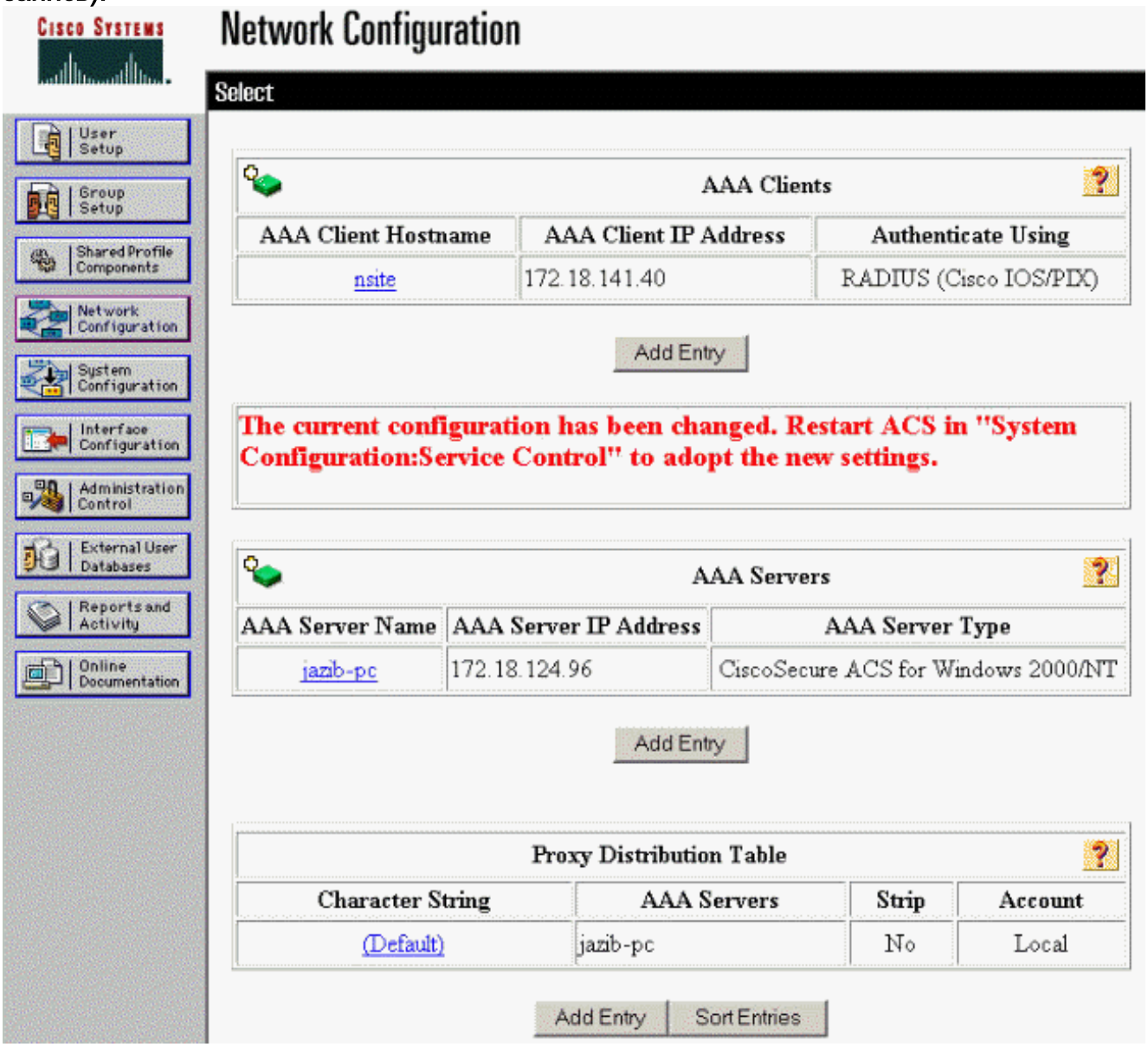
`Authentication Server:` **`172.18.124.96`** `Server Port =` **`0`** `(for default of 1645) Timeout =` **`4`**
`Reties =` **`2`** `Server Secret =` **`cisco123`** `Verify:` **`cisco123`**



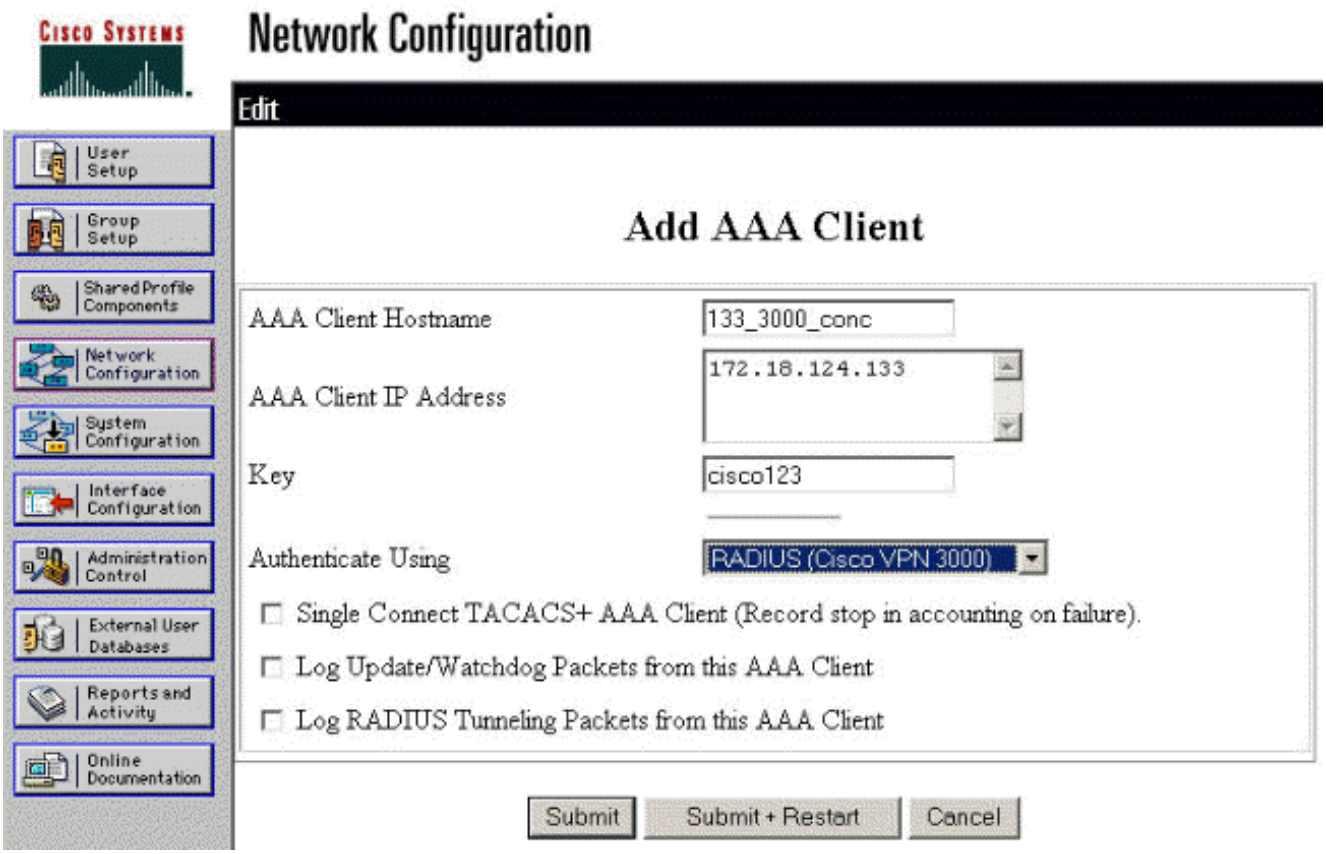
Конфигурирование сервера безопасности сервиса удаленной аутентификации по телефонной линии (RADIUS) Cisco

Настройка записи для концентратора VPN 3000

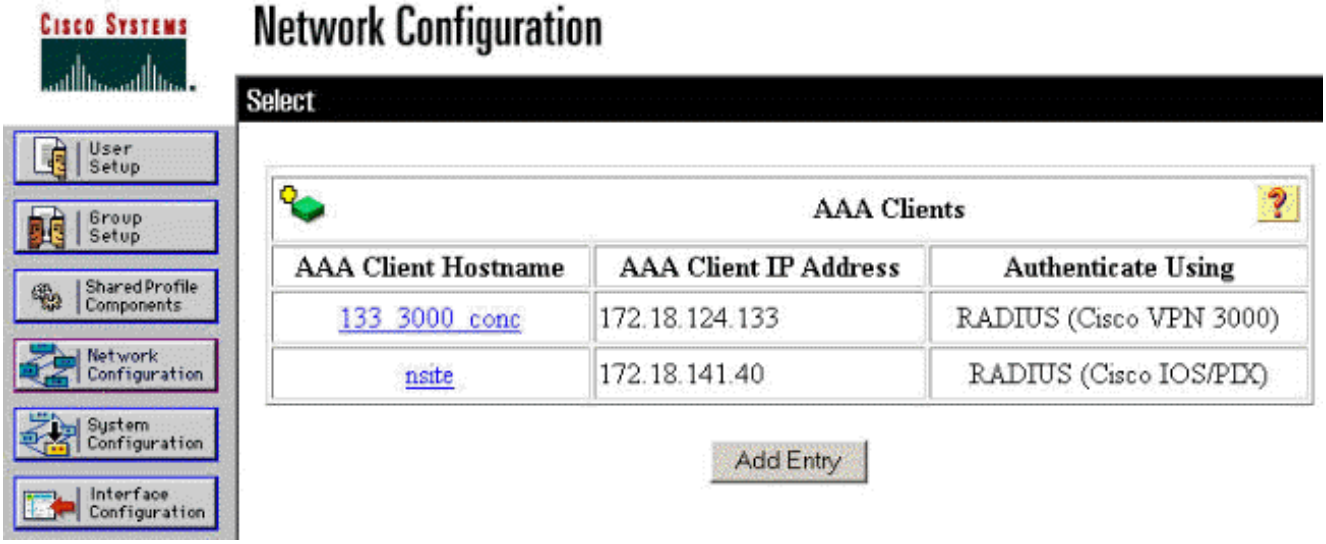
1. Войдите в CSNT и нажмите **Network Configuration** в левой панели. **На вкладке AAA Clients (Клиенты AAA) щелкните Add Entry (Добавить запись).**



2. На экране "Add AAA Client" введите в соответствующих значениях, чтобы добавить концентратор как КЛИЕНТА RADIUS, затем нажать **Submit + Перезапуск**.Пример ниже использует следующие значения.`AAA Client Hostname = 133_3000_conc AAA Client IP Address = 172.18.124.133 Key = cisco123 Authenticate using = RADIUS (Cisco VPN 3000)`

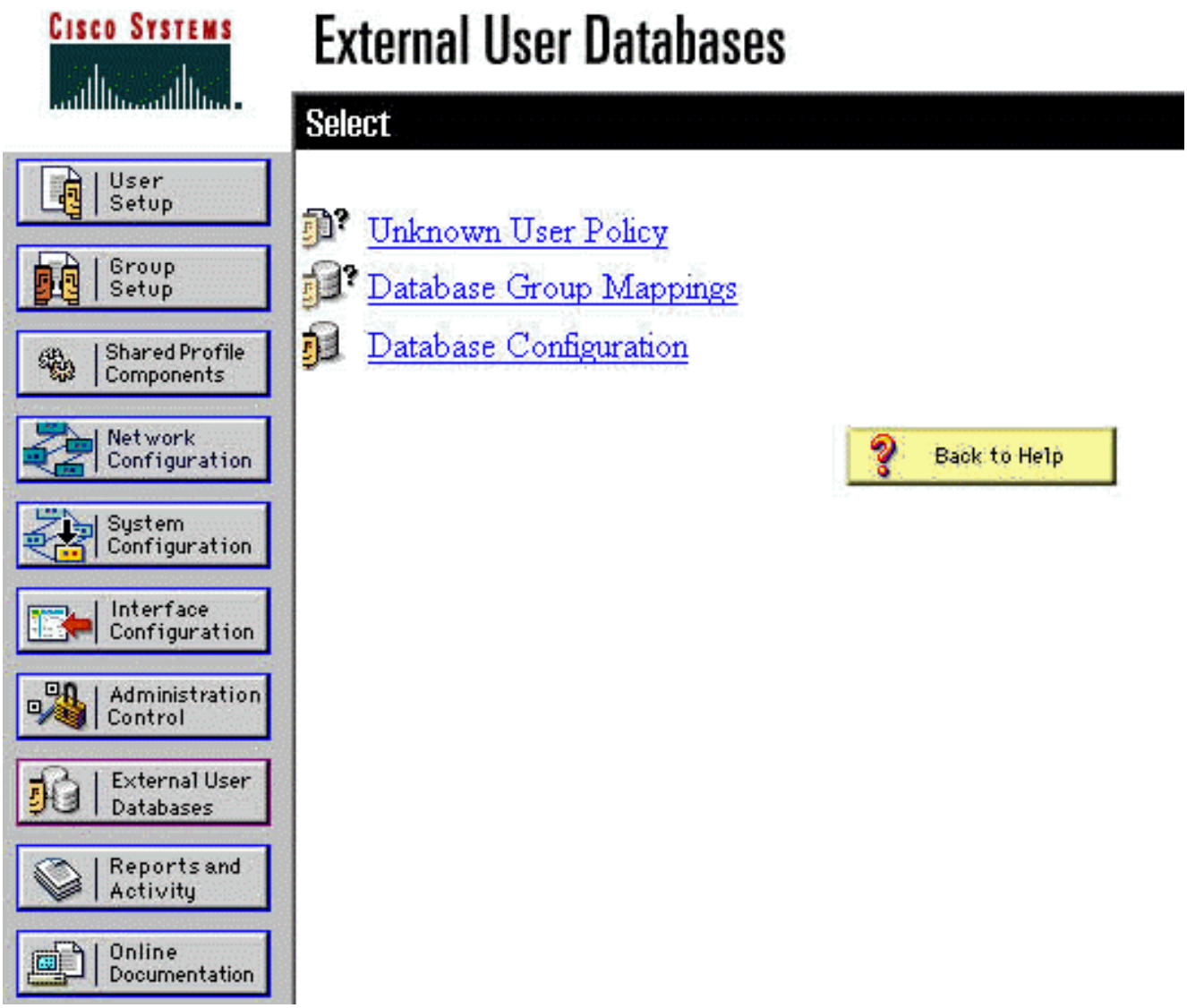


Запись для ваших 3000 концентраторов появится под разделом **"Клиентов AAA"**.

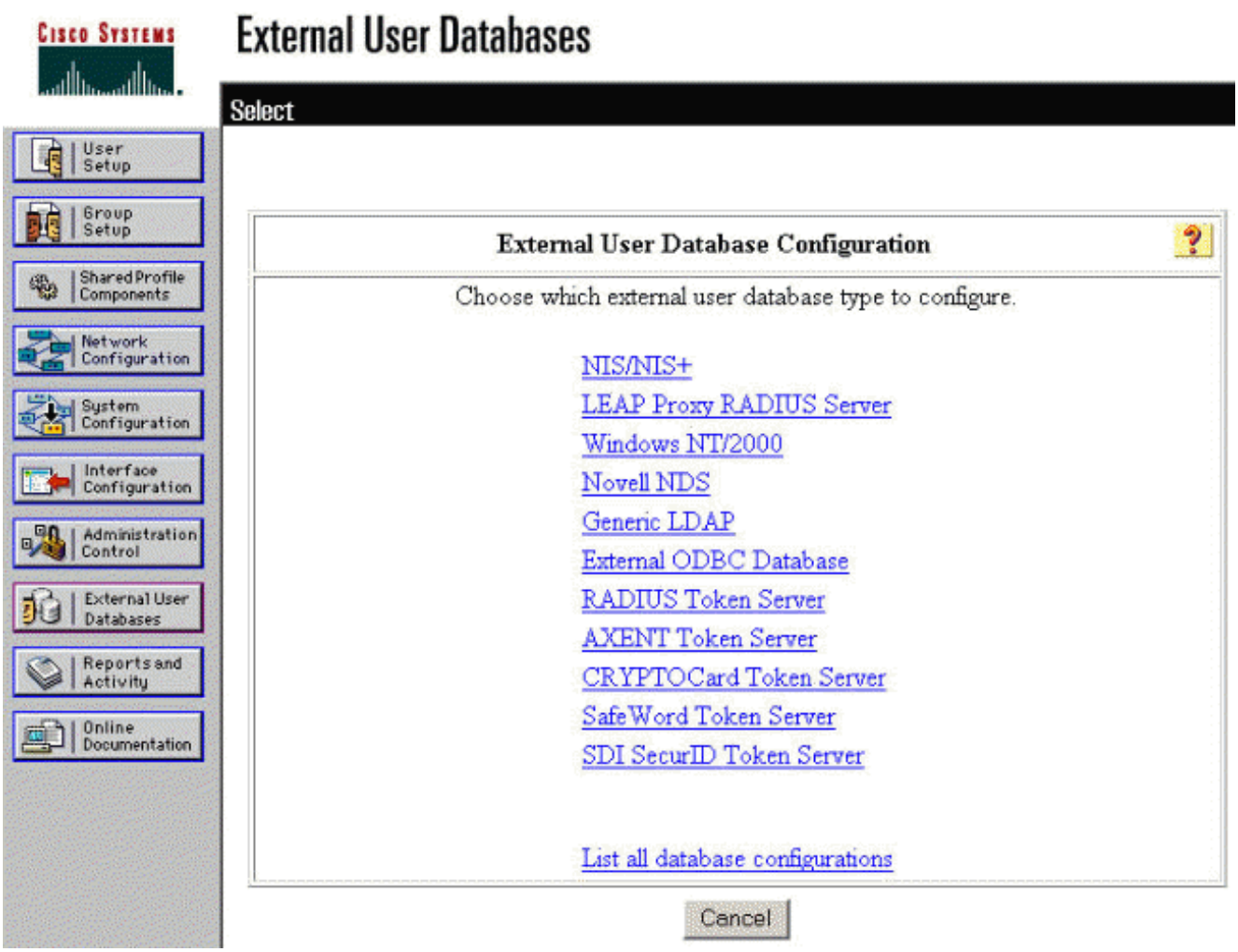


Настройка политики для неизвестного пользователя для аутентификации в домене NT

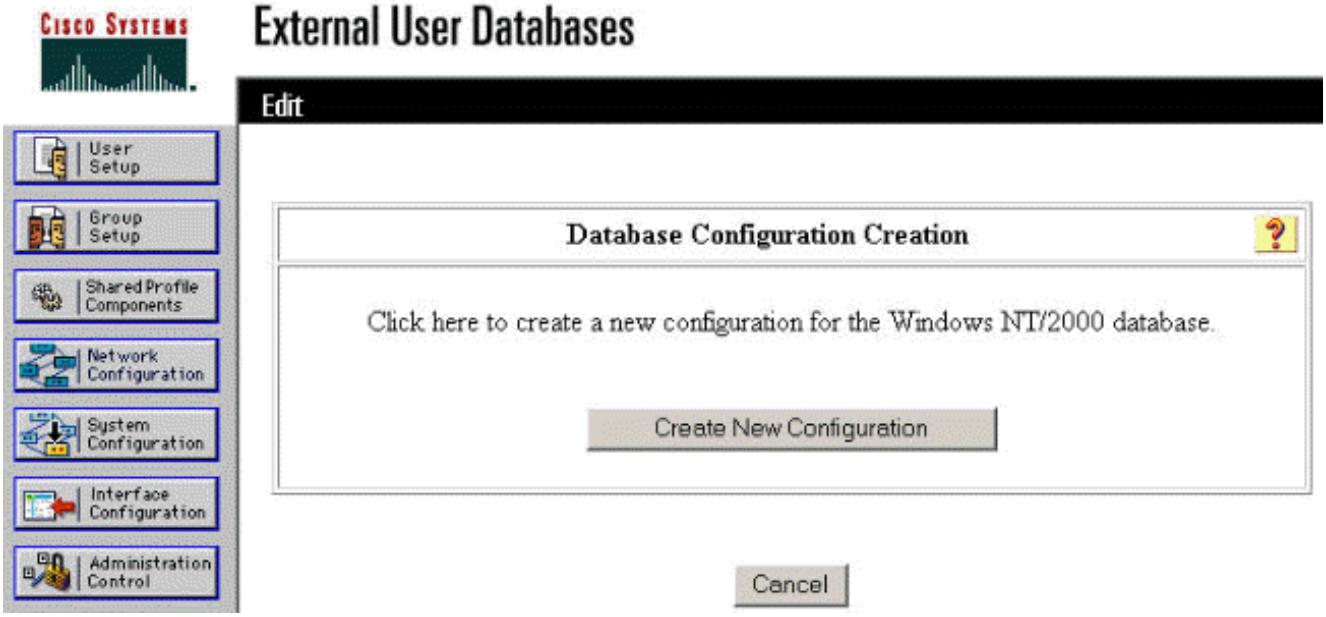
1. Для настройки Проверки подлинности пользователя на сервере RADIUS как часть Неизвестной политики пользователя нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Конфигурации базы данных**.



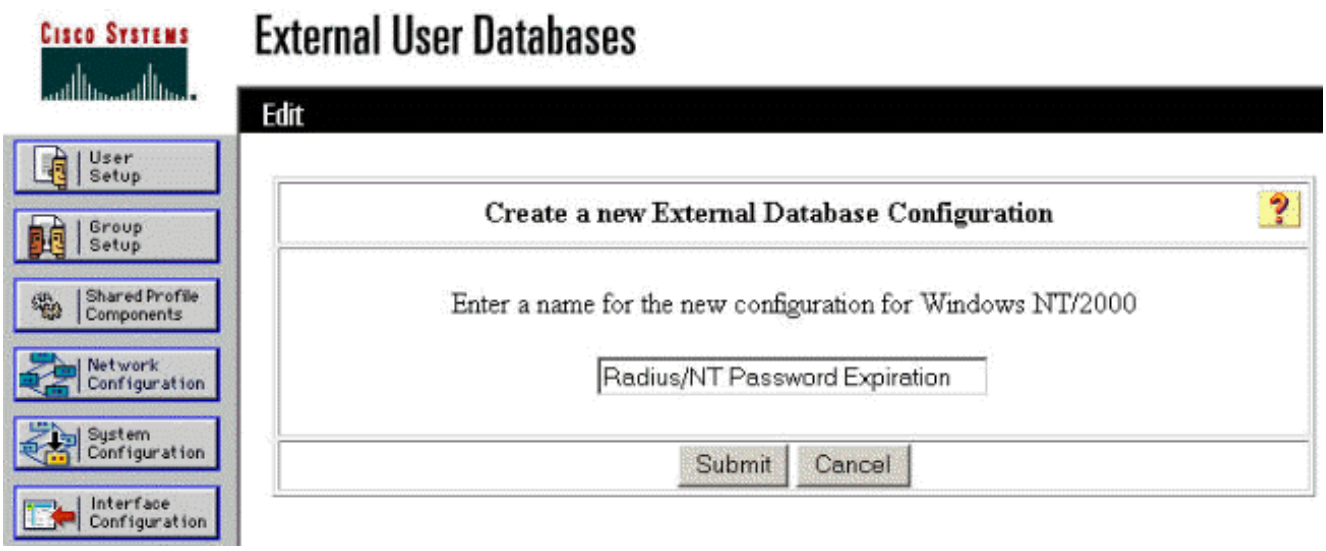
2. Под "Конфигурацией базы данных внешних пользователей" нажмите **Windows NT/2000**.



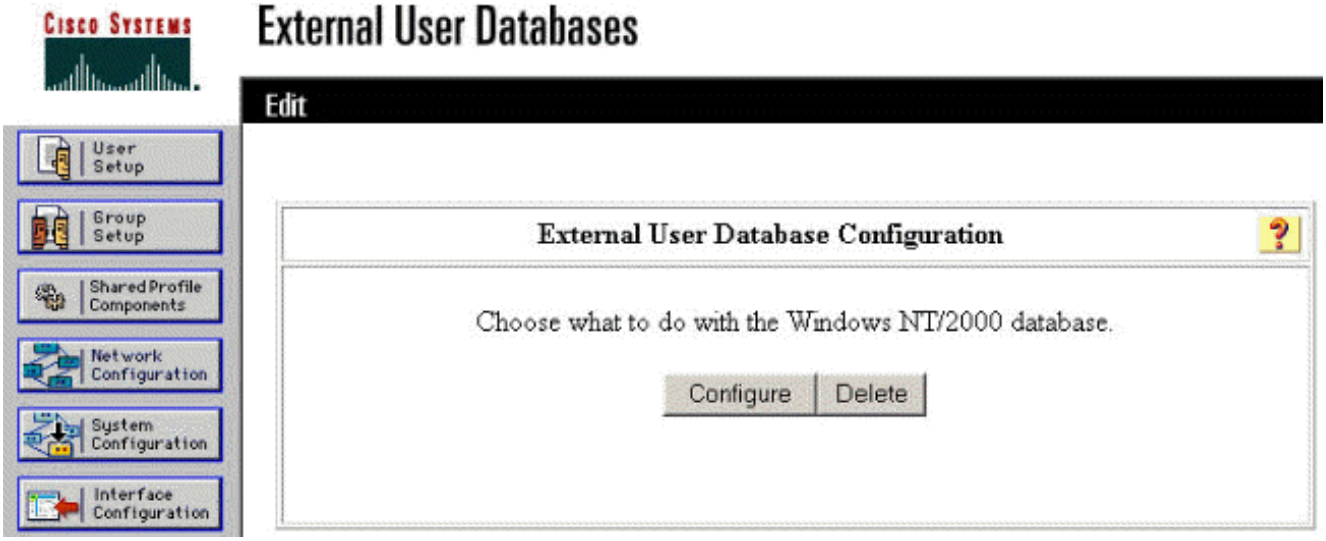
3. На экране "Database Configuration Creation" нажмите **Create New Configuration**.



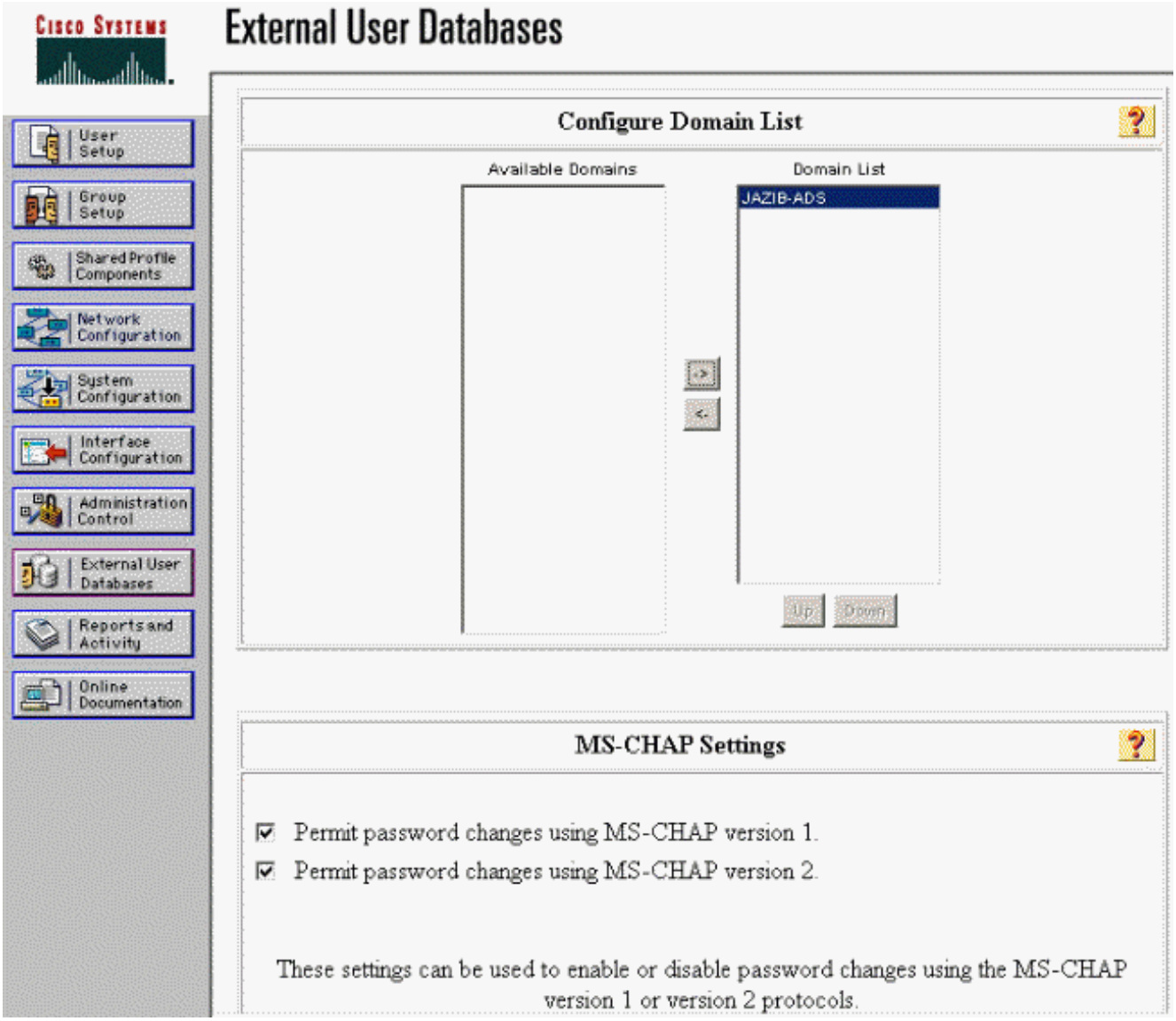
4. Когда предложено, введите имя для Аутентификации NT/2000 и нажмите **Submit**. Пример ниже показов название "Истечение срока действия пароля Радиуса/NT".



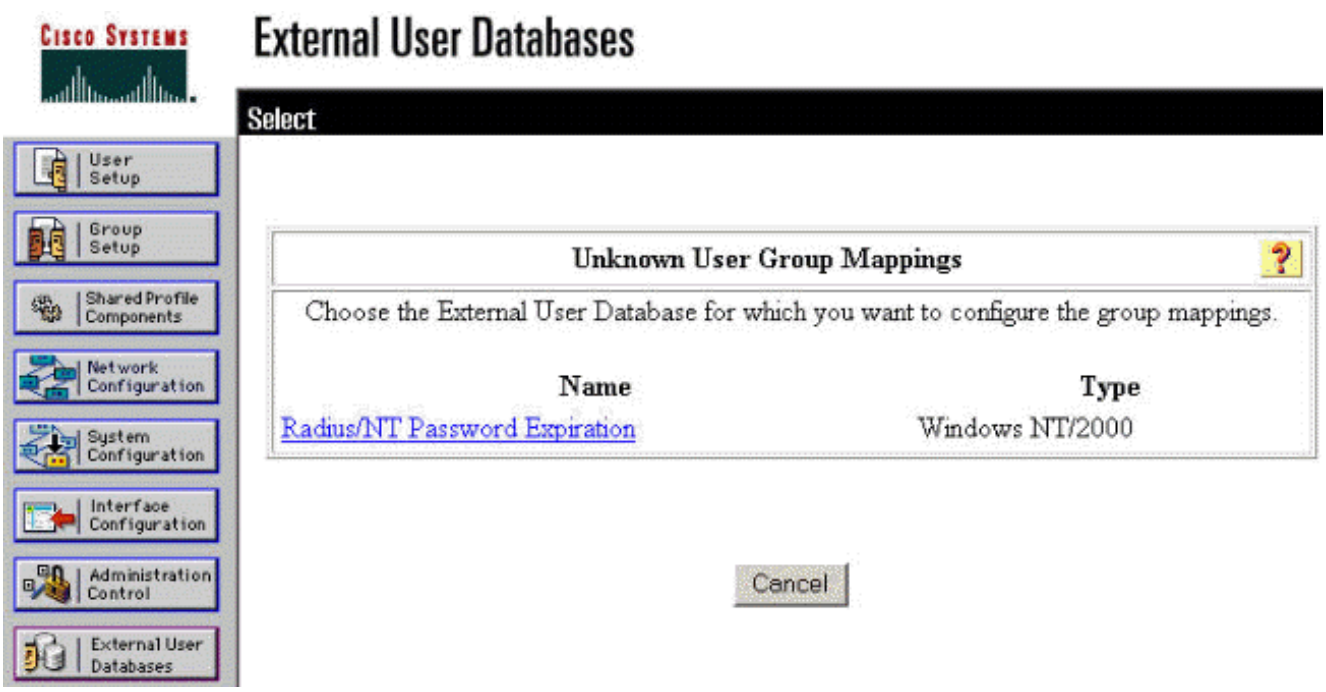
5. Нажмите **Configure** для настройки Доменного имени для Проверки подлинности пользователя.



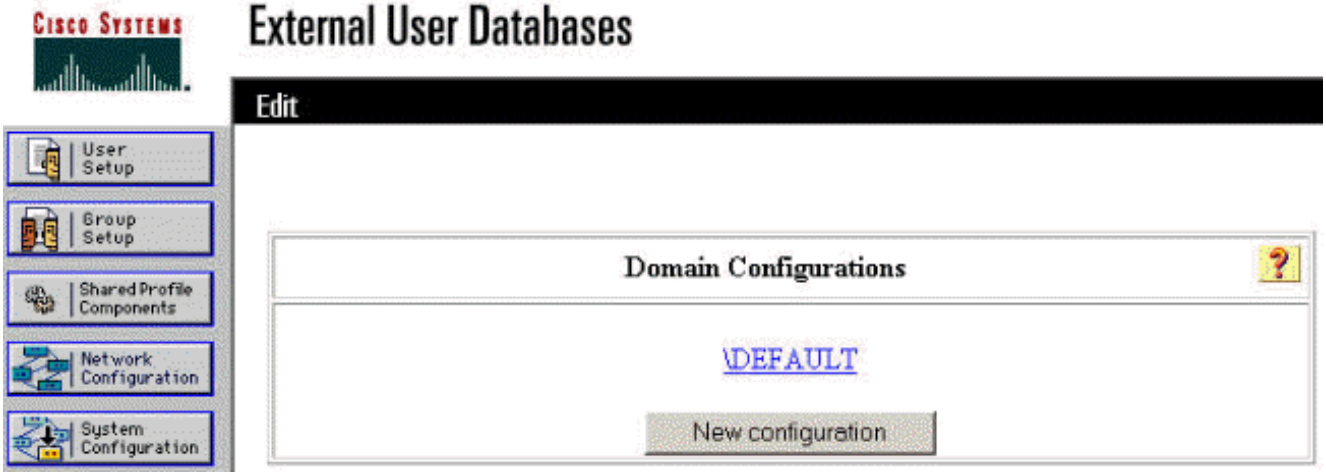
6. Выберите свой домен NT от "Доступных Доменов", затем нажмите кнопку стрелки вправо для добавления его к "Списку доменов". При "Параметрах настройки MS-CHAP", гарантируйте, что выбраны опции для **изменений пароля Разрешения с помощью Версии MS-CHAP 1** и **версии 2**. **По завершении нажмите Submit.**



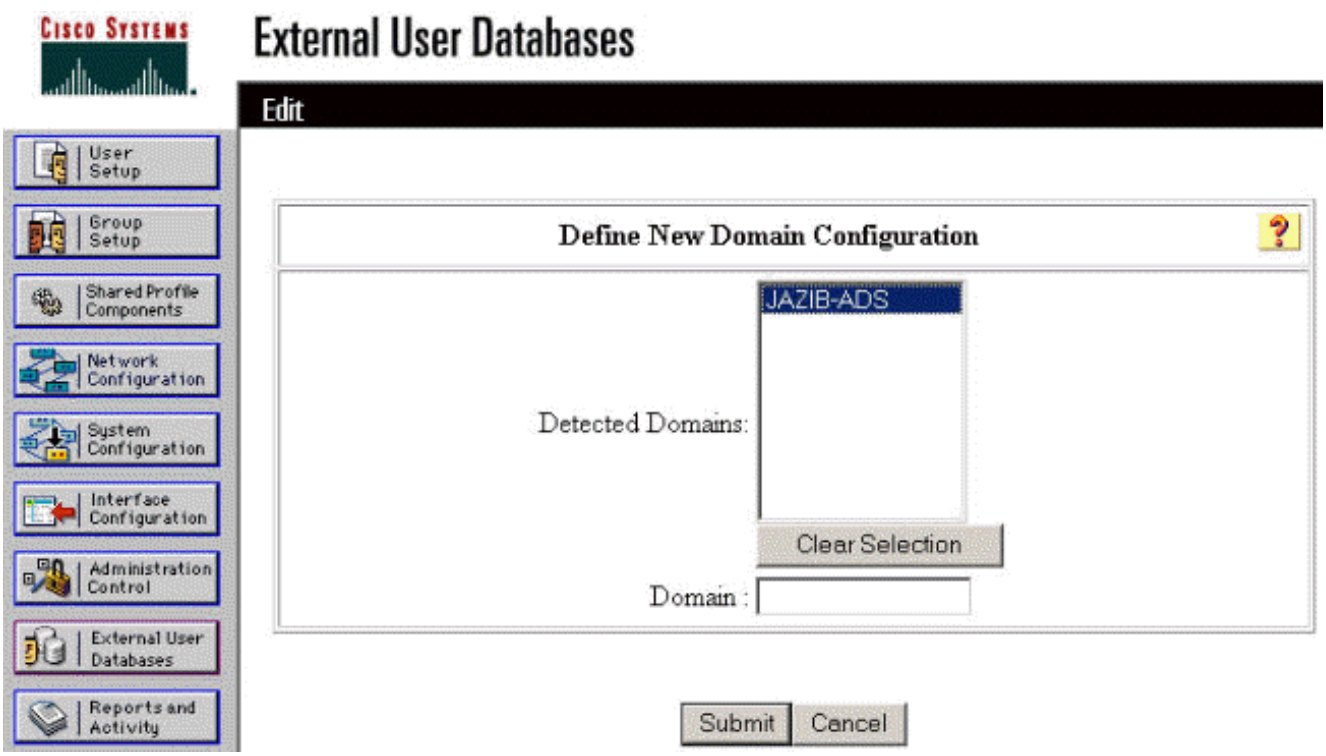
7. Нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Сопоставлений групп баз данных** (как замечено в данном примере). Необходимо видеть запись для ранее настроенной внешней базы данных. Пример ниже показов запись для "Истечения срока действия пароля Радиуса/NT", база данных, которую мы просто
настроили.



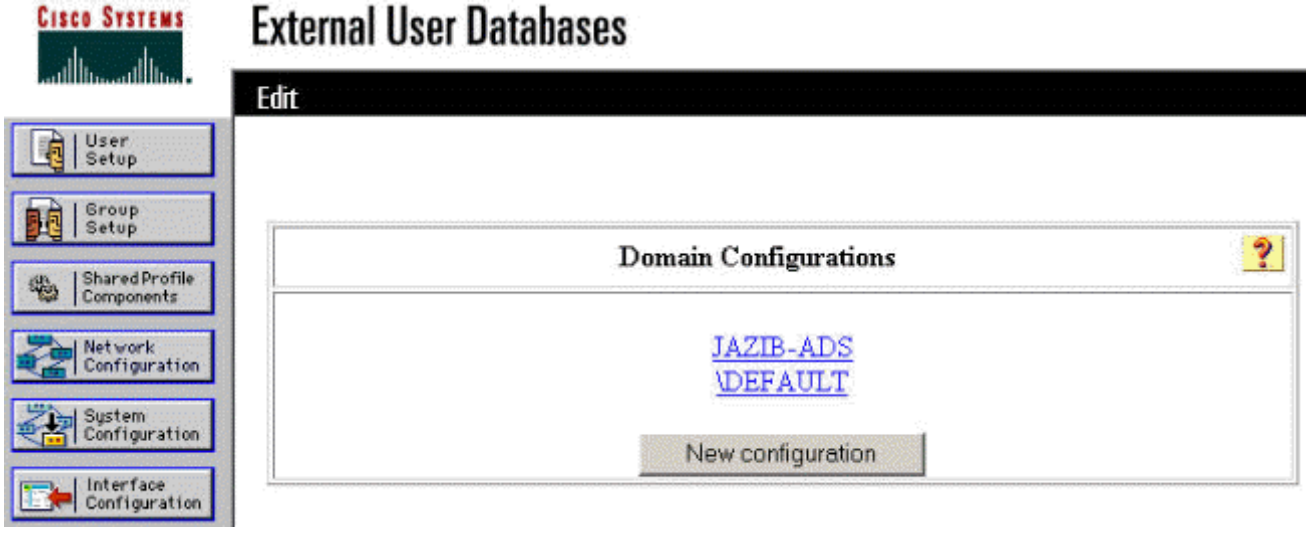
8. На экране "Domain Configurations" нажмите **New configuration** для добавления конфигураций
домена.



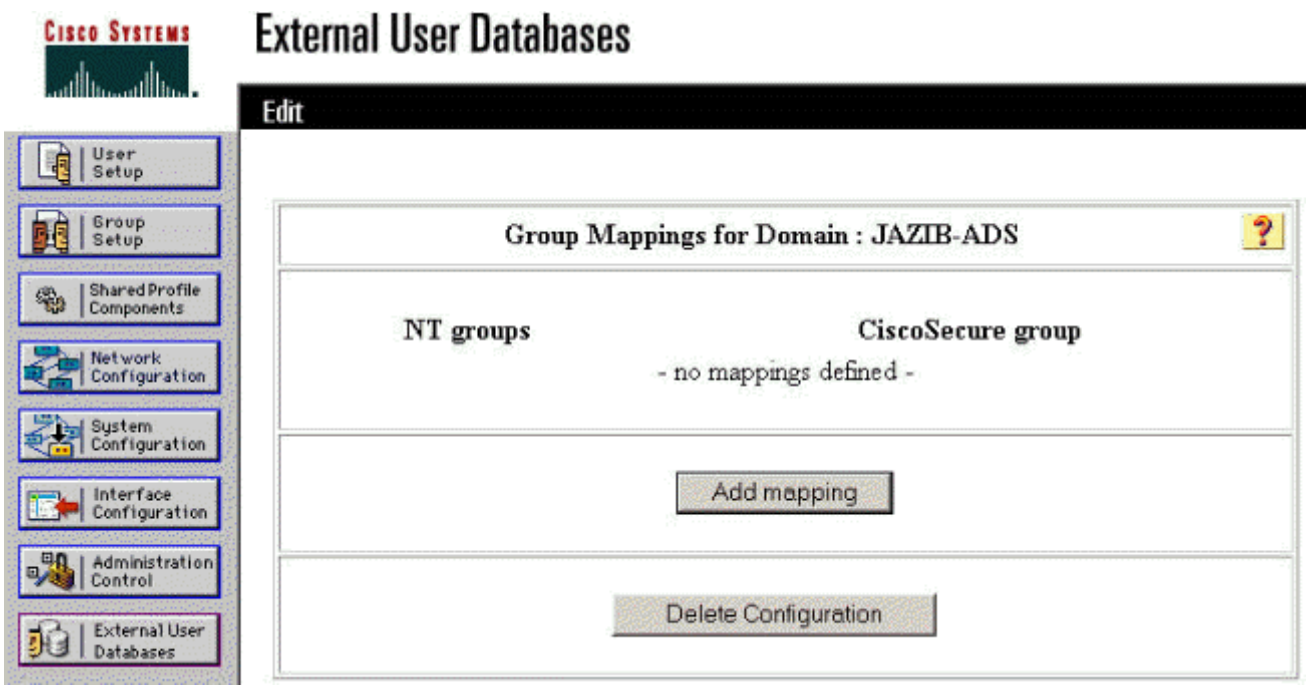
9. Выберите свой домен из списка "Обнаруженных Доменов" и нажмите **Submit**. Пример ниже показов домен назвал "JAZIB-
ADS".



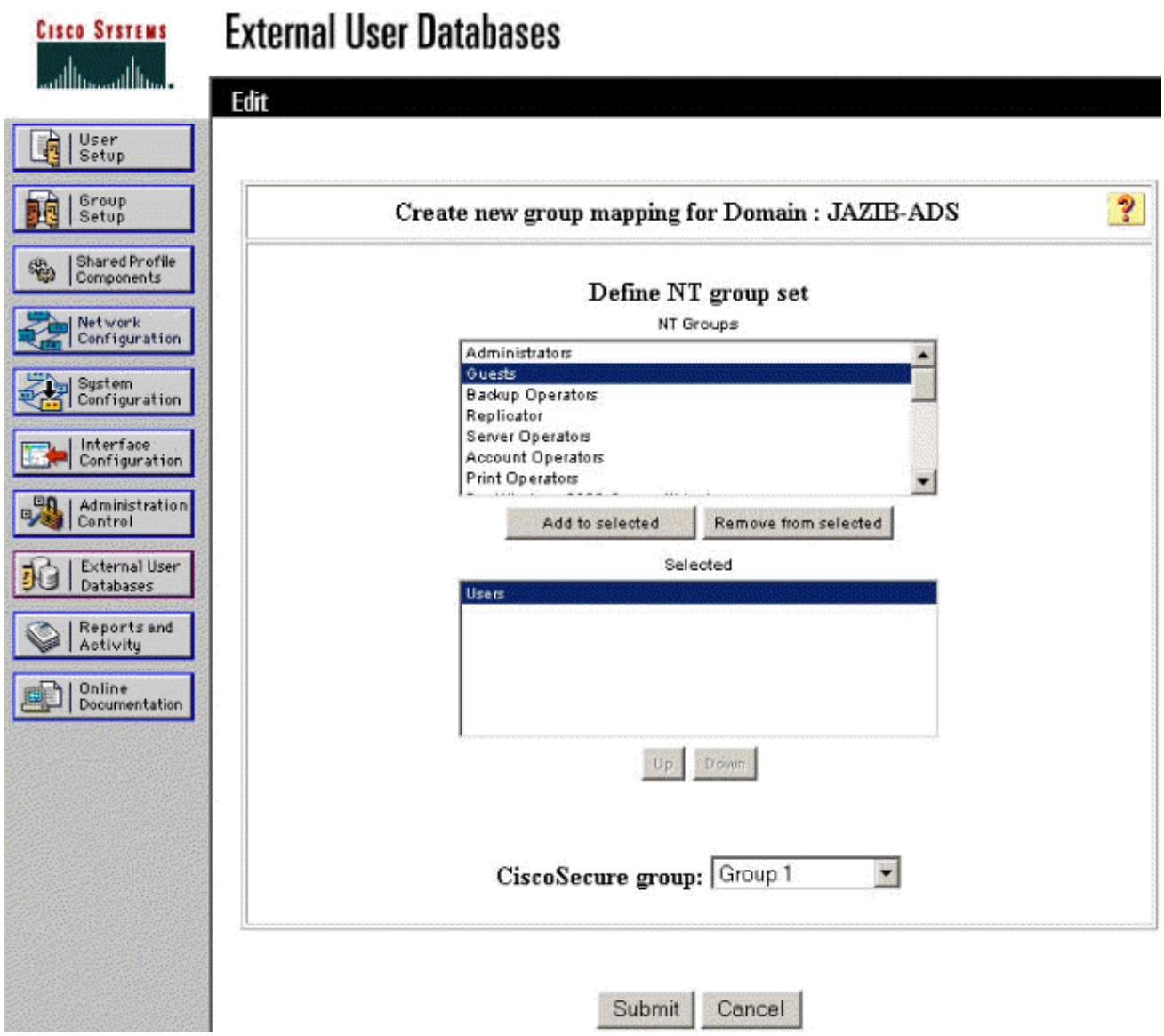
10. Щелкните по своему доменному имени для настройки сопоставлений группы. Данный пример показывает доменный "JAZIB-ADS".



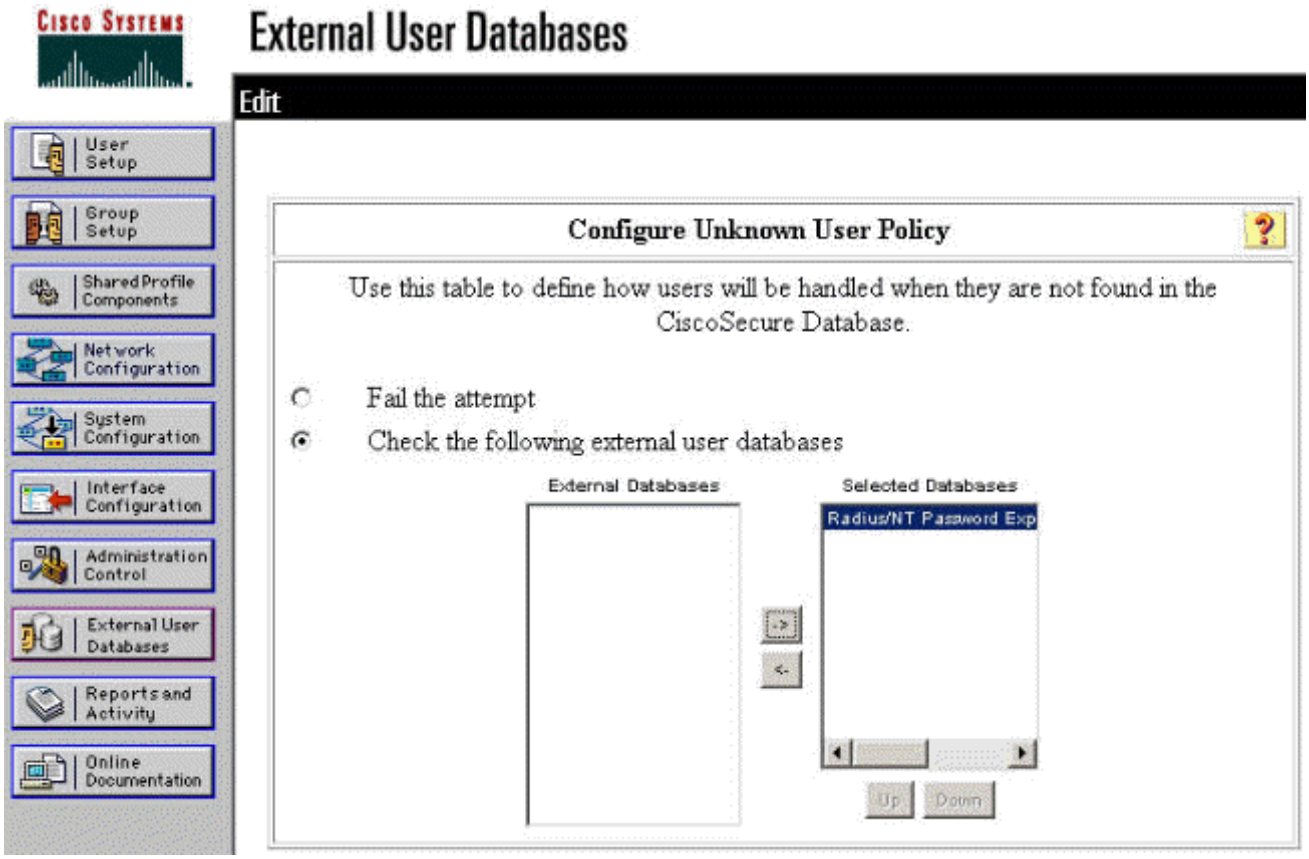
11. **Нажмите Add сопоставление** для определения сопоставлений группы.



12. <ts font_id="Arial" fsize="10"/>На<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>экране<ts font_id="MS Sans Serif"/> "Create new group mapping" <ts font_id="Arial"/>отобразите<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>группу<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>домена<ts font_id="MS Sans Serif"/> NT <ts font_id="Arial"/>на<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>группу<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>сервера<ts font_id="MS Sans Serif"/> CSNT RADIUS, <ts font_id="Arial"/>затем<ts font_id="MS Sans Serif"/> <ts font_id="Arial"/>щелкните<ts font_id="MS Sans Serif"/> Submit.. Ниже привелённый пример отоброжает связь NT группы "Users" с RADIUS группой "Group 1"."



13. Нажмите **External User Database** в левой панели, затем щелкните по ссылке для **Неизвестной политики пользователя** (как замечено в данном примере). Удостоверьтесь, что выбрана опция для **Проверки следующие внешние базы данных пользователей**. Нажмите кнопку стрелки вправо для перемещения ранее настроенной внешней базы данных из списка "Внешних баз данных" к списку "Выбранных баз данных".

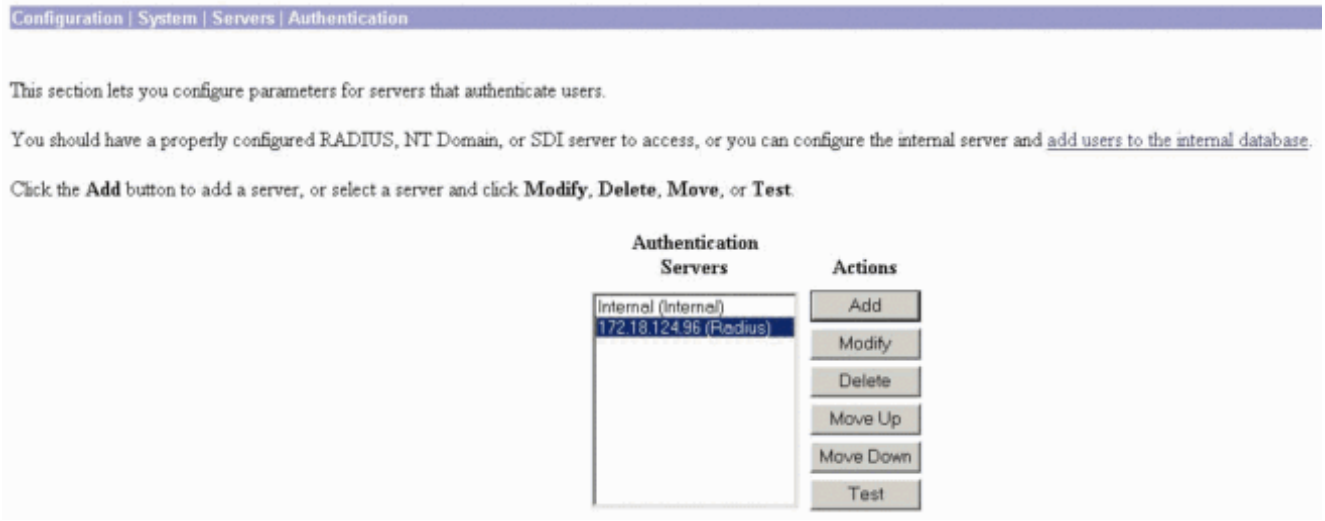


Тестирование функции окончания срока действия пароля NT/RADIUS

Концентратор предлагает функцию для тестирования Проверки подлинности RADIUS. Для тестирования этой функции должным образом удостоверьтесь, что вы выполняете эти действия тщательно.

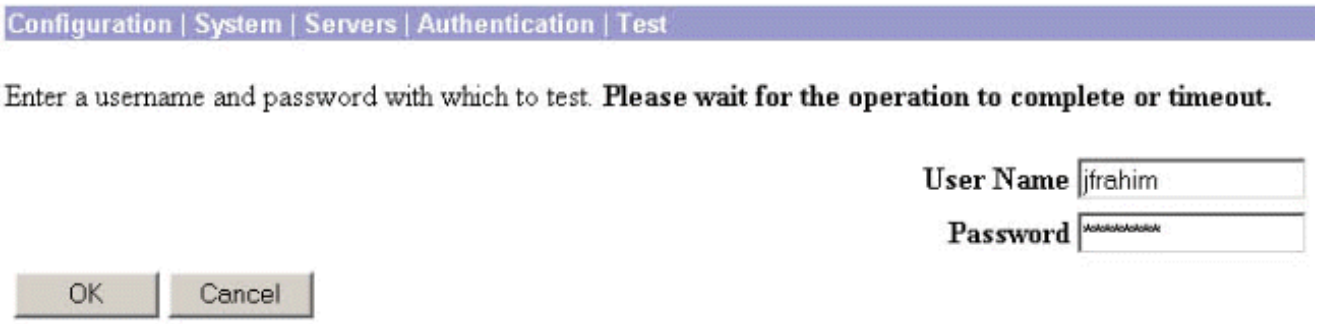
Тестирование аутентификации RADIUS

1. Перейдите к **Configuration> System> Servers> Authentication**. Выберите свой сервер RADIUS и нажмите
Test.



2. Когда предложено, введите свое доменное имя пользователя NT и пароль, и затем нажмите **OK**. Пример ниже имени пользователя показов "jfrahim" настроенный на

сервере домена NT с "cisco123" как
пароль.

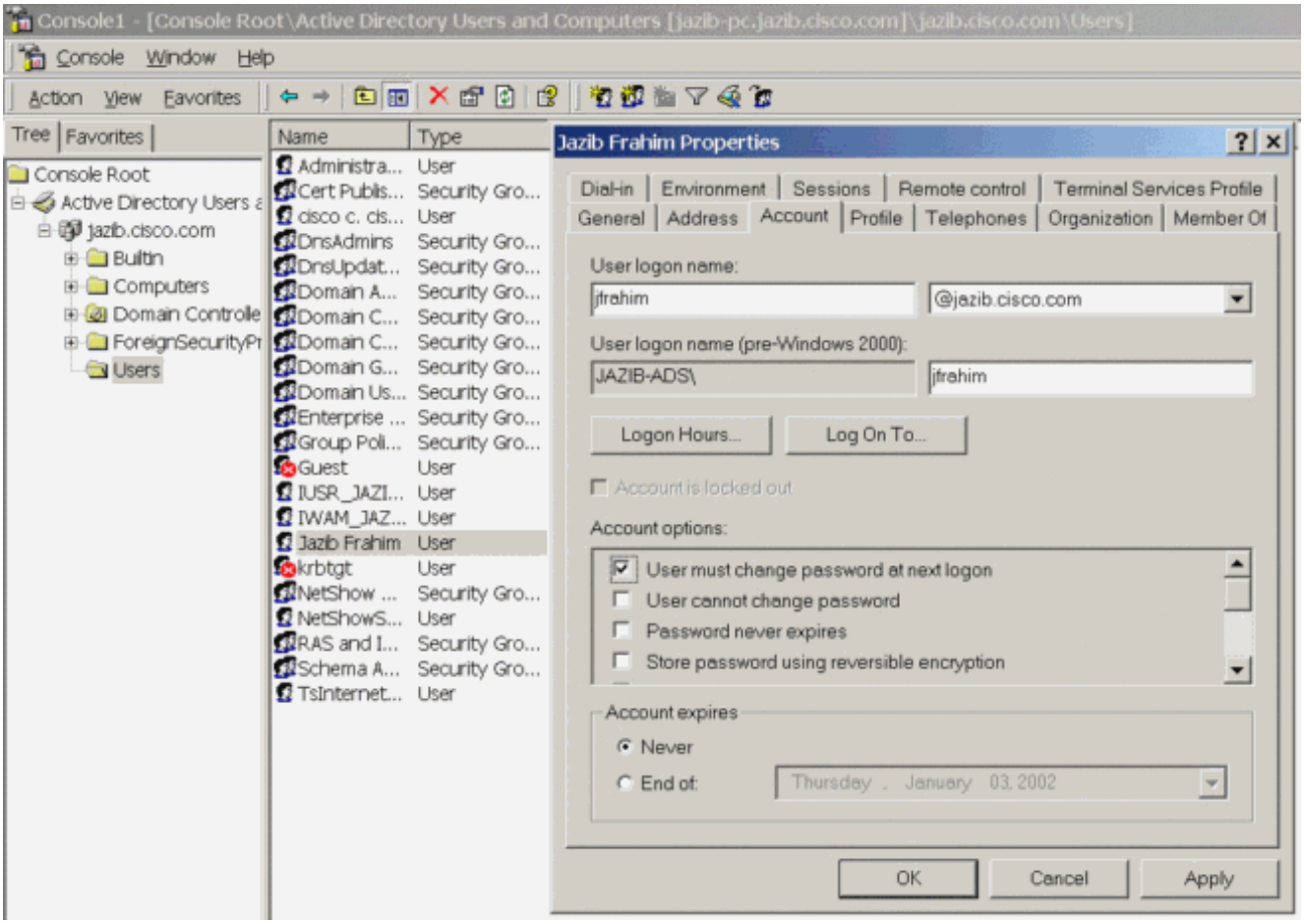


3. Если ваша аутентификация установлена должным образом, необходимо получить сообщение, сообщая "Успешную

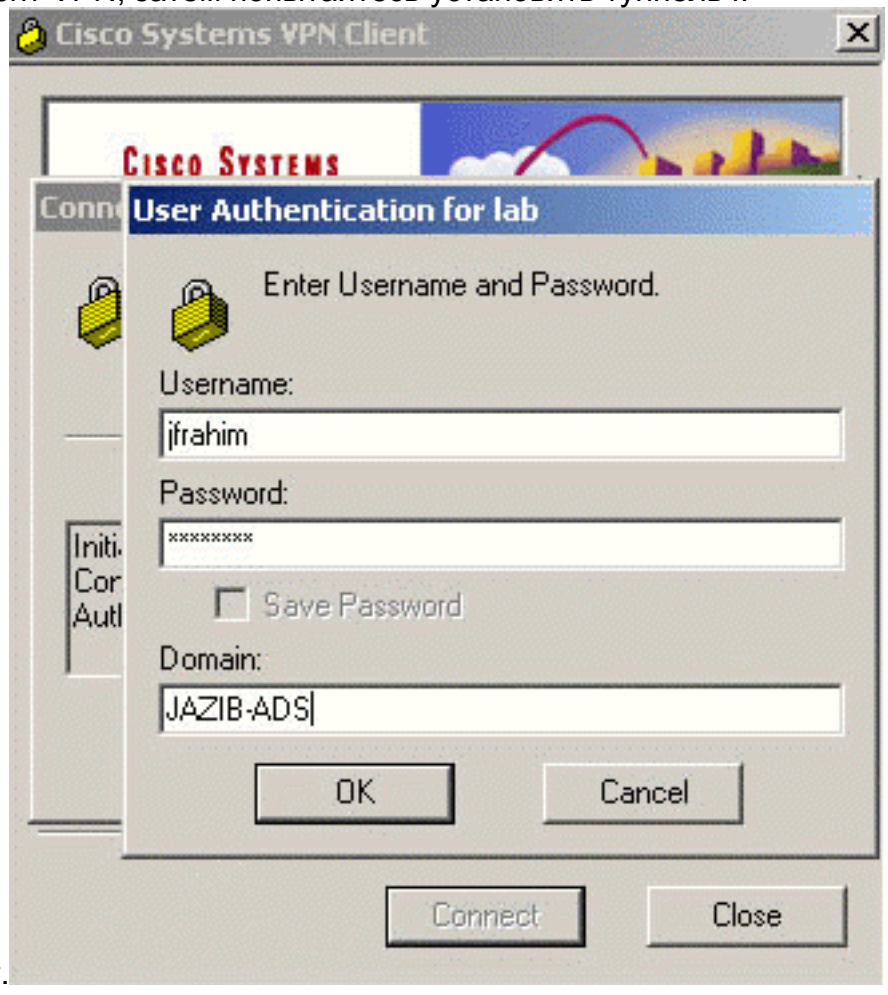
Аутентификацию". При получении какого-либо сообщения кроме один показанный выше существует некоторая конфигурация или проблема с подключением. Повторите конфигурацию и шаги тестирования, выделенные в этом документе, чтобы гарантировать, что все настройки были установлены должным образом. Также проверьте возможность подключения с помощью IP-адреса между своими устройствами.

Фактическая аутентификация в домене NT использует прокси-сервер RADIUS для тестирования функции истечения срока действия пароля

1. Если пользователь уже определен на сервере домена, модифицируйте свойства так, чтобы пользователю предложили изменить пароль при следующем входе в систему. Перейдите к вкладке "Account" диалогового окна со свойствами пользователя, выберите опцию для **Пользователя, должен изменить пароль при следующем входе в систему**, затем нажать
OK.



2. Запустите клиент VPN, затем попытайтесь установить туннель к концентратору.



3. Во время Проверки подлинности пользователя вам нужно предложить изменить

пароль. 

Дополнительные сведения

- Концентратор серии Cisco VPN 3000
- IPSec
- Cisco Secure Access Control Server for Windows
- RADIUS
- Запросы комментариев (RFC)