

27 февраля 2013 в 23:16

Mikrotik (vpn server) + Windows server 2008r2 (ad, radius server)

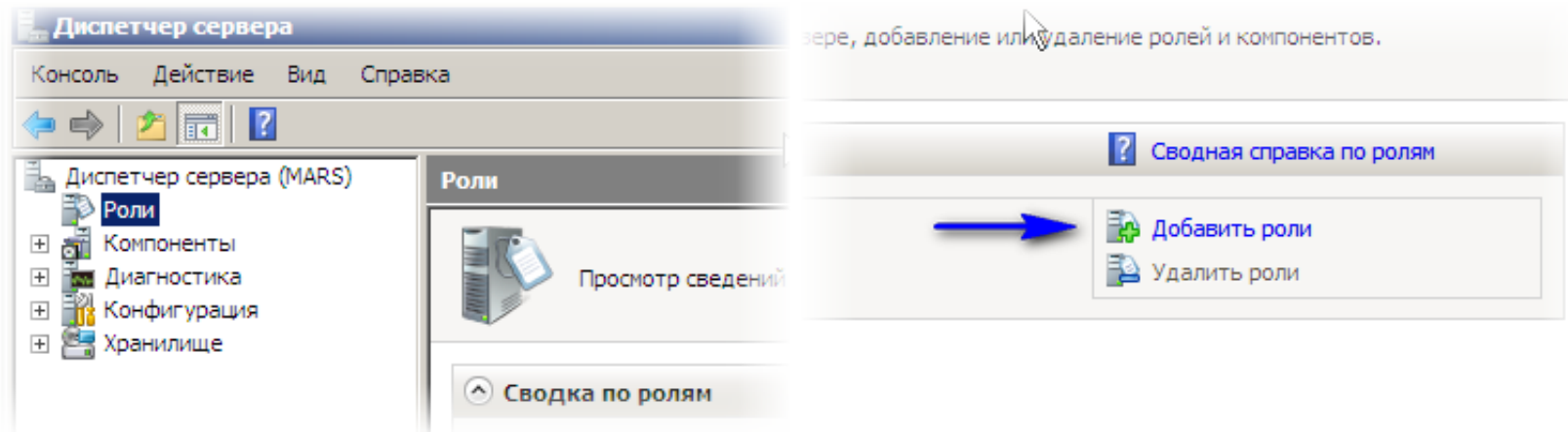
Доброго времени суток!

На днях поставили задачу, настроить удаленный доступ к серверу через VPN. До этого использовали доступ через удаленный рабочий стол. Закрыли доступ к серверу, осталось поднять VPN сервер и добавить пользователей, кому разрешен доступ из дома. В качестве шлюза в организации установлен Mikrotik 450g. Можно было бы просто включить VPN-сервер на Mikrotik'e и завести необходимое кол-во пользователей. Решил пойти другим путем, так как в компании на сервере поднят Active Directory, можно воспользоваться Radius-сервером на Windows 2008r2. И получим не плохую связку, что упростит нам работу в будущем по управлению доступом к серверу. И так опишу как все это дело настроить.

Для начала настроим **Radius-сервер**

Для работы radius сервера нам потребуется установить роль **Службы политики сети и доступа – NPS сервер**

И так открываем **Диспетчер сервера – Роли – Добавить роли**



Находим в списке Службы политики сети и доступа, нажимаем далее, появится информация о данной службе, если необходимо читаем или сразу нажимаем далее, выбираем какие службы данной роли необходимо включить. Для радиус сервера нам понадобится только Сервер политики сети, выбираем, нажимаем далее и установить.

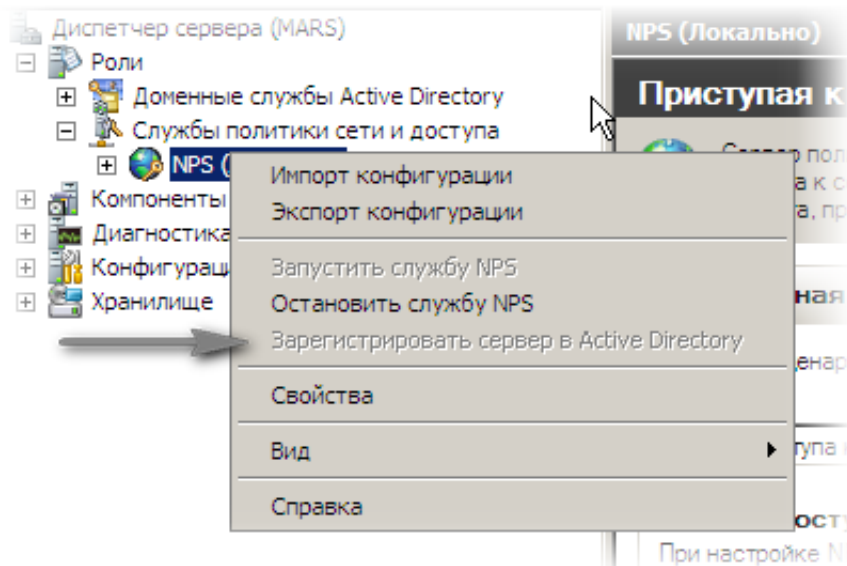
- Службы UDDI
- Службы печати
- Службы политики сети и доступа
- Службы развертывания Windows
- Службы сертификации Active Directory
- Службы терминалов
- Службы управления правами Active Directory
- Службы федерации Active Directory
- Файловые службы
- Факс-сервер

Выберите службы ролей для установки для Службы политики сети

Службы роли:

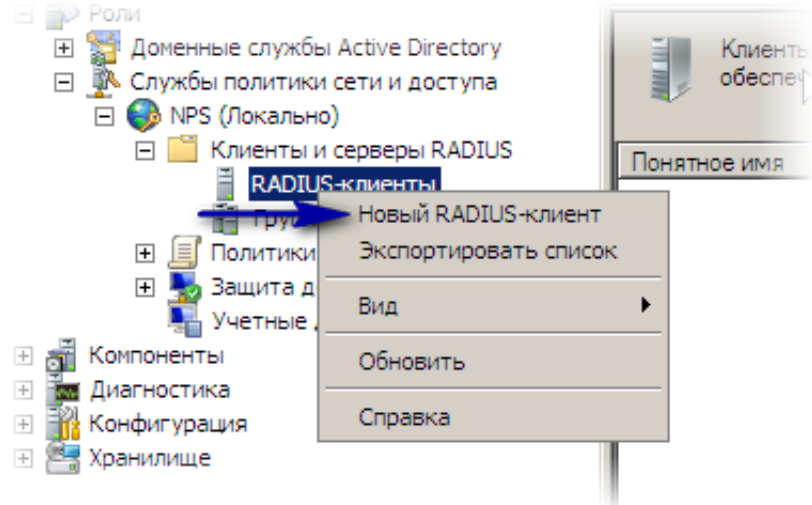
- Сервер политики сети**
- Службы маршрутизации и удаленного доступа
 - Служба удаленного доступа
 - Маршрутизация
- Центр регистрации работоспособности
- Протокол авторизации учетных данных узла

После установки службы, необходимо ее зарегистрировать в Active Directory, это требуется для применения групповых политик применяемых на сервере. Вот тут у меня и возникли проблемы, кнопка активации была не активна.



Причину я не нашел, но двигаемся дальше.

Переходим к настройке сервера. Теперь необходимо добавить radius-клиента. Для этого переходим: **Диспетчер сервера – Роли – Службы политики сети и доступа — NPS (Локально) – Клиенты и серверы RADIUS – RADIUS-клиенты**. Кликаем правой кнопкой мыши на **RADIUS-клиенты**, нажимаем на **Новый RADIUS-клиент**.



В открывшемся диалоговом окне заполняем поля:

- Понятное имя – имя радиус клиента (задается произвольно);
- Адрес (IP или DNS) – тут все понятно, ip адрес либо dns-имя нашего устройства;
- Имя поставщика – поставщик radius клиента (можно оставить Standard);
- Общий секрет – пароль для авторизации радиус-клиента (пароль допустим 12345678).

Новый RADIUS-клиент

Включить RADIUS-клиент

Имя и адрес

Понятное имя:
mikrotik

Адрес (IP или DNS):
mikrotik

Поставщик

Укажите стандартный RADIUS для большинства RADIUS-клиентов или выберите поставщика RADIUS-клиента из списка.

Имя поставщика:
RADIUS Standard

Общий секрет

Чтобы ввести общий секрет вручную, выберите "Вручную". Чтобы автоматически создать общий секрет, выберите "Создать". RADIUS-клиент необходимо настроить с введенным здесь общим секретом. Общие секреты вводятся с учетом регистра.

Вручную Создать

Общий секрет:
●●●●●●

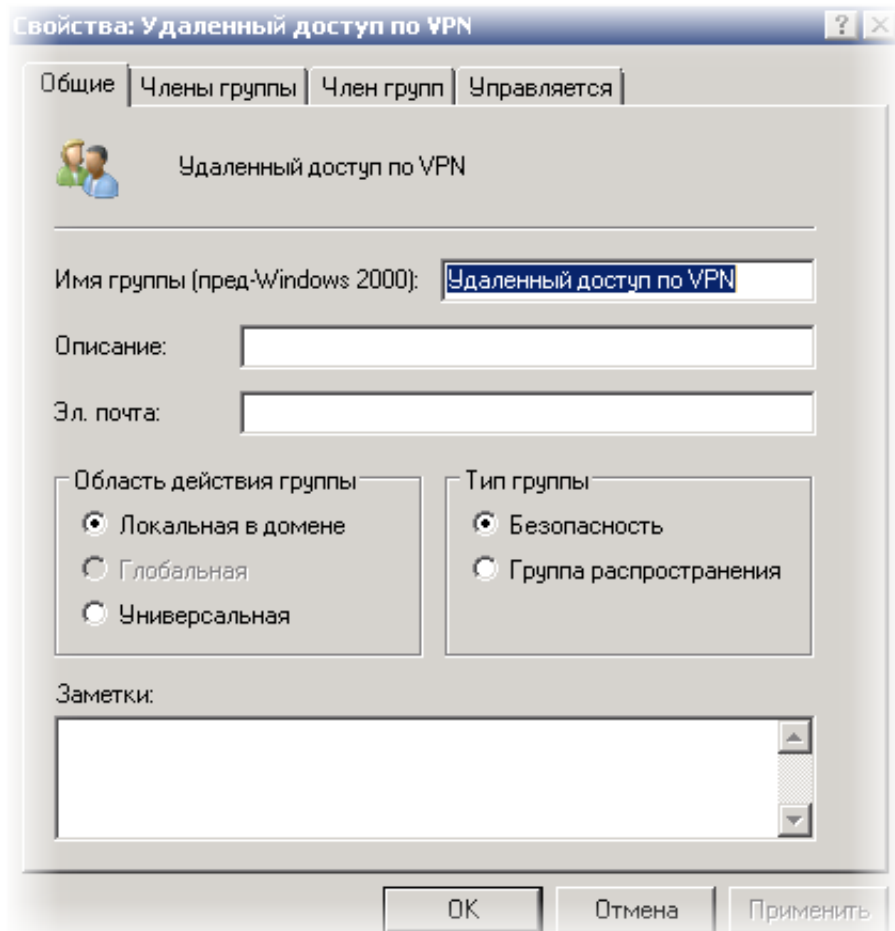
Подтверждение:
●●●●●●

Дополнительные параметры

Сообщения Access-Request должны содержать атрибут Message-Authenticator

RADIUS-клиент поддерживает NAP

Для того что бы настроить политику доступа, необходимо создать в Active Directory локальную группу безопасности. В данную группу будут входить пользователи, которым будет открыт доступ к серверу из дома. Назовем ее *Удаленный доступ по VPN*.



Создаем политику доступа. В службе NPS (Локально) открываем Политики кликаем правой кнопкой мыши **Сетевые политики – Новый документ**. В открывшемся окне заполняем поля:

- Имя политики — произвольное имя;
- Тип сервера доступа к сети – оставляем Unspecified.



Укажите имя политики сети и тип подключения

Можно указать имя политики сети и тип подключений, к которому применяется политика.

Имя политики:

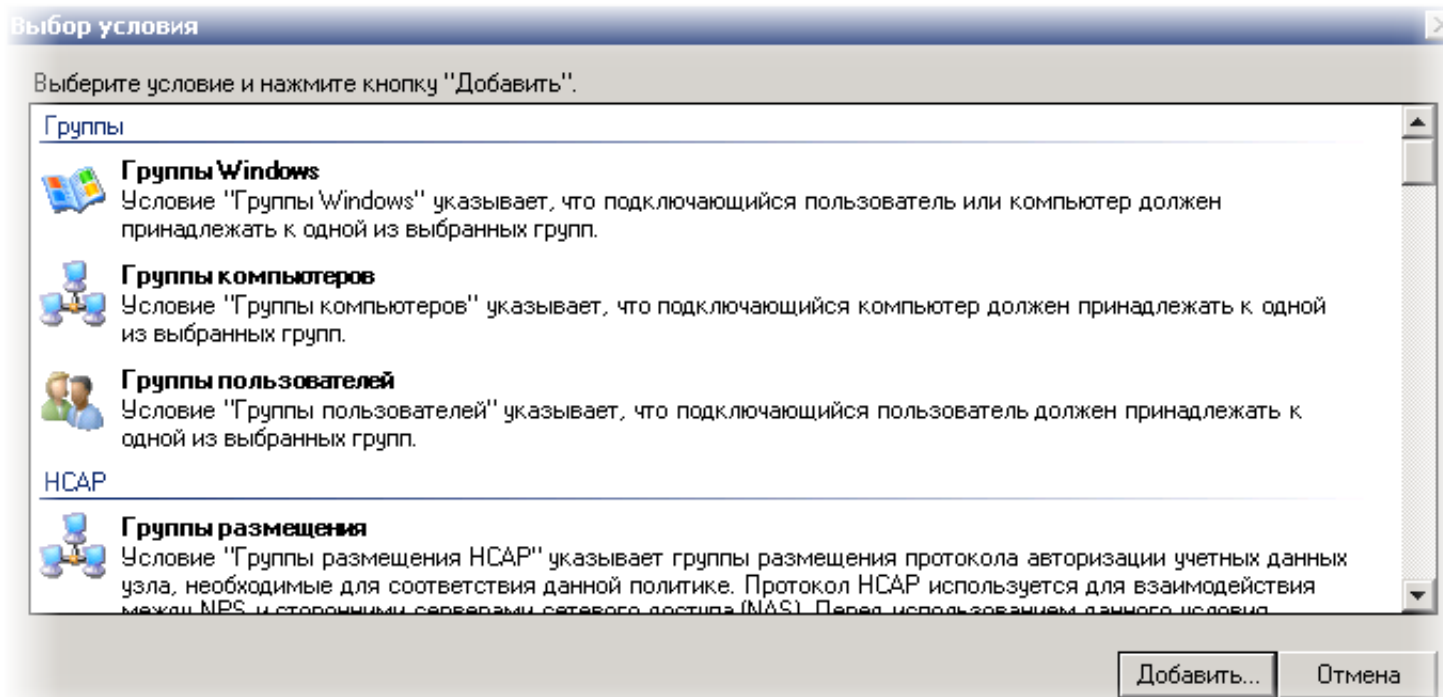
Способ сетевого подключения

Выберите тип сервера доступа к сети, отправляющего запрос на подключение серверу сетевых политик. Можно выбрать тип сетевого сервера или параметр "Зависящие от поставщика" (ни то, ни другое не является обязательным). Если в качестве сервера сетевых политик используется коммутатор 802.1X или беспроводная точка доступа, выберите "Не указано".

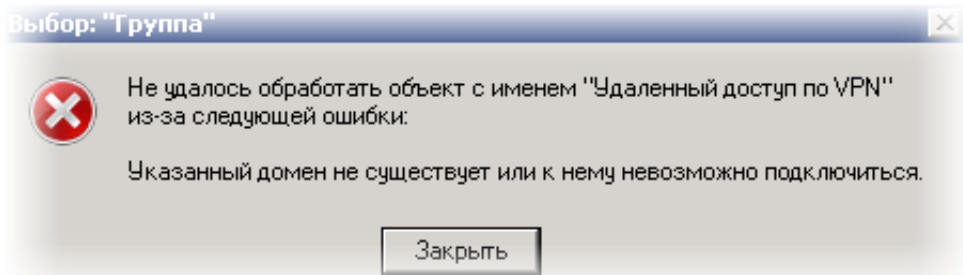
Тип сервера доступа к сети:

Зависящие от поставщика:

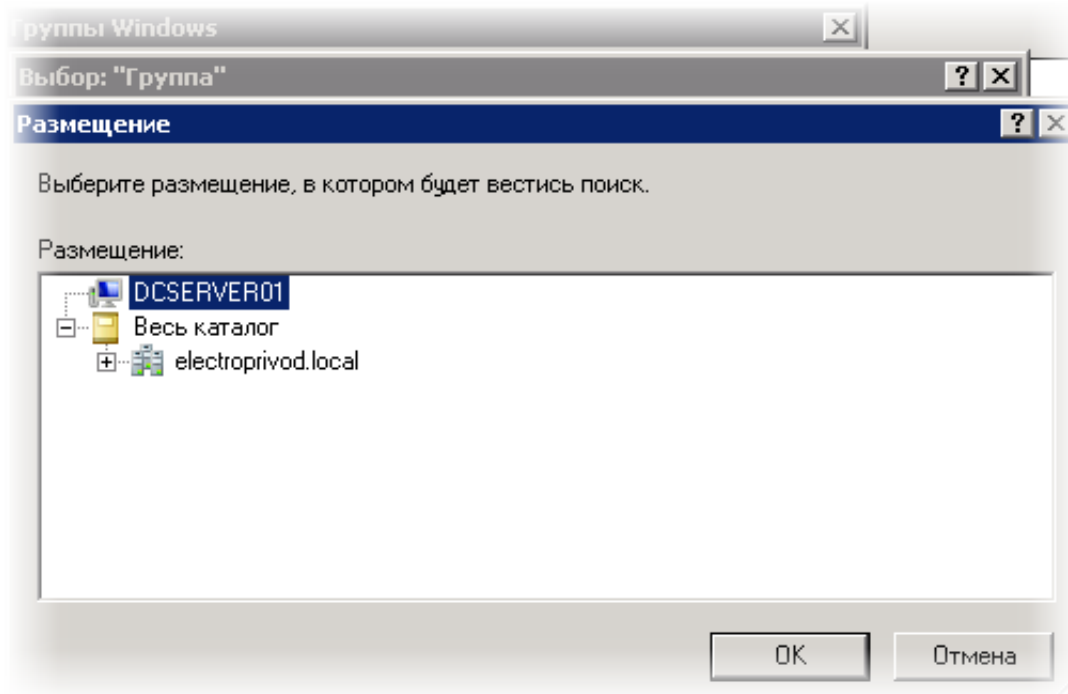
Нажимаем далее, откроется окно Выбор условия, тут все просто на основании чего будем разрешать или запрещать доступ. Нажимаем добавить, **Группы – Группы Windows**.



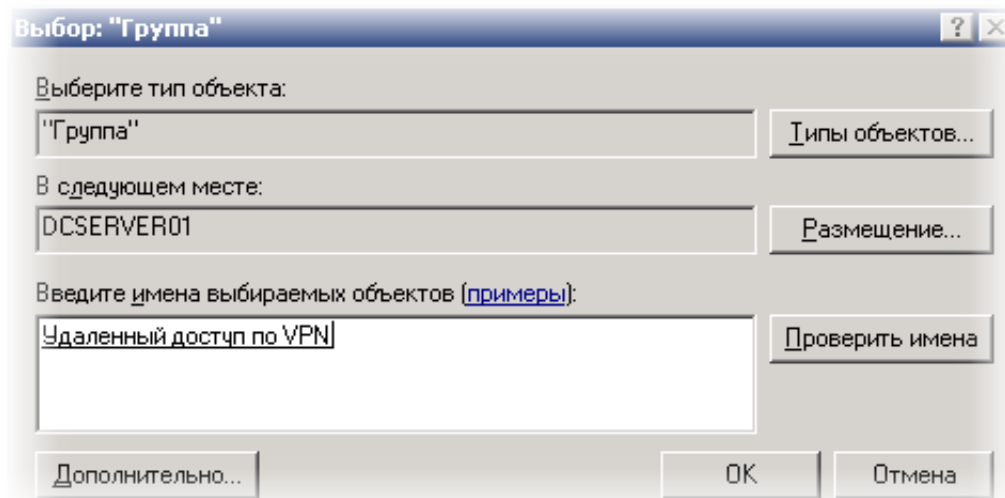
Как помните выше я писал, что у меня не получалось зарегистрировать **Сервер политик сети (NPS (Локально))** в AD, точнее кнопка активации не активна, из-за данной проблемы при выборе группы безопасности выходит ошибка.



Проблему обошел следующим способом, при поиске группы безопасности, выбираем размещение не в домене, а на самом сервере (DNS имя сервера).




Далее уже находим созданную ранее группу Удаленный доступ по VPN. Нажимаем ОК.





Добавим еще одно условие, от какого radius-клиента разрешено подключение. **Свойства клиента RADIUS – Понятное имя клиента**, добавить. Тут указываем, имя Radius-клиента которого создавали ранее, в моем случае mikrotik.


Выберите условие и нажмите кнопку "Добавить".


 **Тип туннеля**
Условие "Тип туннеля" ограничивает политику только клиентами, создающими определенный тип туннеля, такой как PPTP или L2TP.

Свойства клиента RADIUS

 **Код вызывающей станции**
Условие "Код вызывающей станции" задает телефонный номер сервера доступа к сети, набираемый клиентом доступа.

 **Понятное имя клиента**
Условие "Понятное имя клиента" задает имя RADIUS-клиента, передавшего на NPS запрос на подключение.

 **IPv4-адрес клиента**
Условие "IP-адрес клиента" задает IP-адрес клиента RADIUS, передавшего NPS запрос на подключение.

 **IPv6-адрес клиента**
Условие "IPv6-адрес клиента" задает IPv6-адрес RADIUS-клиента, переславшего NPS данный запрос на подключение.



Нажимаем ок, в итоге у нас получается 2 условия, идем далее.



Укажите условия

Задайте условия, определяющие, используется ли данная политика сети для запросов на подключение.
Необходимо указать хотя бы одно условие.

Условия:

Условие	Значение
 Группы Windows	ELECTROPRIVOD\Удаленный доступ по VPN
 Понятное имя клиента	mikrotik

Описание условия:

Условие "Понятное имя клиента" задает имя RADIUS-клиента, передавшего на NPS запрос на подключение.

Укажите разрешение доступа – Доступ разрешен.



Укажите разрешение доступа

Укажите, предоставлять или запрещать сетевой доступ, если запрос на подключение соответствует данной политике.

- Доступ разрешен
Предоставить доступ, если при попытке подключения клиента имеется соответствие условиям политики.
- Доступ запрещен
Запретить доступ, если при попытке подключения клиента имеется соответствие условиям политики.
- Доступ определяется свойствами удаленного доступа пользователя (переопределяющими политику NPS)
Предоставить или запретить доступ в соответствии со свойствам удаленного доступа пользователя, если при попытке подключения клиента имеется соответствие условиям политики.

Далее **Настройка методов проверки подлинности** выбираем метод шифрование mschap и mschap2.



Настройка методов проверки подлинности

Настройте один или несколько методов проверки подлинности, которые требуются для соответствия запроса на подключение данной политике. Для проверки подлинности EAP необходимо настроить тип EAP. Для развертывания NAP с использованием 802.1X или VPN необходимо настроить защищенный EAP в политике запроса на подключение, которая переопределяет параметры проверки подлинности политики сети.

Типы EAP согласуются между сервером сетевых политик (NPS) и клиентом в порядке перечисления.

Типы EAP:

Вверх

Вниз

Добавить...

Изменить...

Удалить

Менее безопасные методы проверки подлинности:

- Шифрованная проверка подлинности (Microsoft), версия 2, (MS-CHAP-v2)
 - Разрешить смену пароля по истечении срока действия
- Шифрованная проверка подлинности Microsoft (MS-CHAP)
 - Разрешить смену пароля по истечении срока действия
- Шифрованная проверка подлинности (CHAP)
- Проверка открытым тестом (PAP, SPAP)
- Разрешить подключение клиентов без согласования метода проверки подлинности.
- Выполнять только проверку работоспособности компьютера

Назад

Далее

Готово

Отмена

Далее **Настройка ограничений**, тут параметры можно оставить по умолчанию.



Настройка ограничений

Ограничения - это дополнительные параметры политики сети, которым должен соответствовать запрос на подключение. Если запрос на подключение не соответствует ограничению, NPS автоматически отклоняет запрос. Ограничения не являются обязательными; если настраивать их не требуется, нажмите кнопку "Далее".

Настроить ограничения для сетевой политики.

Если запрос на подключение не удовлетворяет всем ограничениям, доступ к сети запрещается.

Ограничения:

Ограничения	
Тайм-аут простоя	<p>Укажите в минутах максимальное время простоя сервера до прерывания подключения</p> <p><input type="checkbox"/> Максимальное время простоя до отключения</p> <p><input type="text" value="1"/></p>
Тайм-аут сеанса	
Идентификатор вызываемой станции	
Ограничения по дням недели и времени суток	
Тип порта NAS	

Настройка параметров, в Атрибуты RADIUS – Стандарт, удаляем атрибут Service-Type Framed, оставляем только PPP.



Настройка параметров

NPS применяет параметры к запросу на подключение, если выполняются все условия и ограничения для данной политики сети.

Настроить параметры для политики сети.

Если условия и ограничения соответствуют запросу на подключение, и политика предоставляет доступ, то параметры применяются.

Параметры:

Атрибуты RADIUS

- Стандарт
- Зависящие от поставщика
- Защита доступа к сети**
- Принудительное использование NAP
- Расширенное состояние
- Маршрутизация и удаленный доступ**
- Протокол распределения пропускной способности и многоканальных соединений (VAP)
- IP-фильтры

Чтобы отправить дополнительные атрибуты RADIUS-клиентам, выберите стандартный атрибут RADIUS и нажмите кнопку "Изменить". Если атрибут не задан, он не отправляется RADIUS-клиентам. Перечень необходимых атрибутов см. в документации RADIUS-клиента.

Атрибуты:

Имя	Значение
Framed-Protocol	PPP

На этом настройка Radius-сервера заканчивается. Нажимаем далее и готово.

Переходим к настройке Mikrotik'a.

Создадим пул ip адресов для подключения наших пользователей:

```
/ip pool add name=vpnserverusers ranges=10.0.18.2-10.0.18.99 next-pool=none
```

Профиль для VPN сервера:

```
/ppp profile add name=vpnserverhome use-encryption=yes change-tcp-mss=yes local-address=10.0.18.1 remote-address=vpnserverusers
```

В качестве VPN сервера выбрал PPTP сервер, включаем:

```
/interface pptp-server server set enabled=yes authentication=mschap1,mschap2 max-mtu=1460 max-mru=1460 default-profile=vpnserverhome
```

Необходимо включить авторизацию с помощью radius-сервера

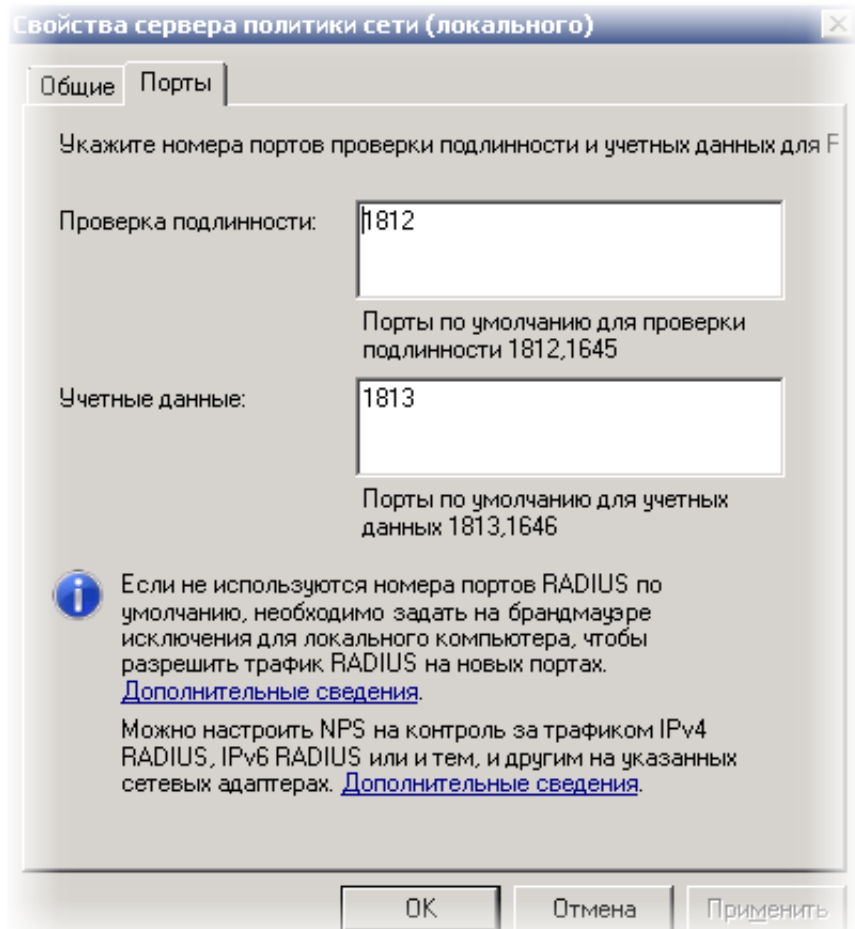
```
/ppp aaa set use-radius=yes accounting=yes
```

Включаем radius-клиент, и настраиваем его под наш сервер

```
/radius add service=ppp secret=12345678 address=192.168.0.100 authentication-port=1812 accounting-port=1813
```

Какие задействованы порты на нашем Radius-сервере можно посмотреть в свойствах Сервера политики сети

Диспетчер сервера – Роли – Службы политики сети и доступа — NPS (Локально) правой кнопкой мыши Свойства



Так же на микротике потребуется отключить **masquerade** в firewall'e для диапазона ip адресов 10.0.18.2-10.0.18.99, что бы наши пользователи не использовали интернет от данного соединения VPN.

```
/ip firewall nat edit number=1 src-address
```

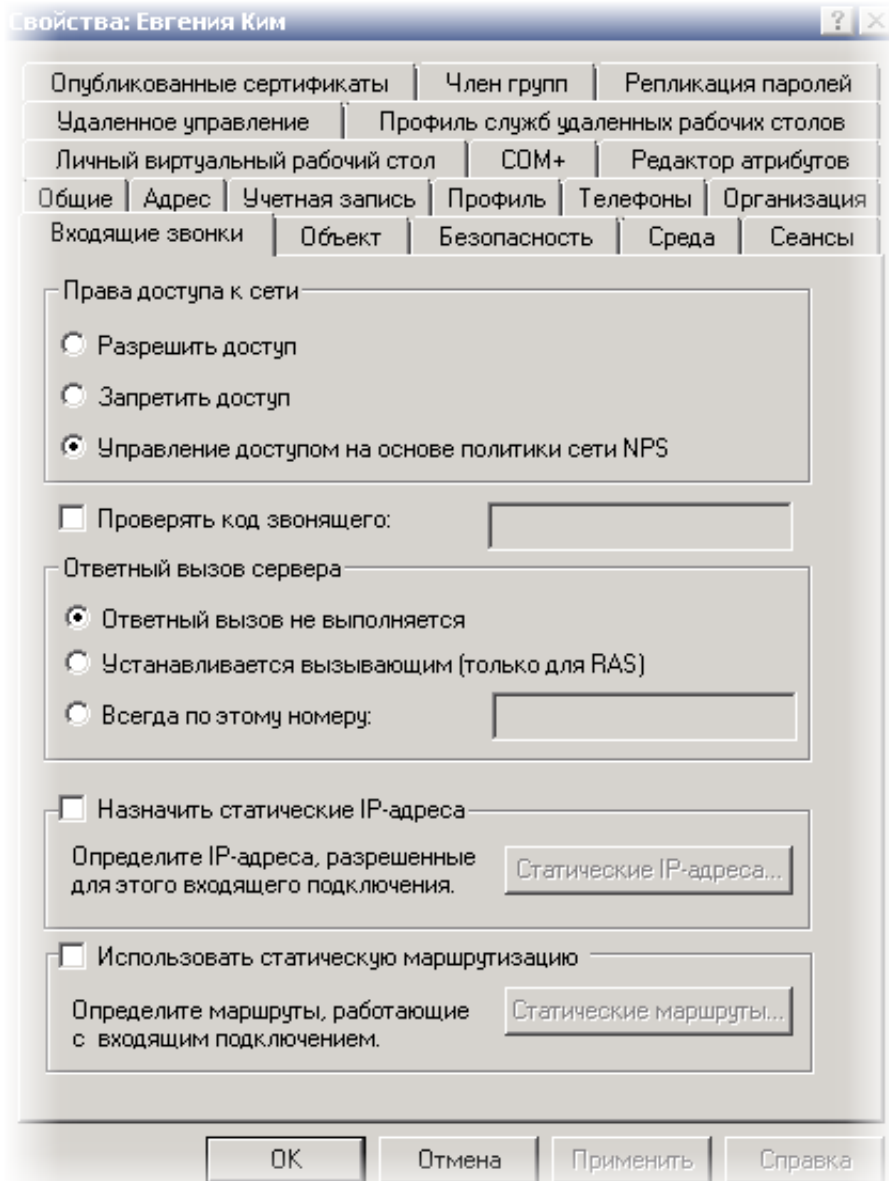
откроется окно, пишем наш диапазон

```
!10.0.18.2-10.0.18.99
```

У меня masquerade идет первым по списку в NAT, поэтому number=1.

Осталось только добавить в группу безопасности «Удаленный доступ по VPN», пользователей, которым разрешен доступ.

Есть еще момент, в свойствах учетной записи пользователя необходимо в настройках **Входящие звонки — Права доступа** к сети включить Управление доступом на основе политики NPS



Что бы у пользователей не возникло проблем с настройкой VPN соединения дома, и избавить себя от звонков в вечернее время. С помощью утилиты СМАК:

Пакет администрирования диспетчера подключений (СМАК) — это средство для настройки и управления способом подключения пользователей к Интернету или корпоративной частной сети.

создал автоматическое подключение для Windows7 (32 бит, 64 бит) и WindowsXP (32 бит), со стандартными настройками и написал не большую инструкцию как все это дома установить.

~~Несколько скриншотов делал уже после настройки на виртуальной машине, а именно добавление роли Службы политики сети и~~

доступа. Из-за этого разные dns-имена серверов:

mikrotik, vpn-сервер, windows server 2008 r2, radius

Испанский лётчик

Bitcoin: основные принципы майнинга

Стимпанк-кофейня в Южной Африке

Биржа убийств — правильное использование Bitcoin

Все мозги в одном месте

Q&A-сервис для разработчиков

Заказы для фрилансеров

Вакансии для айтишников

Уютная и дружелюбная