Построение корпоративных wifi сетей с авторизацией на microsoft radius

2018

Об авторе

Александр Рагозин

Системный администратор группы компаний HomeMe и MIXIT

по Северо-Западу

Сертификаты MikroTik

MTCNA, MTCTCE, MTCRE, MTCINE

Alexander@Ragozin.spb.ru

Требования к беспроводной сети

- Наличие централизованного управления
- Бесшовность сети
- Управление авторизацией через AD
- Разделение доступа через vlan
- Доступ до ресурсов сети вне зависимости от территориального расположения офиса

Алгоритм доступа в wifi сети

- Сотрудники центрального офиса должны из любого филиала иметь доступ до локальной сети своего офиса
- Сотрудники филиалов должны в своих офисах иметь доступ в общую сеть. В центральном офисе гостевой доступ (только интернет)

Исходная конфигурация

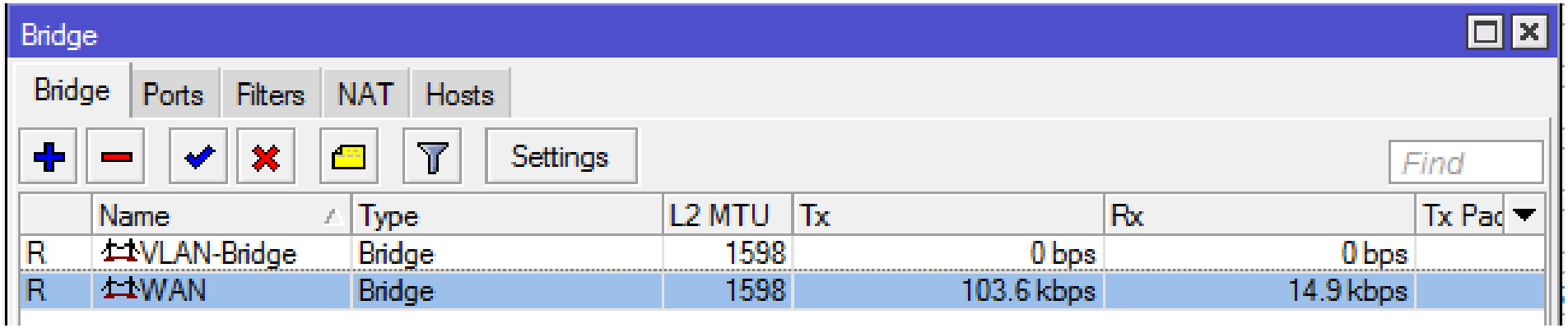
Настраивать Wifi будем в следующей сети:

- Все точки доступа и удалённые офисы связаны в единую сеть туннелями
- В сети созданы VLAN`ы для разграничения доступа к ресурсам:

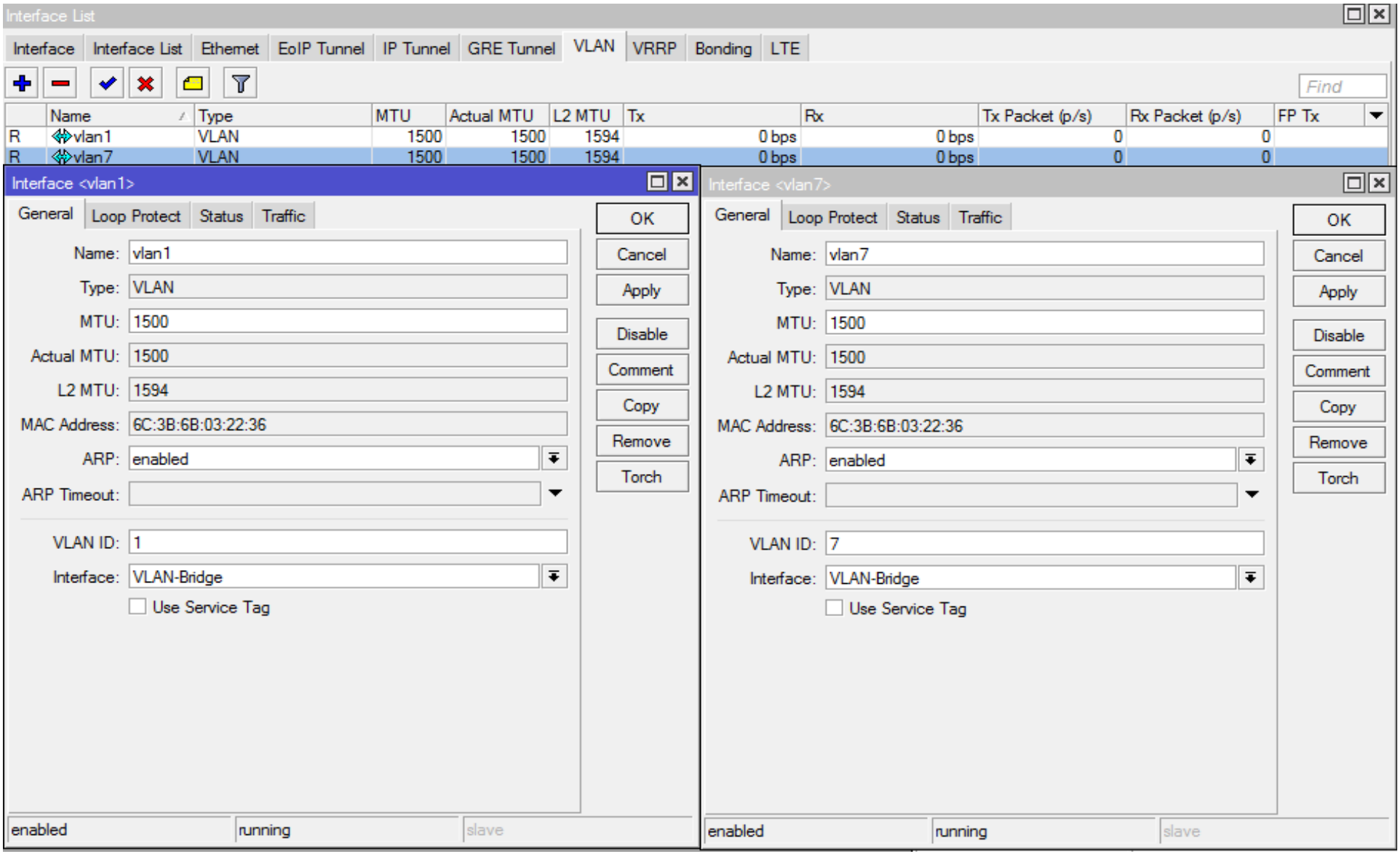
  VLAN 1 – Доступ ко всем ресурсам локальной сети

  VLAN 7 – В офисе Ограниченный доступ (только интернет)

  В филиалах – доступ в основную сеть
- Все VLAN`ы приходят на бридж VLAN-Bridge

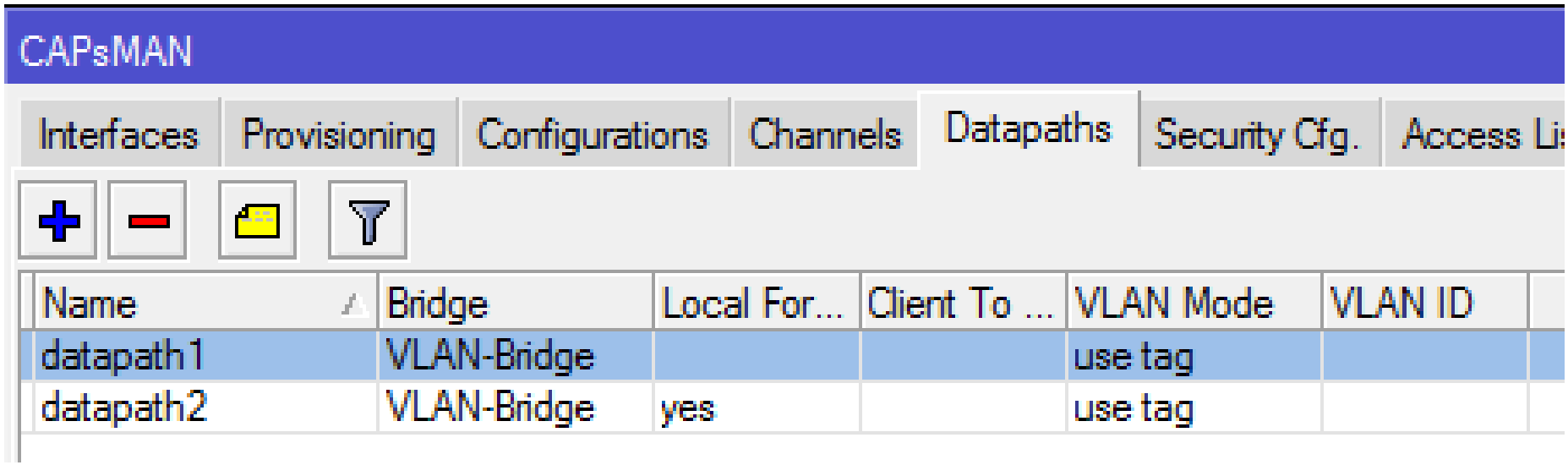


Созданные vlan`ы

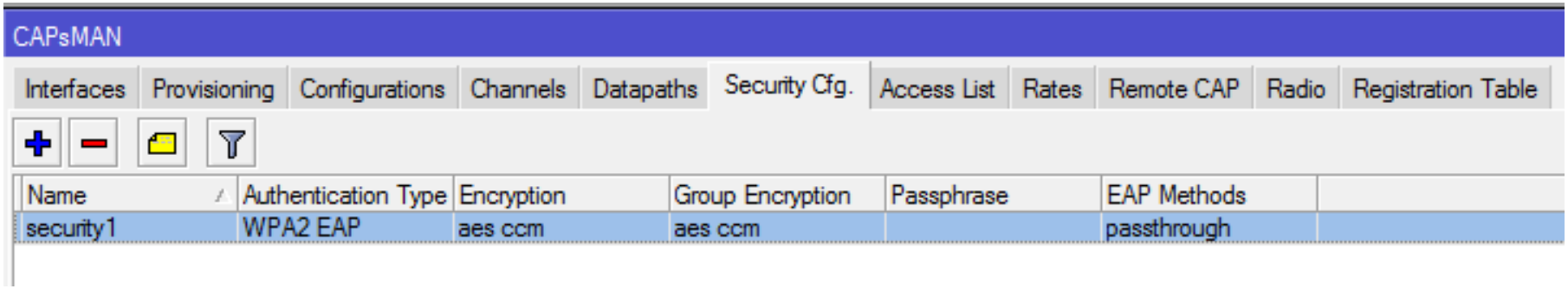


Настраиваем capsman

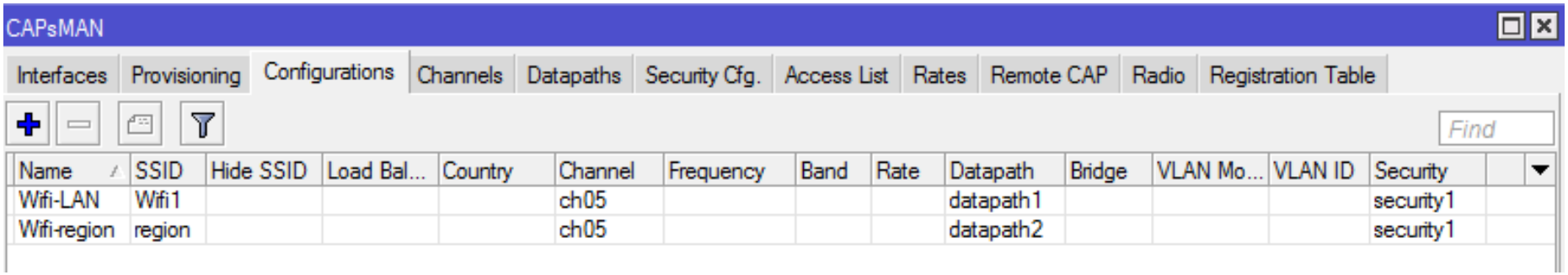
Создаём пути. Первый путь пойдёт на capsman, а второй путь пойдёт на точку доступа (это для филиалов)



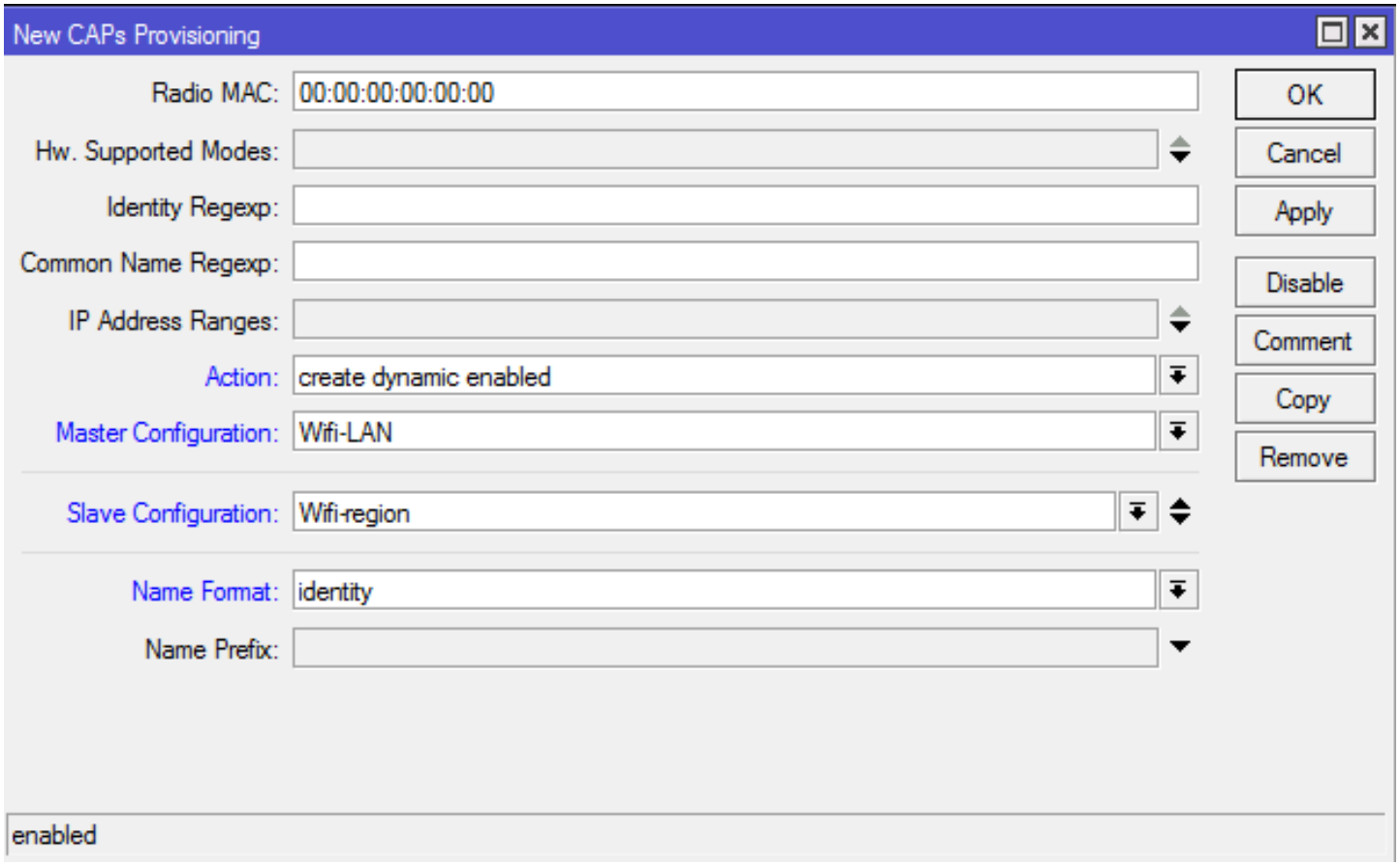
Безопасность настраиваем одну для всех, она будет направлять проверку на радиус



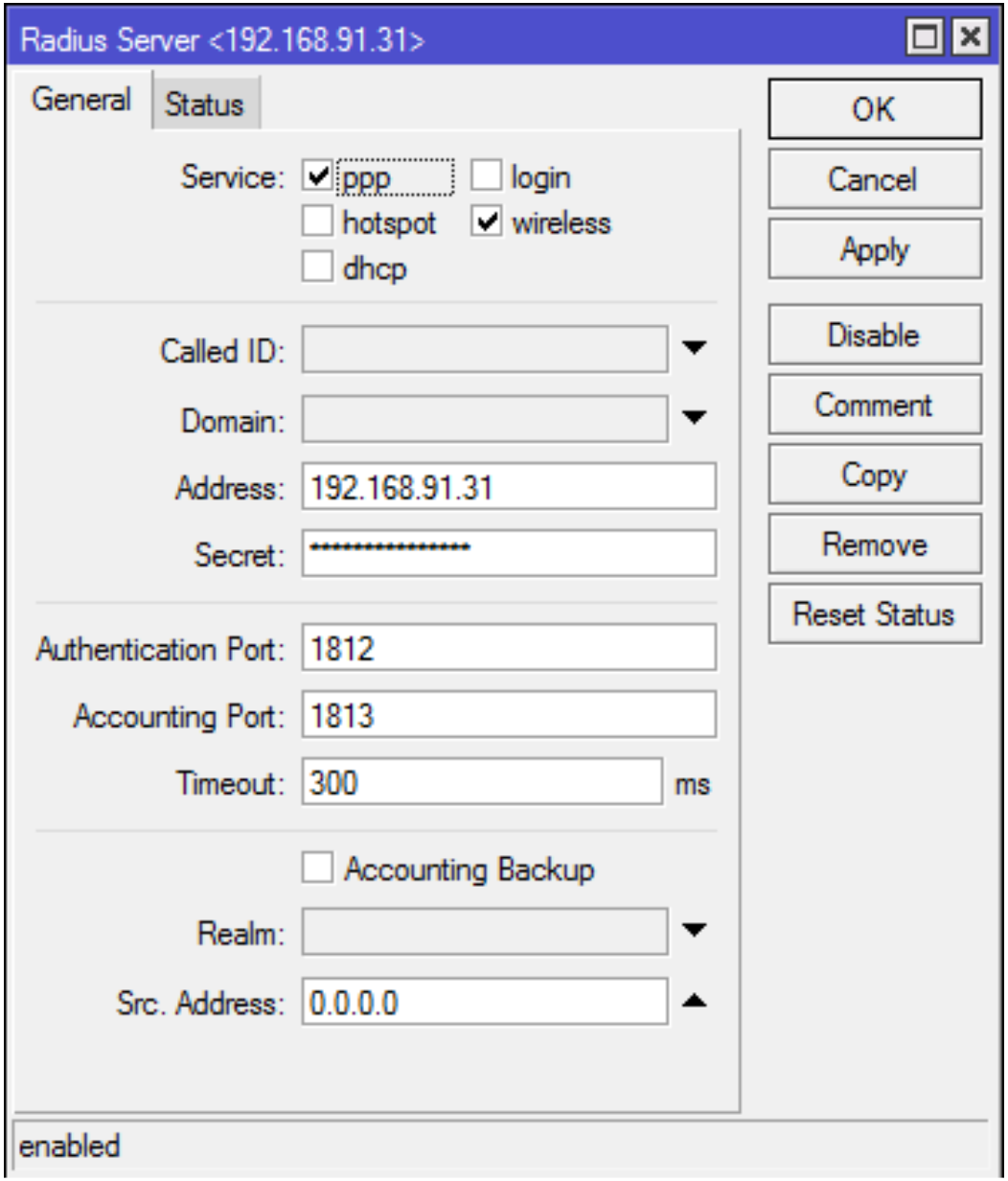
И создаём в capsman`е несколько сетей wifi1 – для всего офиса, region для сетей в регионах



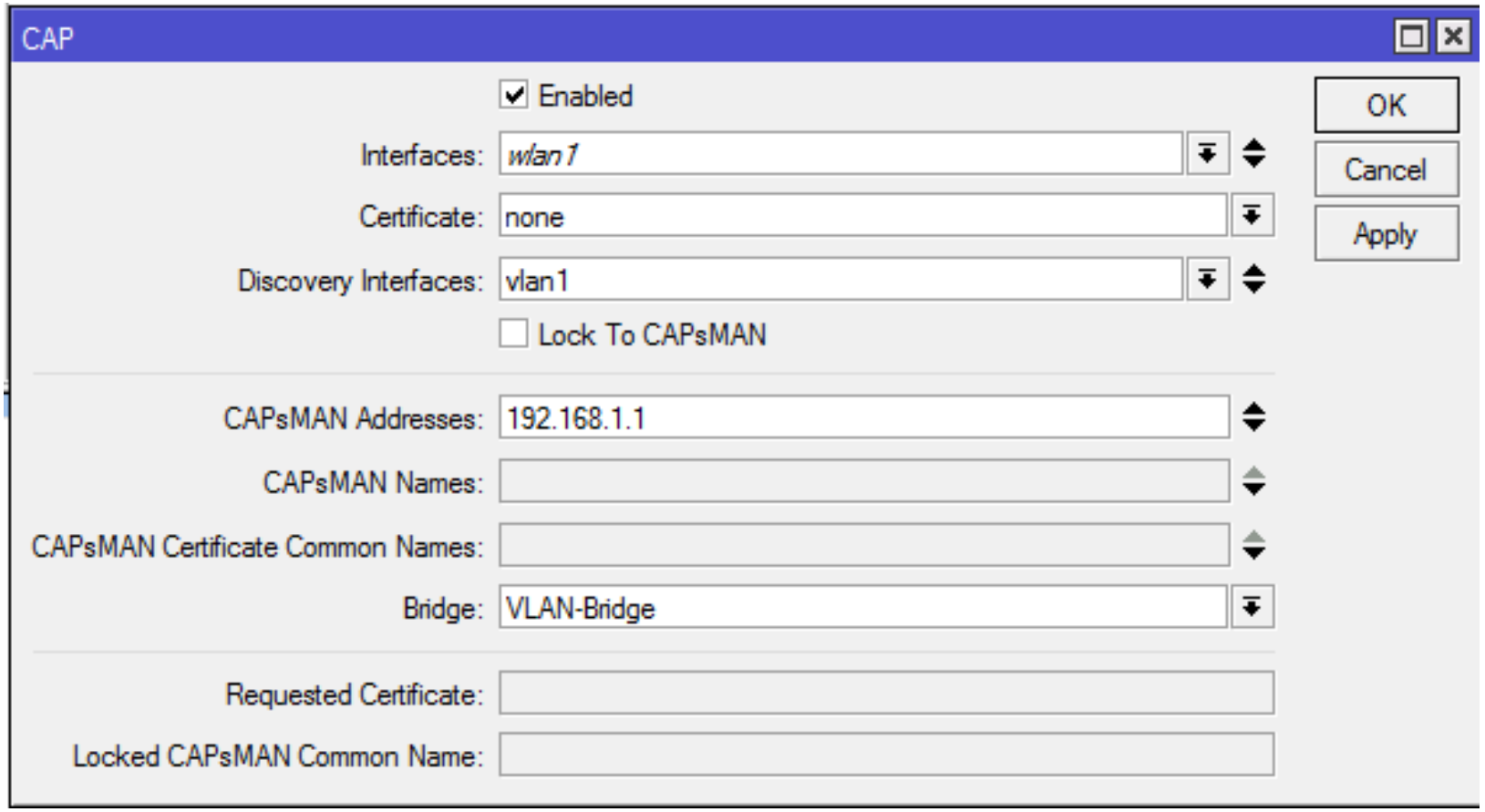
Настраиваем Provisioning для авто подключения точек или для каждой точки отдельно



Настраиваем radius, в этом примере передаются запросы от wifi и vpn

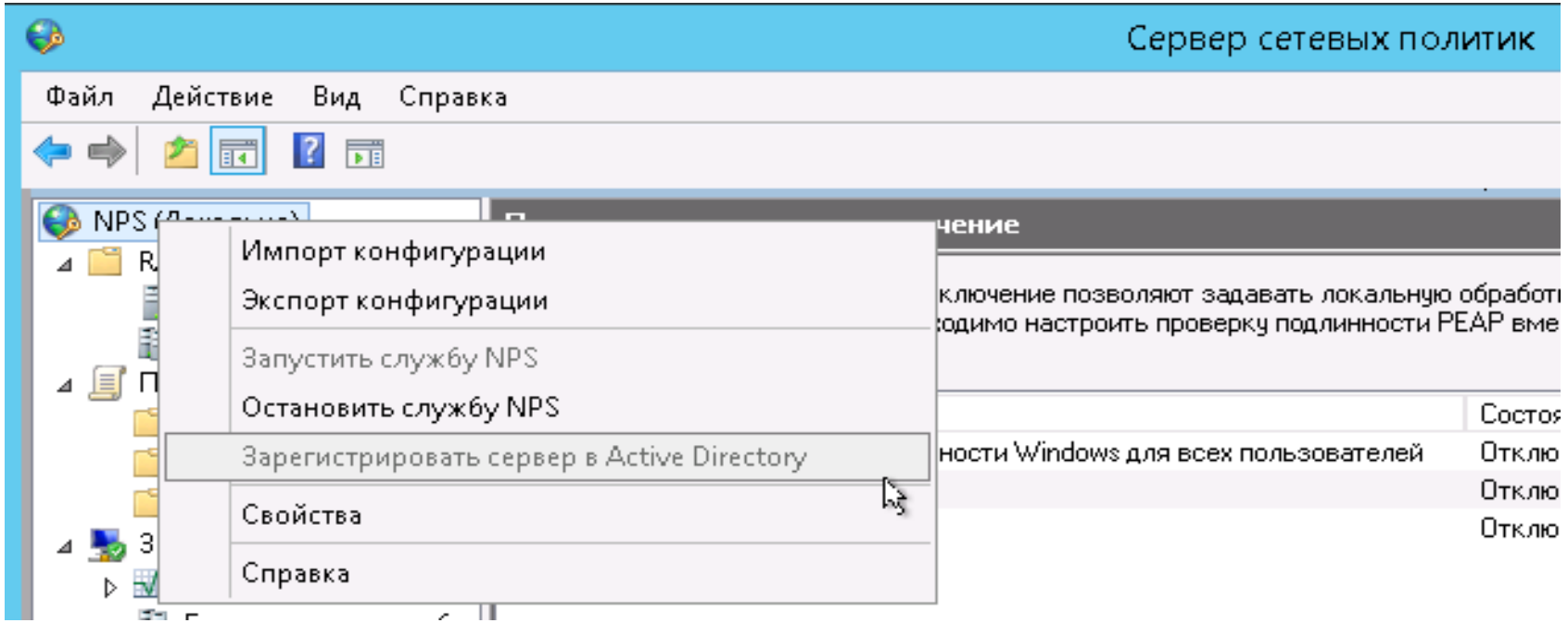


Включаем CAP на каждой точке.

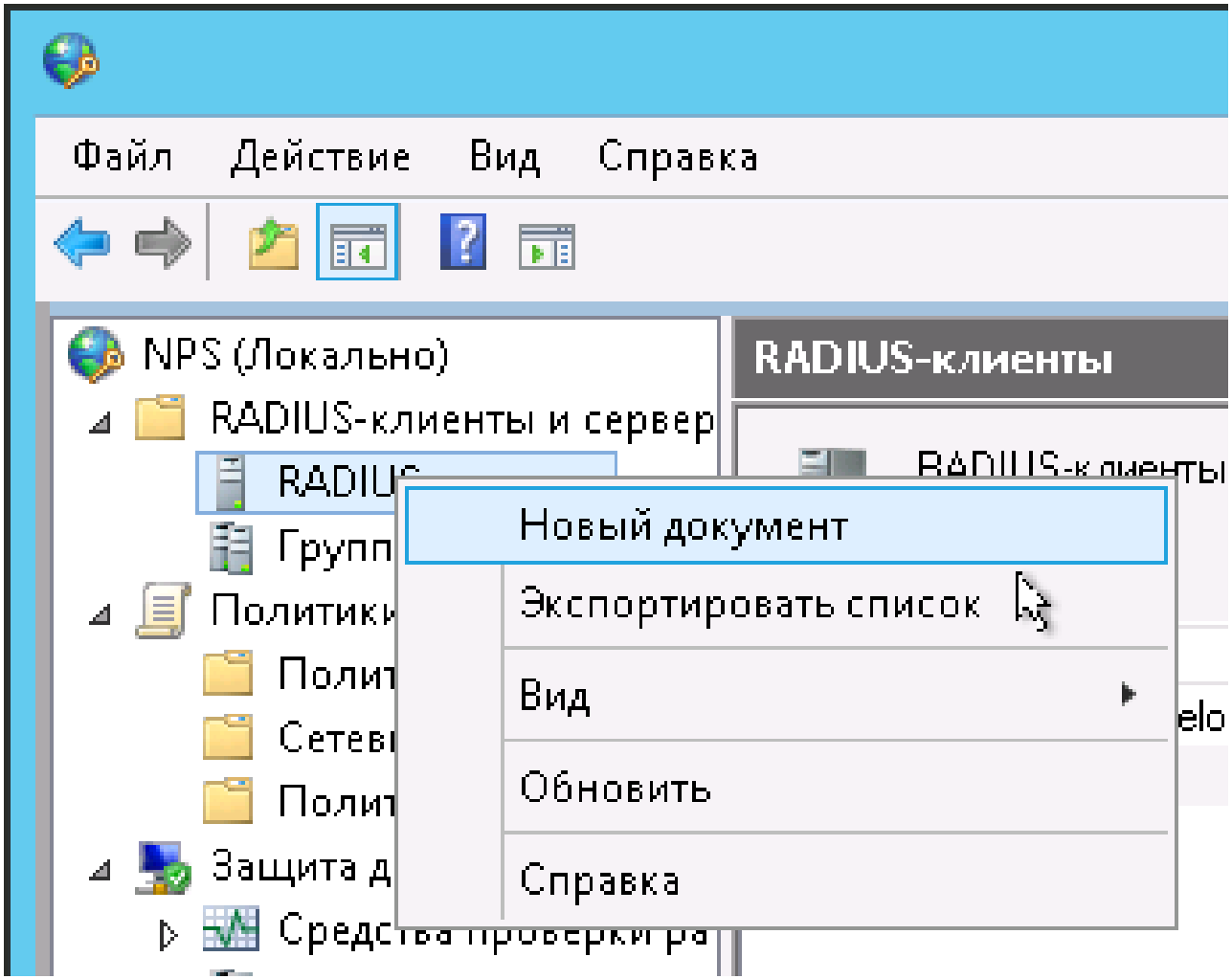


Настройка RADIUS сервера

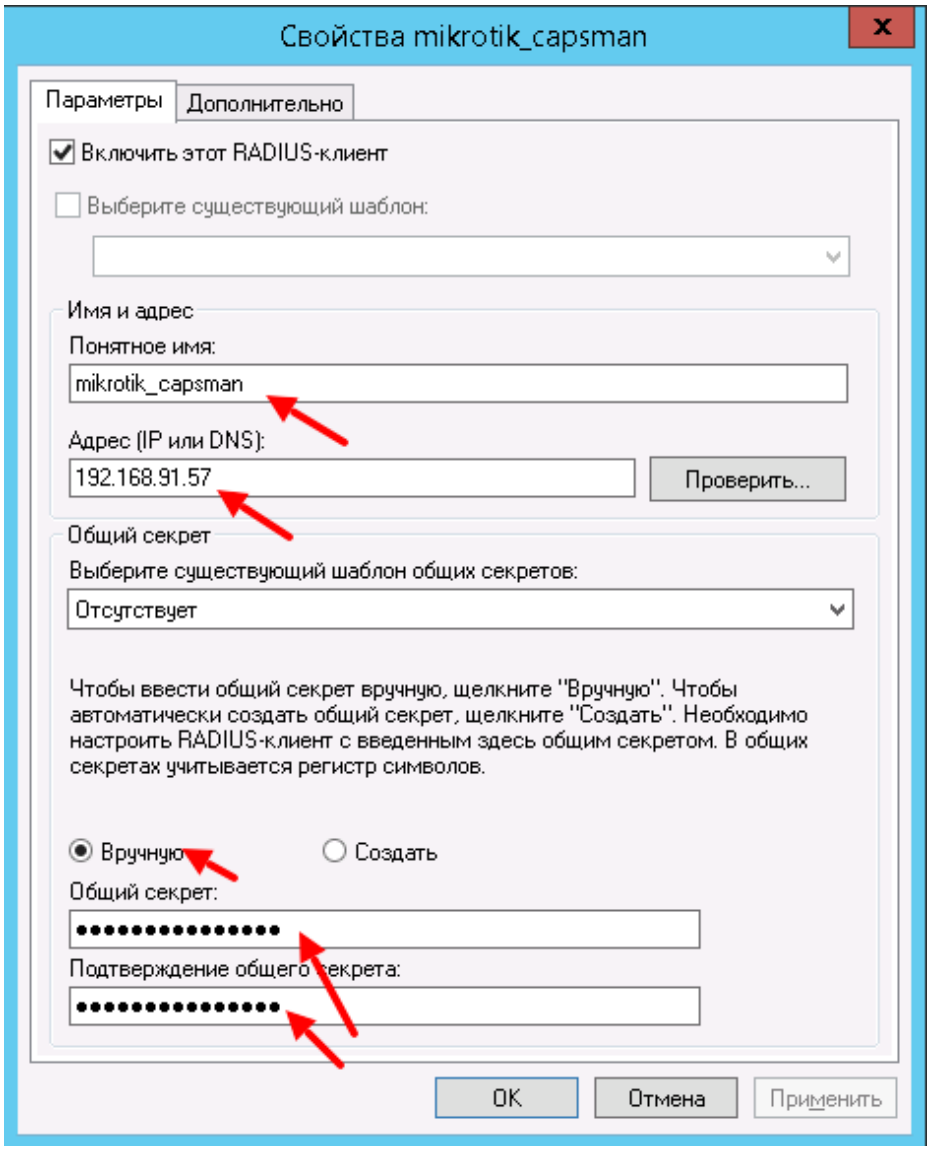
- Устанавливаем Сервер сетевых политик (NSP)
- Регистрируем его в AD



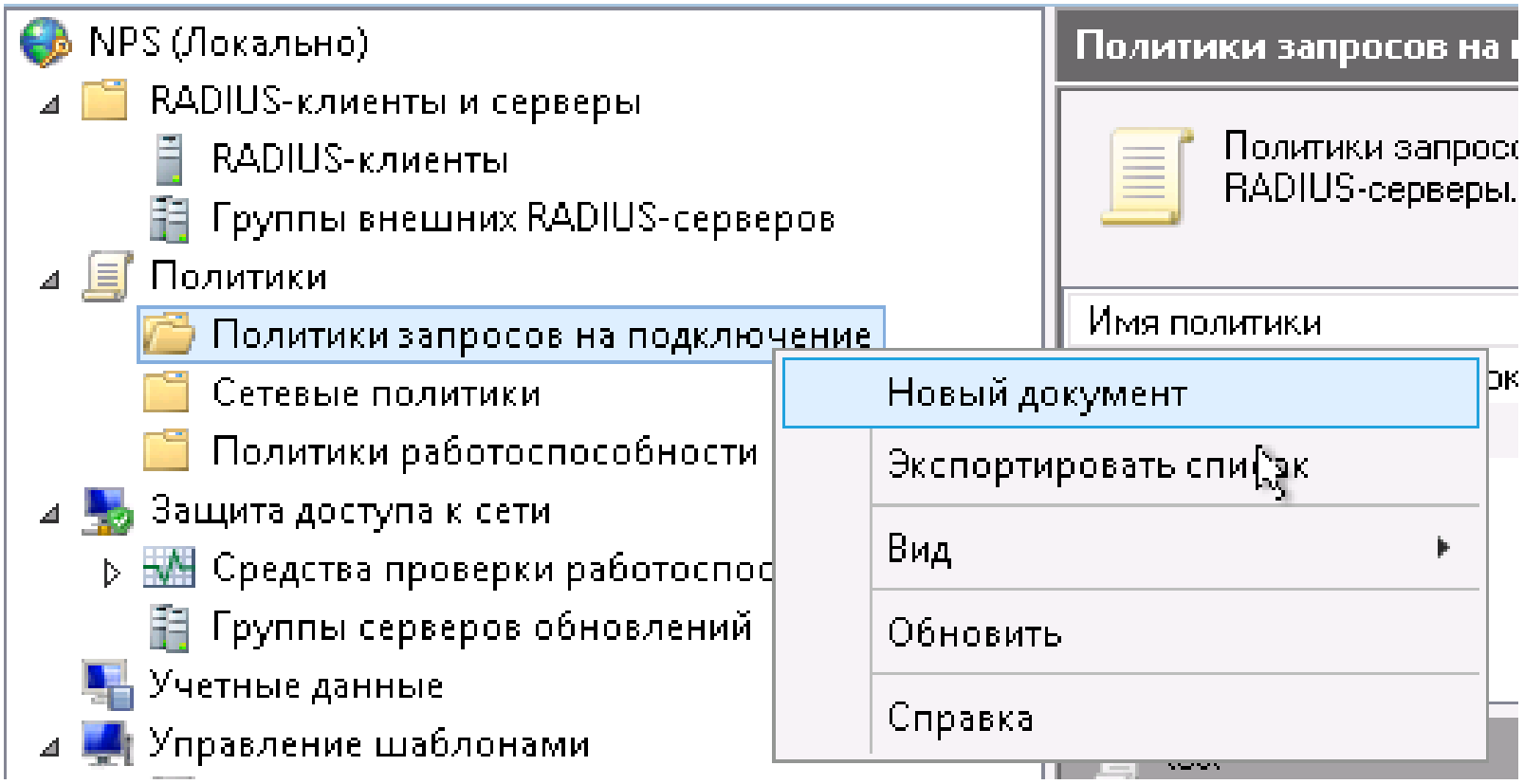
Добаваляем radius клиента (наш MikroTik)



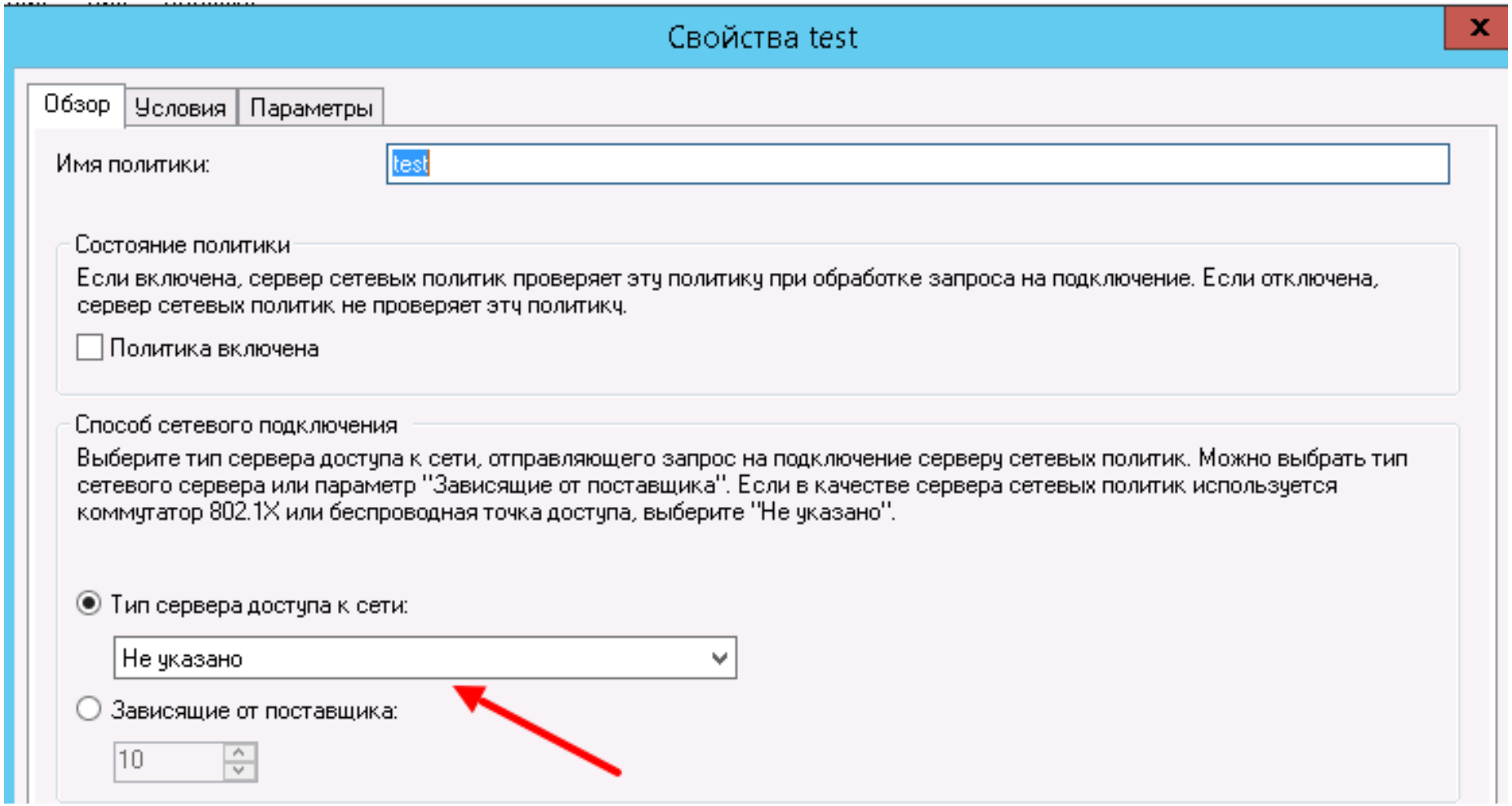
Вводим в поле “Понятное имя” название, по которому дальше будем идентифицировать запросы с этого MikroTik`a. Указываем адрес нашего capsman`a и введённый на нём секрет



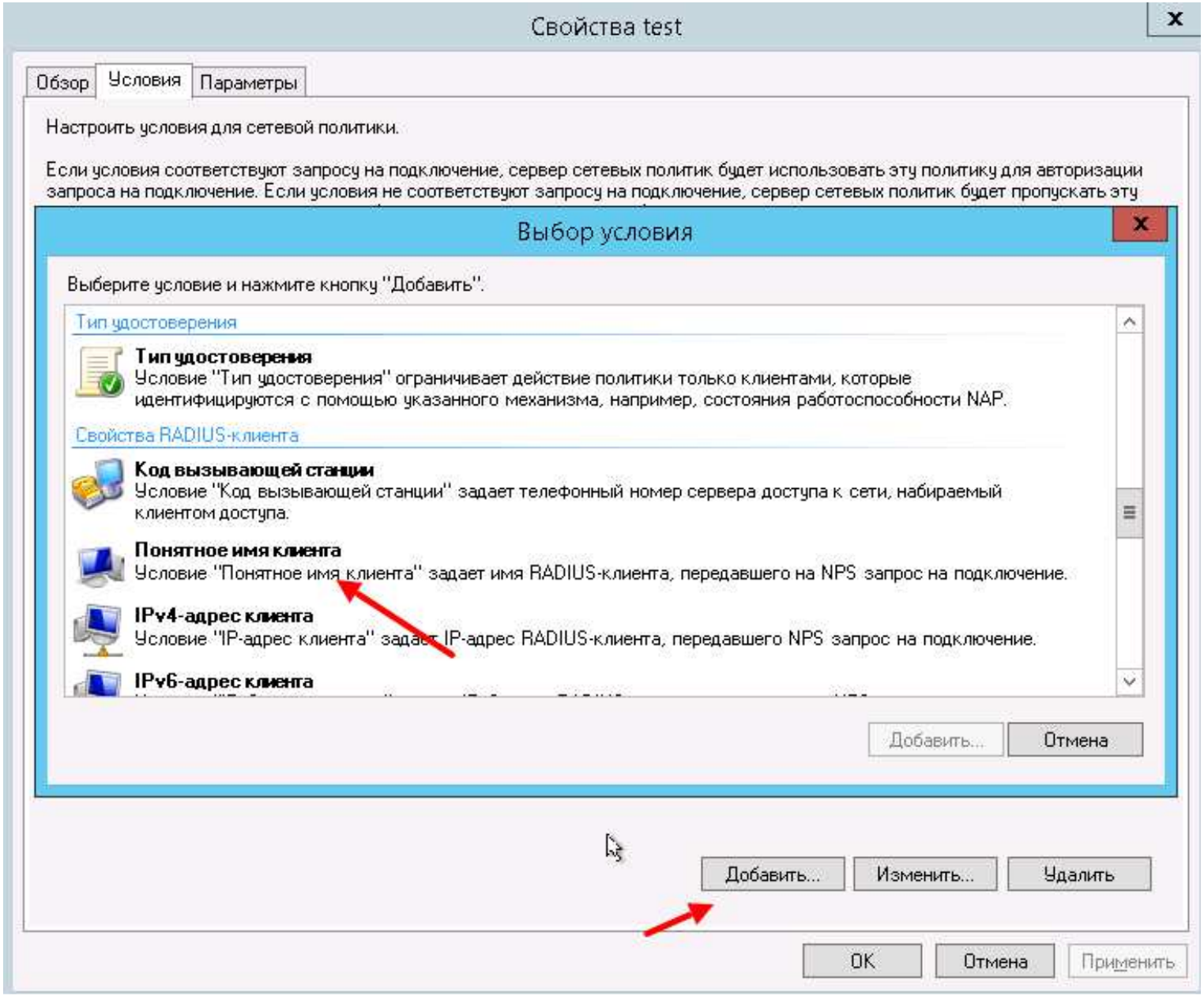
Создаём политику запросов, одну на capsman



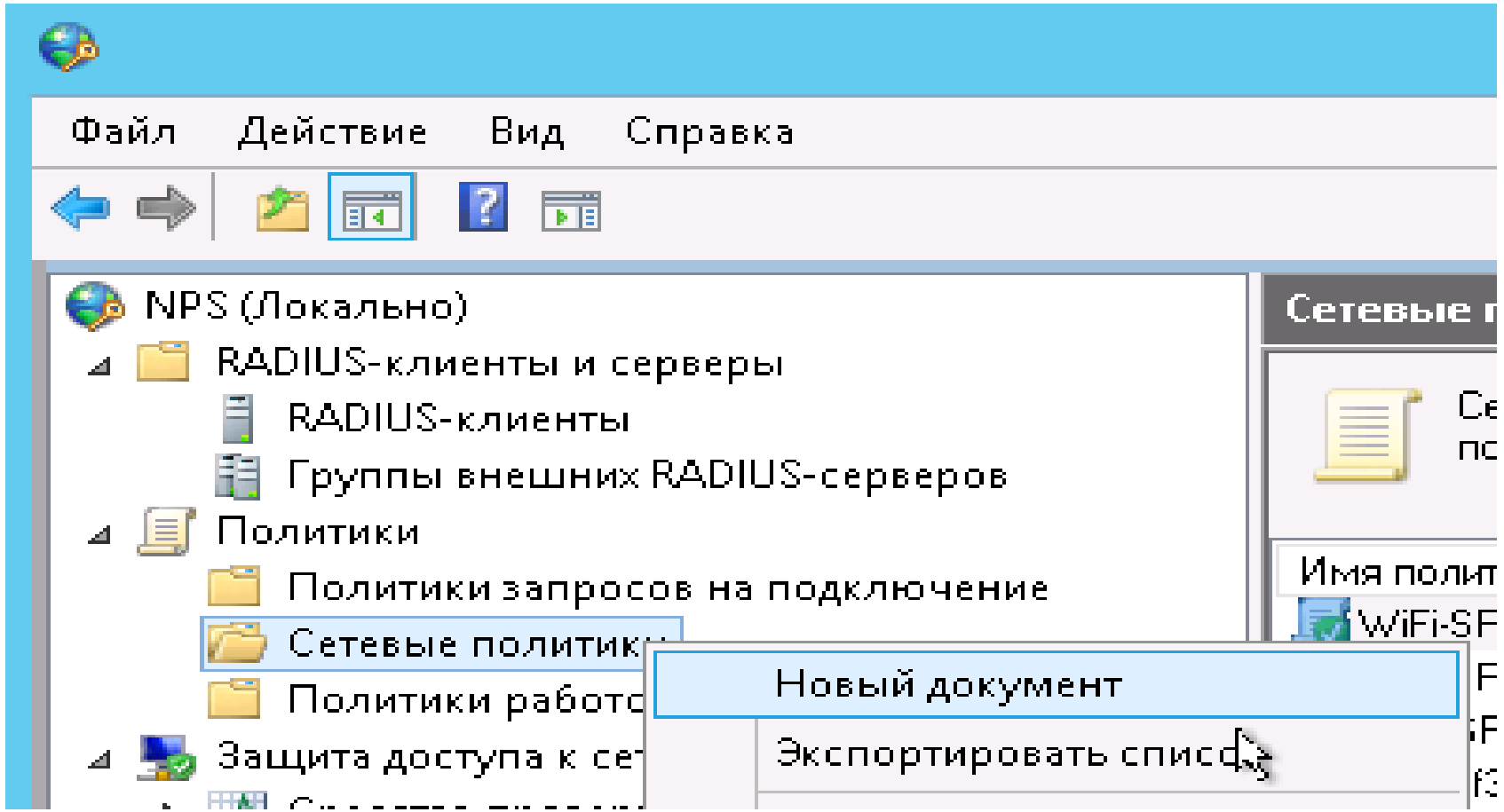
Вводим имя, Тип доступа к сети оставляем ”не указано”



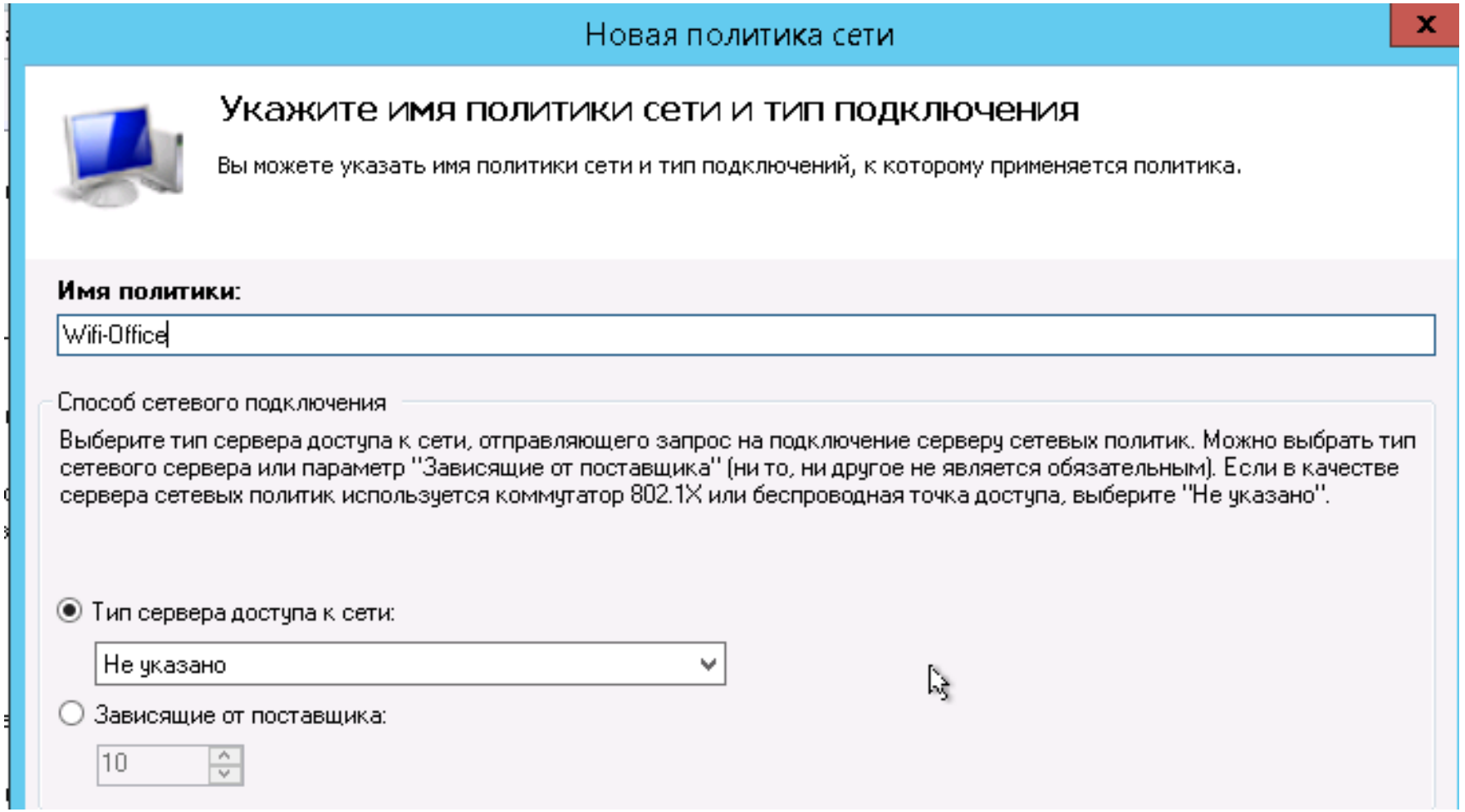
На закладке условия нажимаем на кнопку добавить и выбираем из меню пункт понятное имя клиента. Вводим то имя, что мы ввели раньше



Закрываем окна кнопками ОК. И создаём саму политику для wifi в офис сети

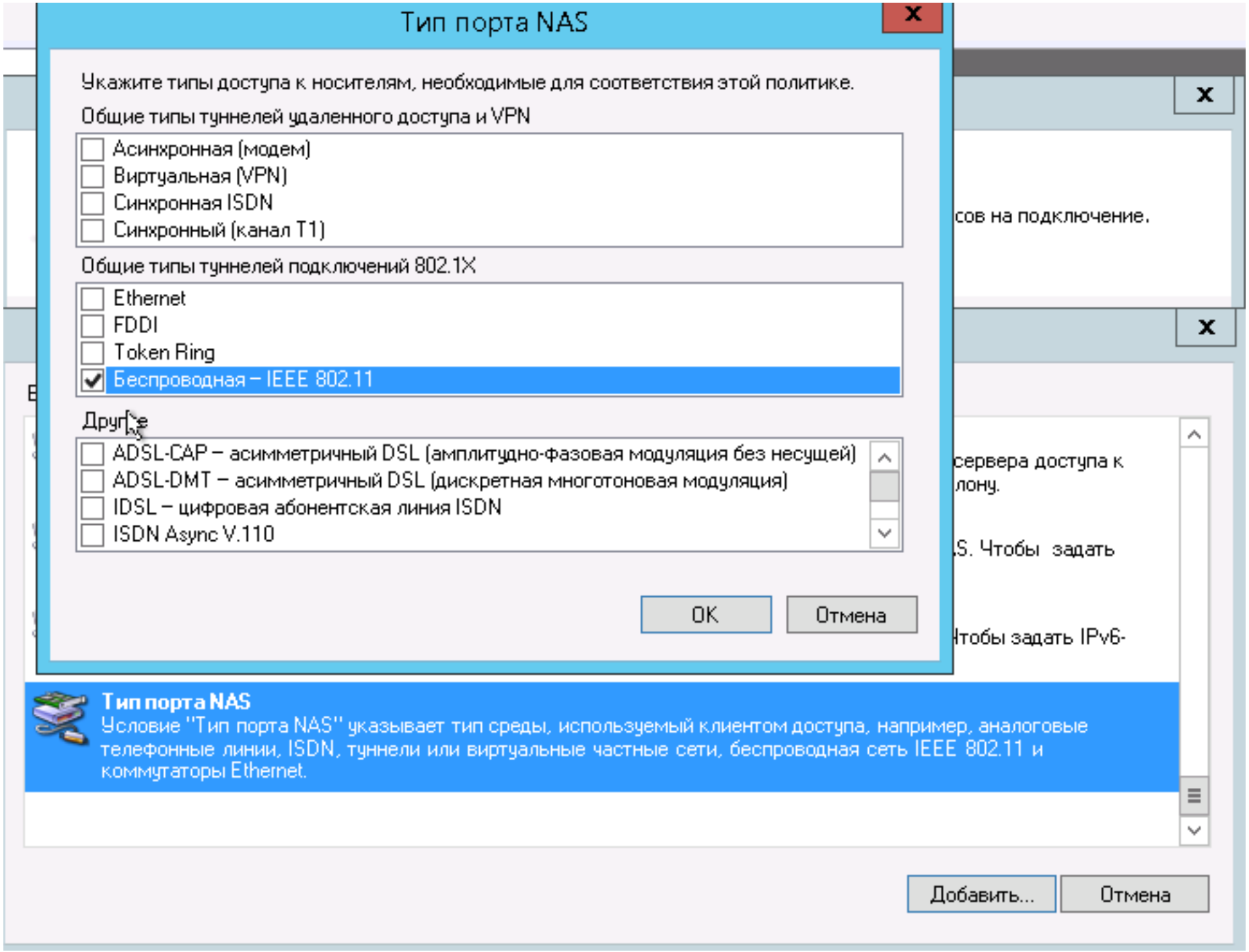


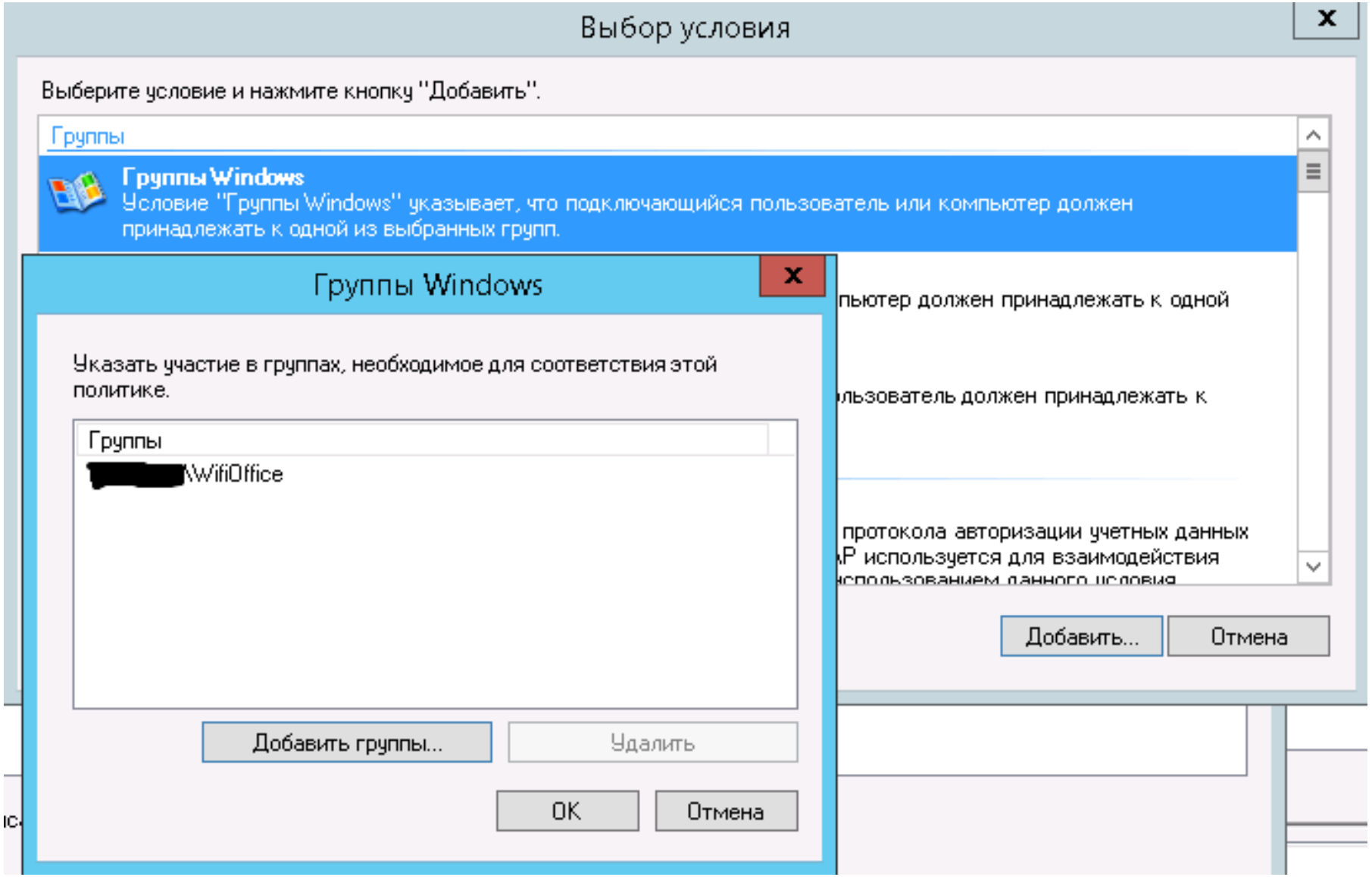
Задаём имя политики



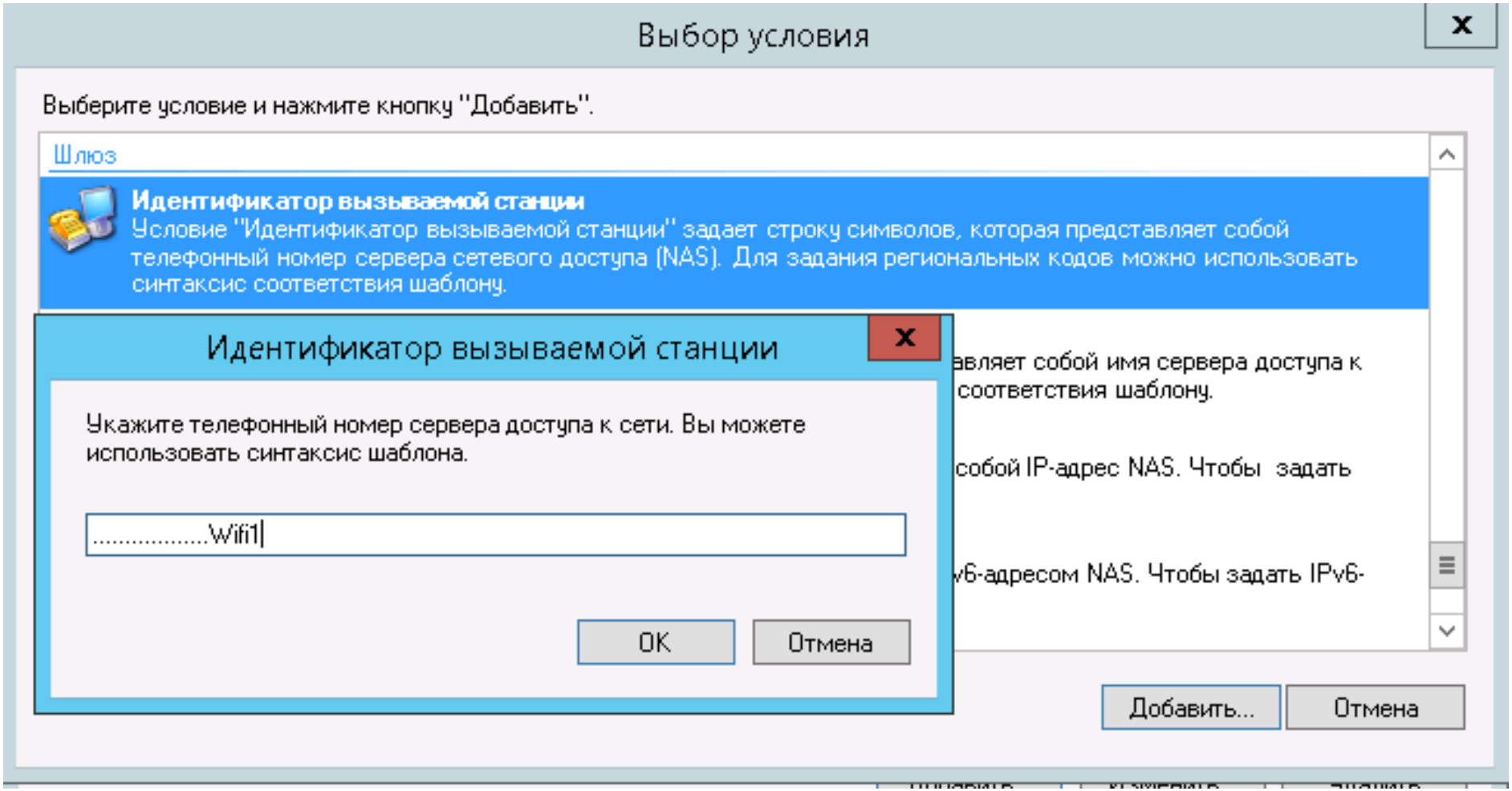
Указываем условия.

- Если у нас планируется использование нескольких radius клиентов (capmsan`ов или других), то заново добавляем ”Понятное имя клиента”.
- Условие “Тип порта NAS” позволит нам отличить запрос с wifi от запросов vpn.
- А так же добавляем условия ”Группы Windows” – здесь мы выбираем какой группе из AD разрешать подключаться к wifi сети
- И ”идентификатор вызываемой станции” – это название нашей wifi сети (Wifi1 или region)

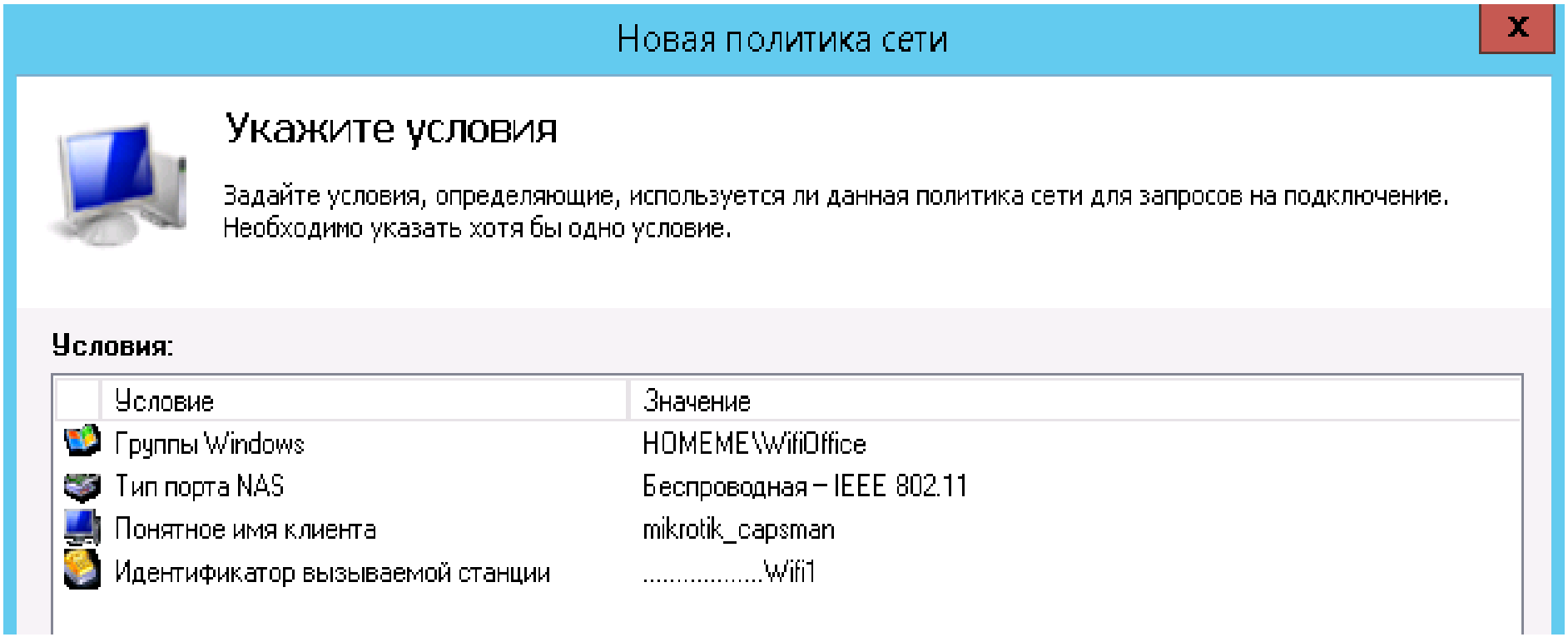

Тип порта NAS
Укажите типы доступа к носителям, необходимые для соответствия этой политике.
Общие типы туннелей удаленного доступа и VPN
Асинхронная (модем)
Виртуальная (VPN)
Синхронная ISDN
Синхронный (канал T1)
Общие типы туннелей подключений 802.1X
Ethernet
FDDI
Token Ring
Беспроводная – IEEE 802.11
Другие
ADSL-CAP – асимметричный DSL (амплитудно-фазовая модуляция без несущей)
ADSL-DMT – асимметричный DSL (дискретная многотоновая модуляция)
IDSL – цифровая абонентская линия ISDN
ISDN Async V.110
OK
Отмена
Тип порта NAS
Условие "Тип порта NAS" указывает тип среды, используемый клиентом доступа, например, аналоговые телефонные линии, ISDN, туннели или виртуальные частные сети, беспроводная сеть IEEE 802.11 и коммутаторы Ethernet.
Добавить...
Отмена


Выбор условия
Выберите условие и нажмите кнопку "Добавить".
Группы
Группы Windows
Условие "Группы Windows" указывает, что подключающийся пользователь или компьютер должен принадлежать к одной из выбранных групп.
Группы Windows
Указать участие в группах, необходимое для соответствия этой политике.
Группы
[redacted]\WifiOffice
Добавить группы...
Удалить
OK
Отмена
пьютер должен принадлежать к одной
льзователь должен принадлежать к
протокола авторизации учетных данных
P используется для взаимодействия
Добавить...
Отмена

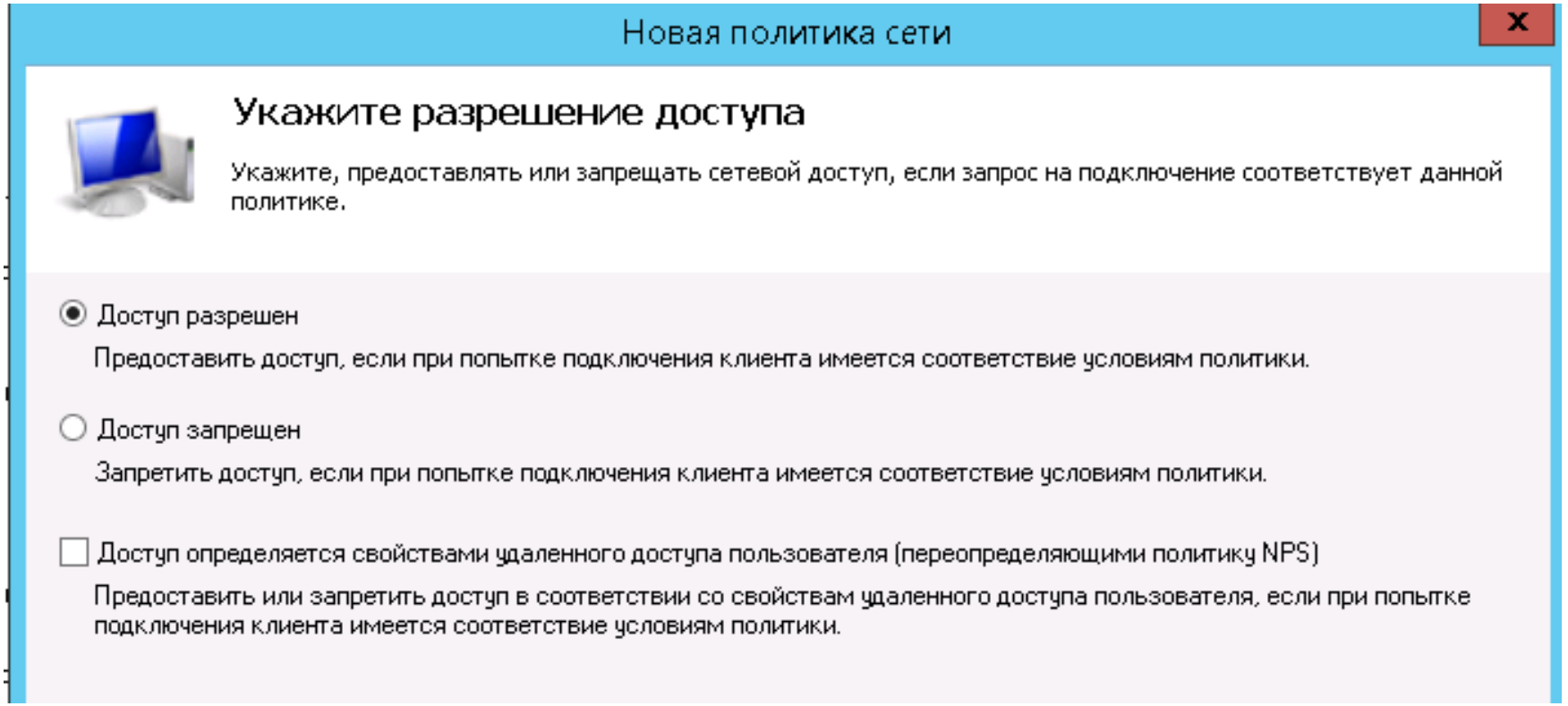
Так как radius получает имя сети вместе с mac адресом wifi интерфейса, к которому идёт подключение (в виде XX-XX-XX-XX-XX-XX:Wifi1), то нам надо составить шаблон для получения только имени сети .....Wifi1 (18 точек, потом имя сети).



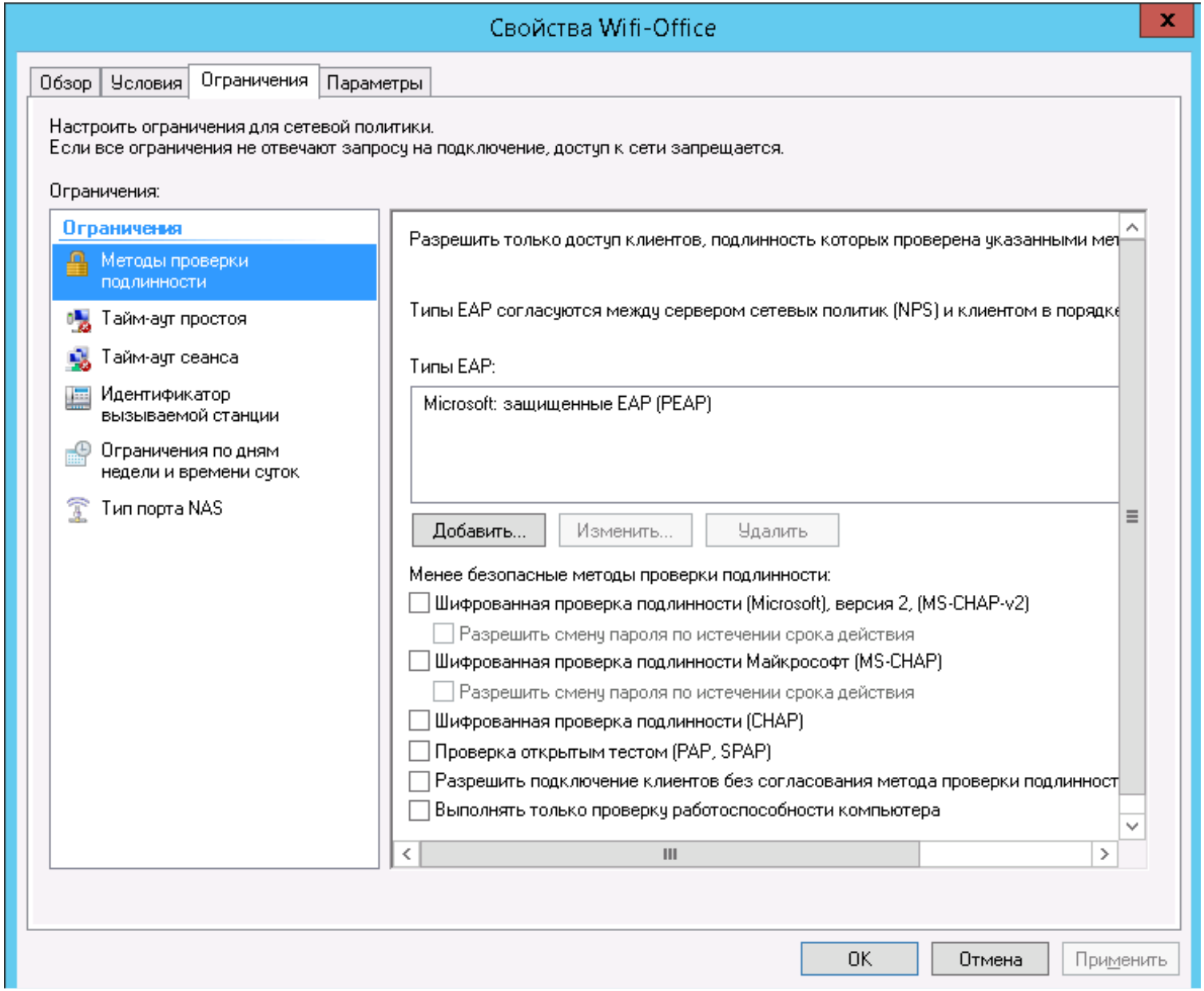
Получаем такой список условий



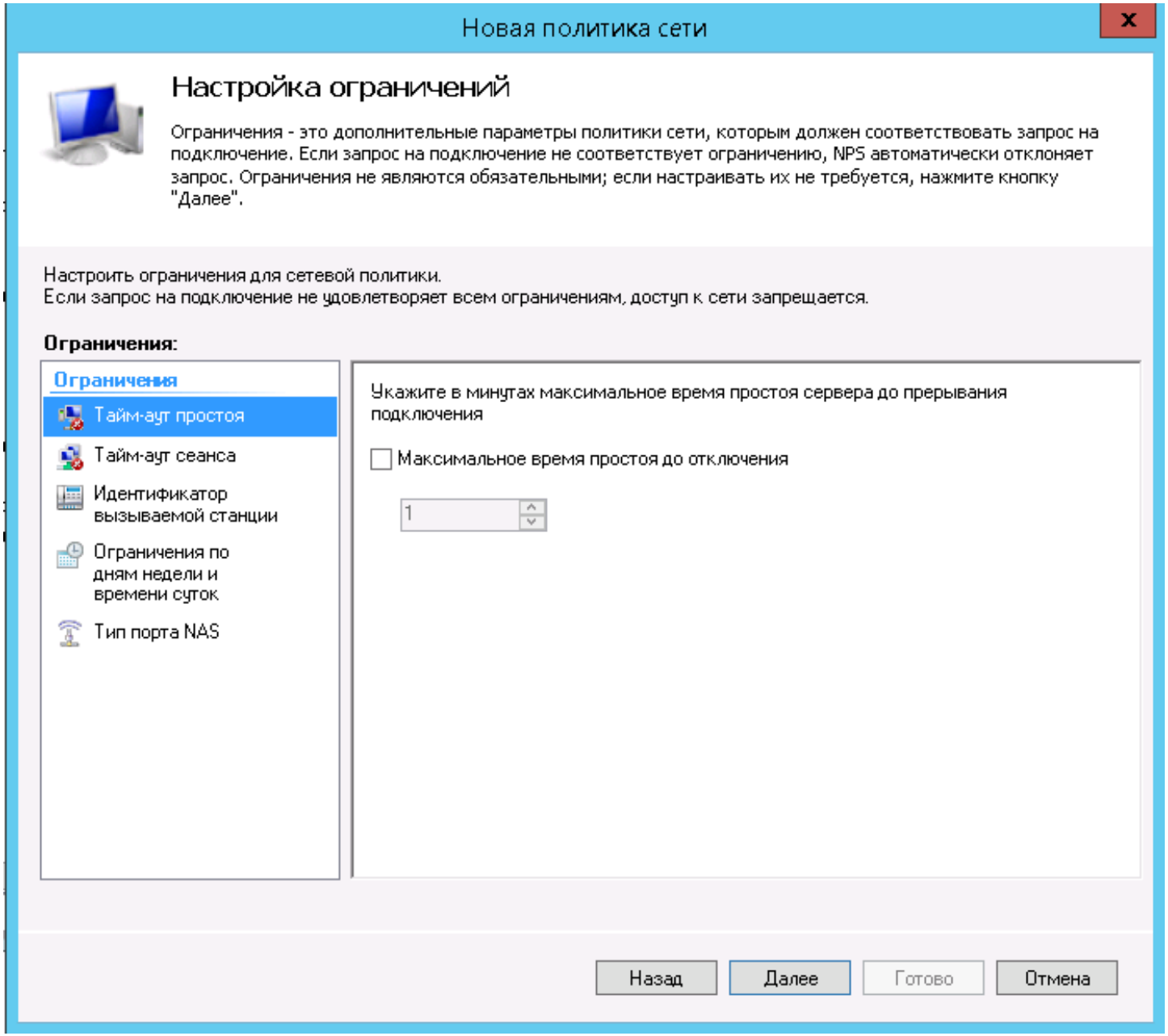
На следующей вкладке задаём действие (разрешаем доступ)



Добавляем используемый тип EAP. Так как нам не охота возиться с сертификатами, то выбираем PEAP

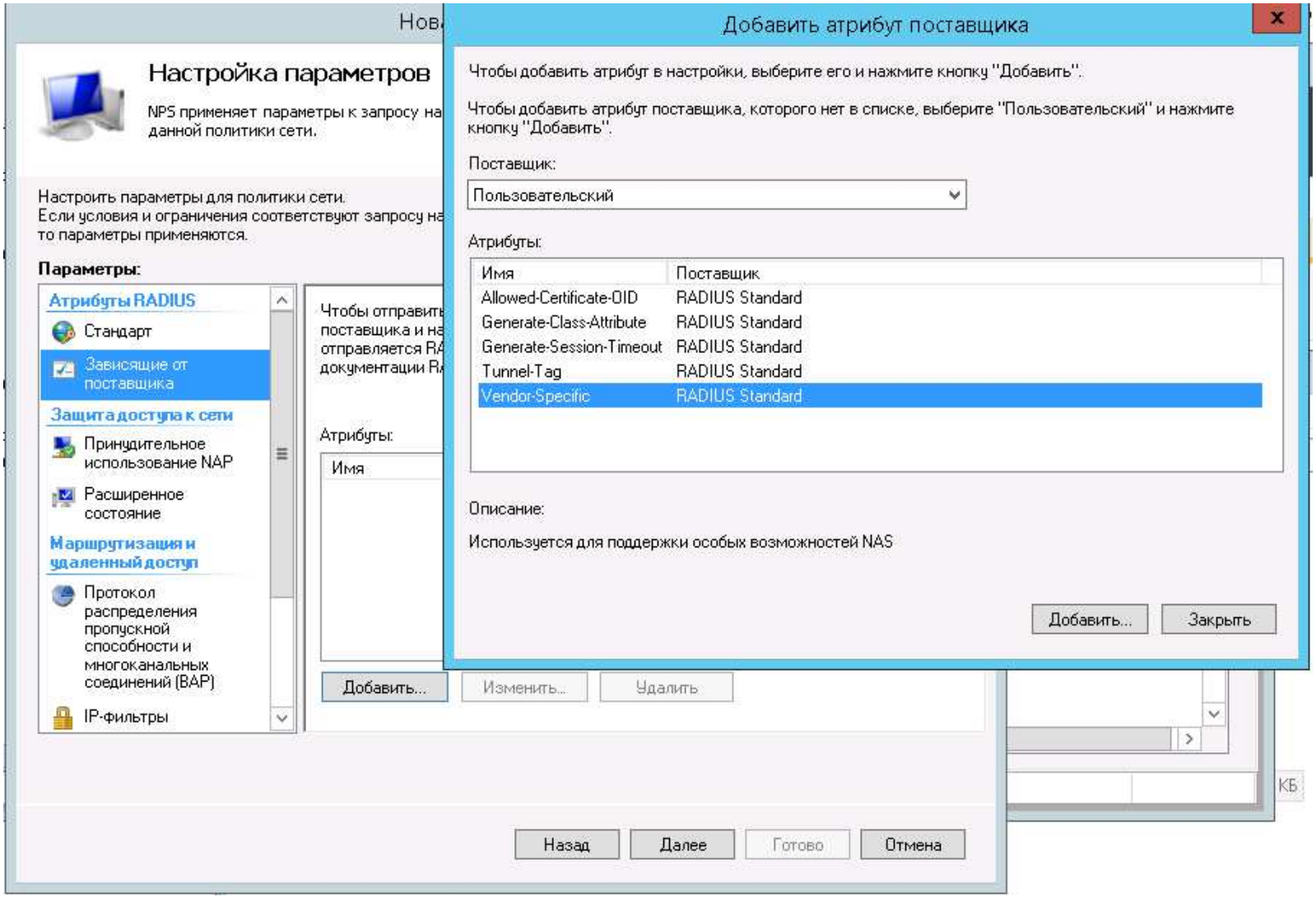


Ограничения оставляем как есть. При желании можно задать ограничения, например по времени подключения.

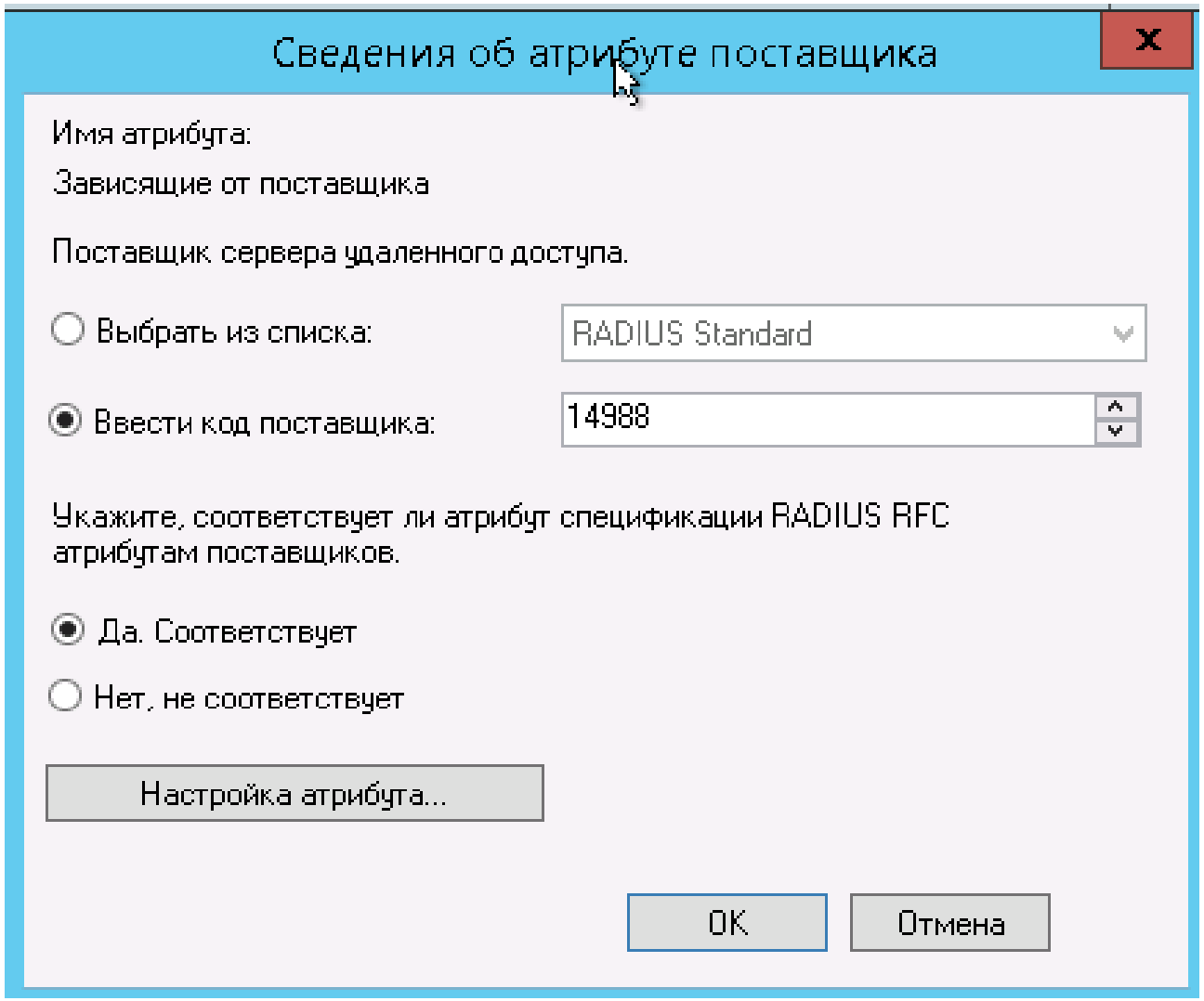


В настройке параметров мы можем передать микротику требуемый vlan. Для этого в Атрибутах Radius выбираем раздел ”Зависящие от поставщика” и нажимаем на кнопку добавить

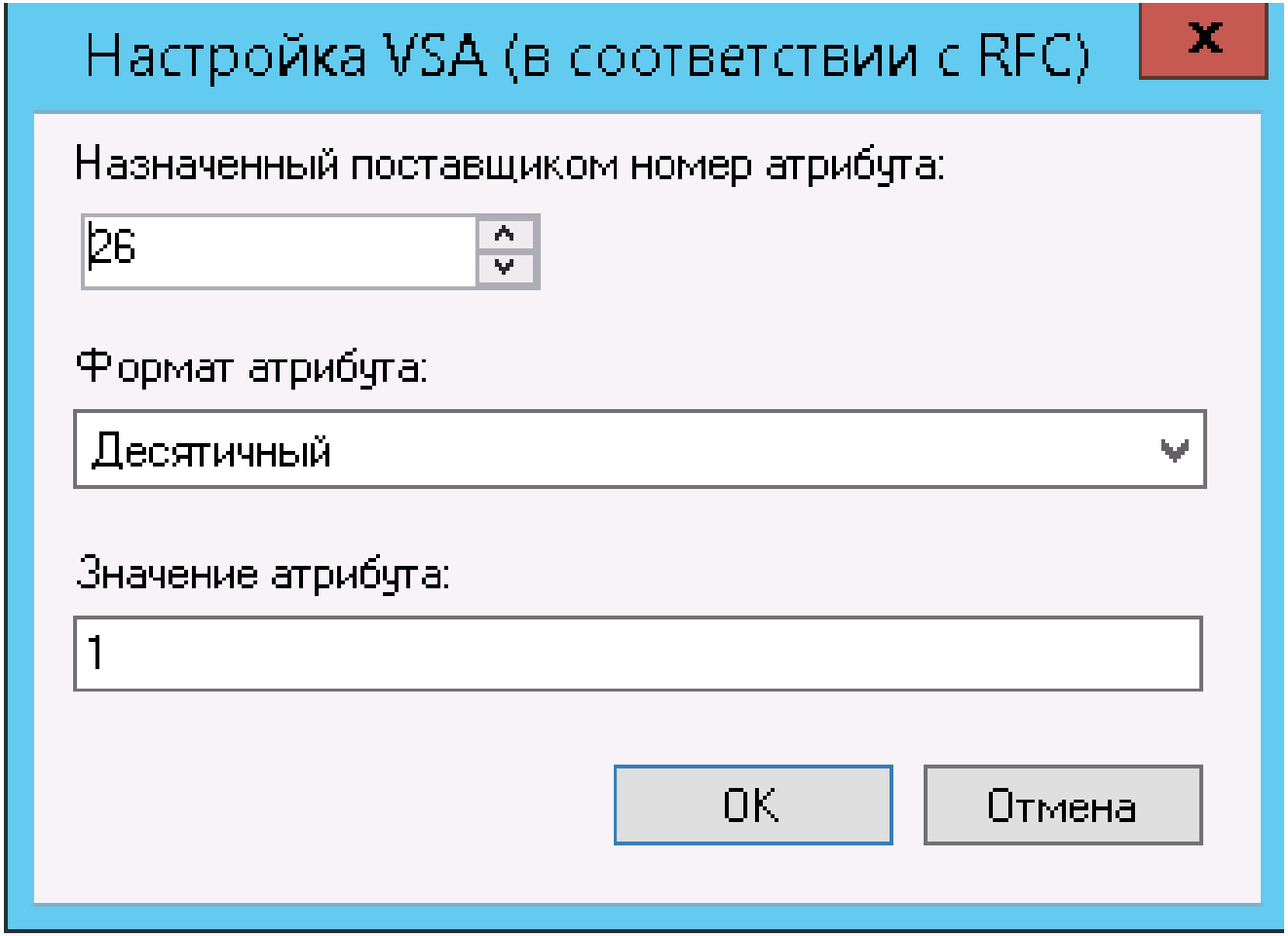
В открывшемся окне выбираем Поставщик: Пользовательский. Атрибут: Vendor-Specific и нажимаем добавить



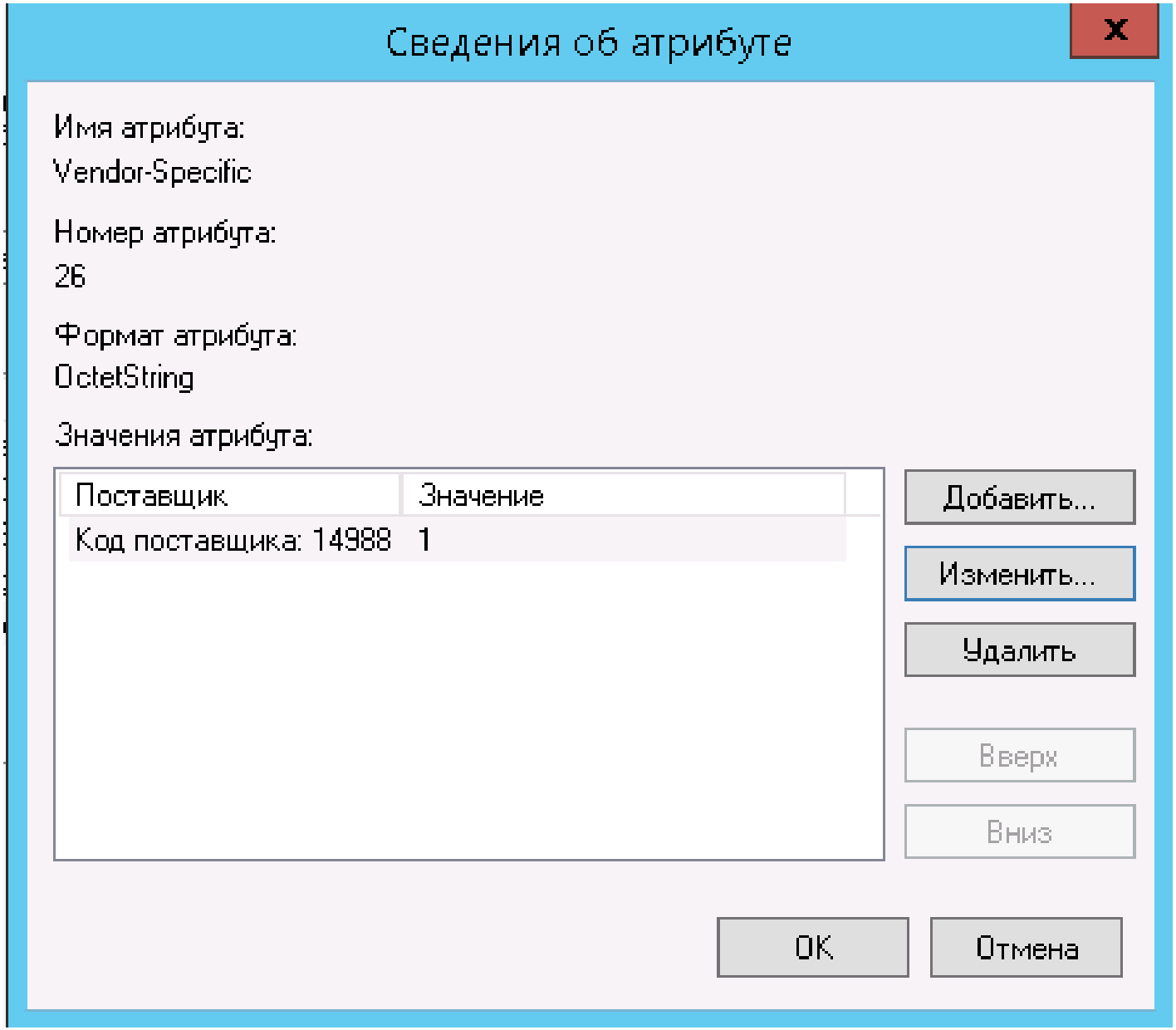
В открывшемся окне выбираем добавить и настраиваем свойства:
Выбираем галочку ”Ввести код поставщика” и пишем 14988
Ставим галочку соответствия атрибута спецификации ”Да, соответствует”



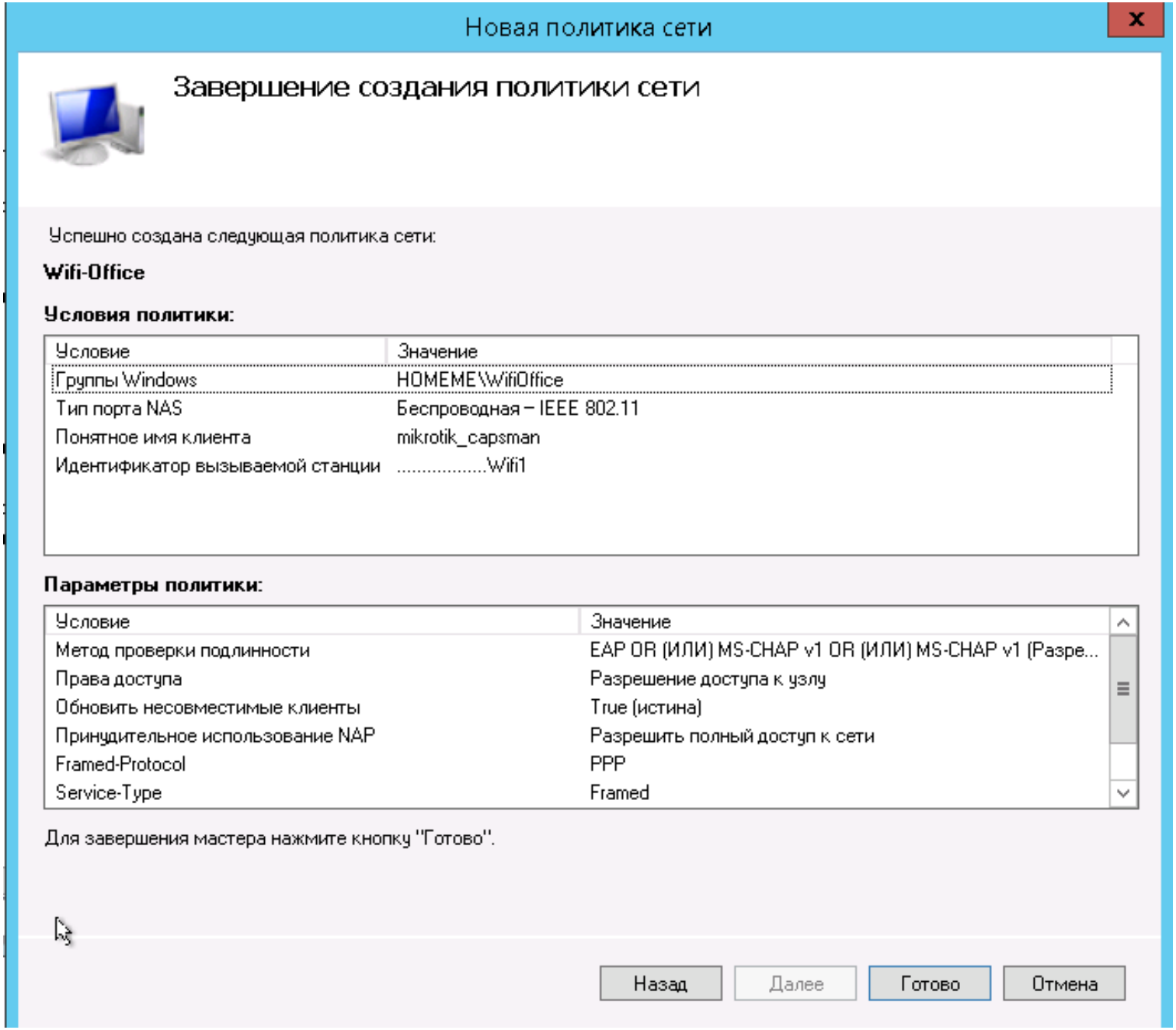
Нажимаем кнопку ”Настройка арибута…”
Вводим ”Назначенный поставщиком номер атрибута” 26
Формат атрибута выбираем десятичный
В поле значение атрибута проставляем нужный нам vlan



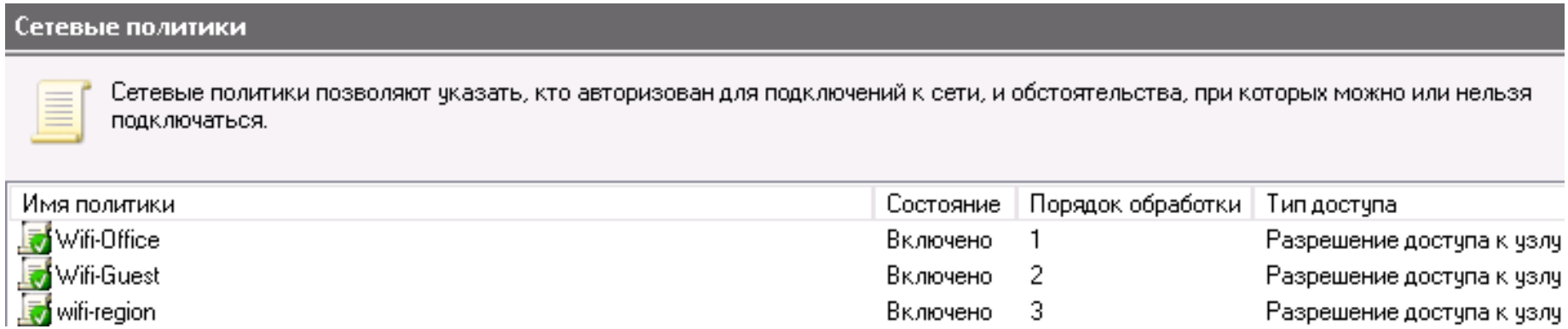
Закрываем окно и видим результат



В итоге получили настроенную политику



Аналогично создаём политику для гостевой wifi сети с тем же именем, но выбираем другую доменную группу (all_users) и vlan указываем 7-ой.
И создаём политику для сети регионов, в которой указываем имя сети region и vlan тот, который есть в регионах.



Политики обрабатываются сверху вниз, по этому поднимаем наши политики на самый верх. Первой располагаем политики Офисной сети, затем гостевой сети. При подключении к сети Wifi1 это позволит вначале проверить на допуск во внутреннюю сеть, а затем на допуск в гостевой wifi.

Результаты настройки:

Пользователь 1 Включён в группы all_users и WiFiOffice
Пользователь 2 Включён в группу all_users

	Офисная сеть		Филиалы	
SSID	wifi1	region	wifi1	region
Пользователь 1	Локальная сеть	Гостевой доступ в интернет	Офисная сеть	Локальная сеть
Пользователь 2	Гостевой доступ в интернет	Гостевой доступ в интернет	Доступ в интернет через офис	Локальная сеть