

Построение корпоративных wifi сетей с авторизацией на microsoft radius

Об авторе

Александр Рагозин

**Системный администратор группы
компаний HomeMe и MIXIT
по Северо-Западу**

Сертификаты MikroTik

МТСНА, МТСТСЕ, МТСРЕ, МТСИНЕ

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

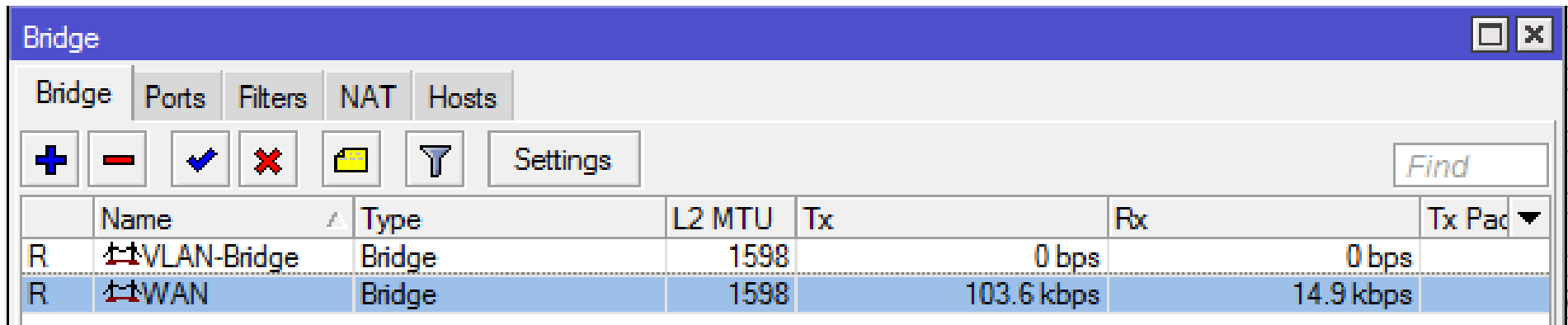
Алгоритм доступа в wifi сети

- 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



The screenshot shows the Mikrotik WinBox interface for configuring a bridge. The window title is "Bridge". There are tabs for "Bridge", "Ports", "Filters", "NAT", and "Hosts". Below the tabs is a toolbar with icons for adding (+), deleting (-), enabling (checkmark), disabling (X), adding a new bridge (folder), and filtering (funnel), along with a "Settings" button and a "Find" search box. The main area contains a table with the following data:

	Name	Type	L2 MTU	Tx	Rx	Tx Pac
R	VLAN-Bridge	Bridge	1598	0 bps	0 bps	
R	WAN	Bridge	1598	103.6 kbps	14.9 kbps	

Созданные vlan`ы

Interface List

Interface | Interface List | Ethernet | EoIP Tunnel | IP Tunnel | GRE Tunnel | VLAN | VRRP | Bonding | LTE

+ - ✓ ✗ 📁 🗑️ Find

	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
R	vlan1	VLAN	1500	1500	1594	0 bps	0 bps	0	0	
R	vlan7	VLAN	1500	1500	1594	0 bps	0 bps	0	0	

Interface <vlan1>

General | Loop Protect | Status | Traffic

Name: vlan1
Type: VLAN
MTU: 1500
Actual MTU: 1500
L2 MTU: 1594
MAC Address: 6C:3B:6B:03:22:36
ARP: enabled
ARP Timeout:
VLAN ID: 1
Interface: VLAN-Bridge
 Use Service Tag

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled | running | slave

Interface <vlan7>

General | Loop Protect | Status | Traffic

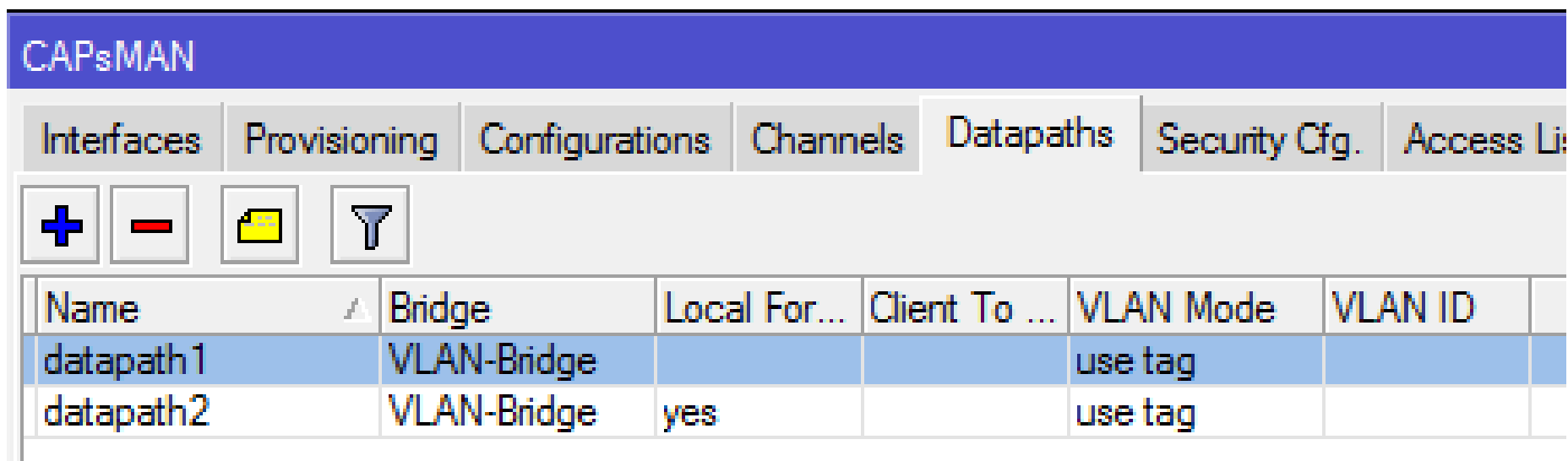
Name: vlan7
Type: VLAN
MTU: 1500
Actual MTU: 1500
L2 MTU: 1594
MAC Address: 6C:3B:6B:03:22:36
ARP: enabled
ARP Timeout:
VLAN ID: 7
Interface: VLAN-Bridge
 Use Service Tag

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

enabled | running | slave

Настраиваем capsmn

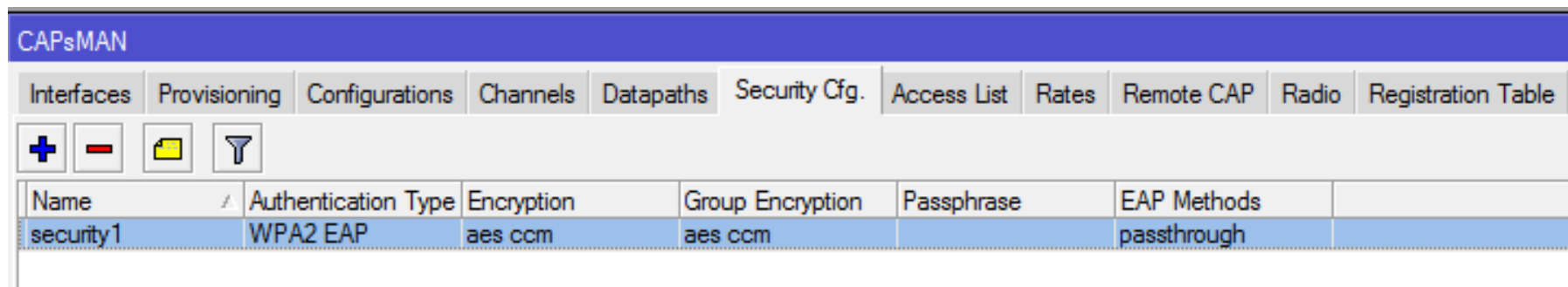
Создаём пути. Первый путь пойдёт на capsmn, а второй путь пойдёт на точку доступа (это для филиалов)



The screenshot shows the CAPsMAN configuration interface. The 'Datapaths' tab is selected. Below the navigation tabs, there are four icons: a blue plus sign, a red minus sign, a yellow folder icon, and a grey funnel icon. The main area contains a table with the following data:

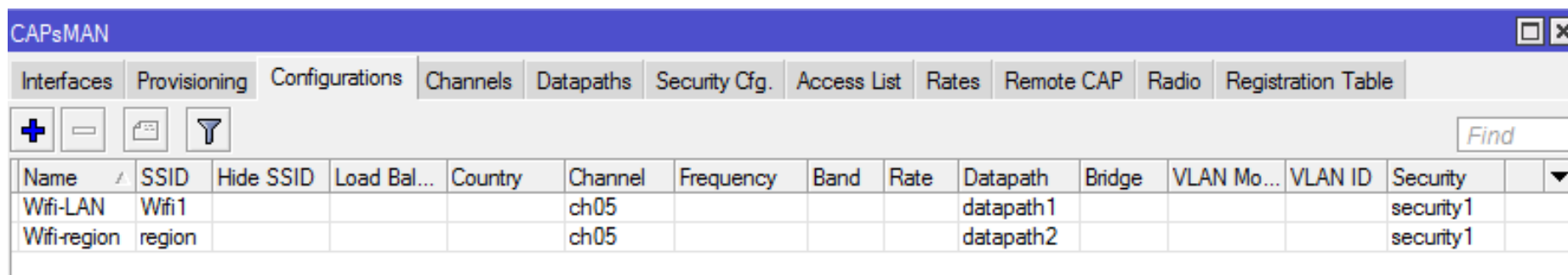
Name	Bridge	Local For...	Client To ...	VLAN Mode	VLAN ID
datapath1	VLAN-Bridge			use tag	
datapath2	VLAN-Bridge	yes		use tag	

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



Name	Authentication Type	Encryption	Group Encryption	Passphrase	EAP Methods
security1	WPA2 EAP	aes ccm	aes ccm		passthrough

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



Name	SSID	Hide SSID	Load Bal...	Country	Channel	Frequency	Band	Rate	Datapath	Bridge	VLAN Mo...	VLAN ID	Security
Wifi-LAN	Wifi1				ch05				datapath1				security1
Wifi-region	region				ch05				datapath2				security1

Настраиваем Provisioning для авто подключения точек или для каждой точки отдельно

New CAPs Provisioning

Radio MAC: 00:00:00:00:00:00

Hw. Supported Modes:

Identity Regexp:

Common Name Regexp:

IP Address Ranges:

Action: create dynamic enabled

Master Configuration: Wifi-LAN

Slave Configuration: Wifi-region

Name Format: identity

Name Prefix:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled

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

Radius Server <192.168.91.31>

General Status

Service: ppp login
 hotspot wireless
 dhcp

Called ID:

Domain:

Address: 192.168.91.31

Secret:

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

Accounting Backup

Realm:

Src. Address: 0.0.0.0

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Status

enabled

Включаем CAP на каждой точке.

CAP

Enabled

Interfaces:

Certificate:

Discovery Interfaces:

Lock To CAPsMAN

CAPsMAN Addresses:

CAPsMAN Names:

CAPsMAN Certificate Common Names:

Bridge:

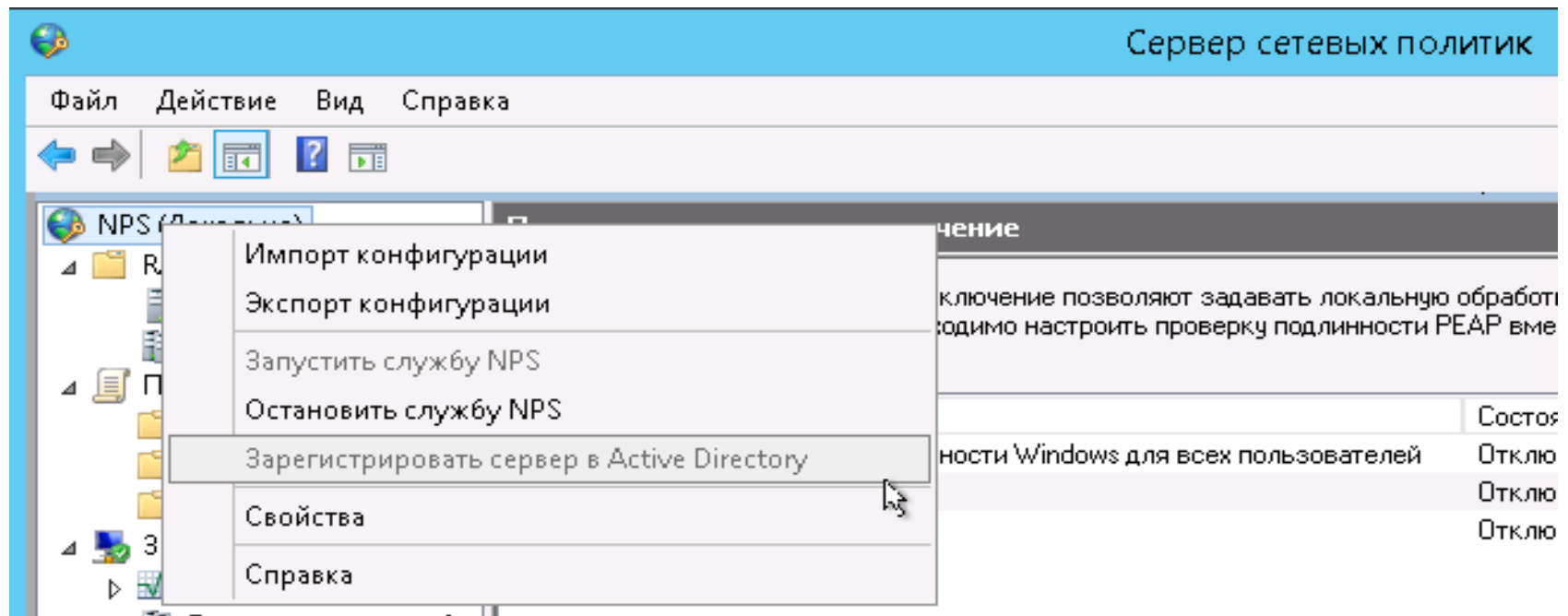
Requested Certificate:

Locked CAPsMAN Common Name:

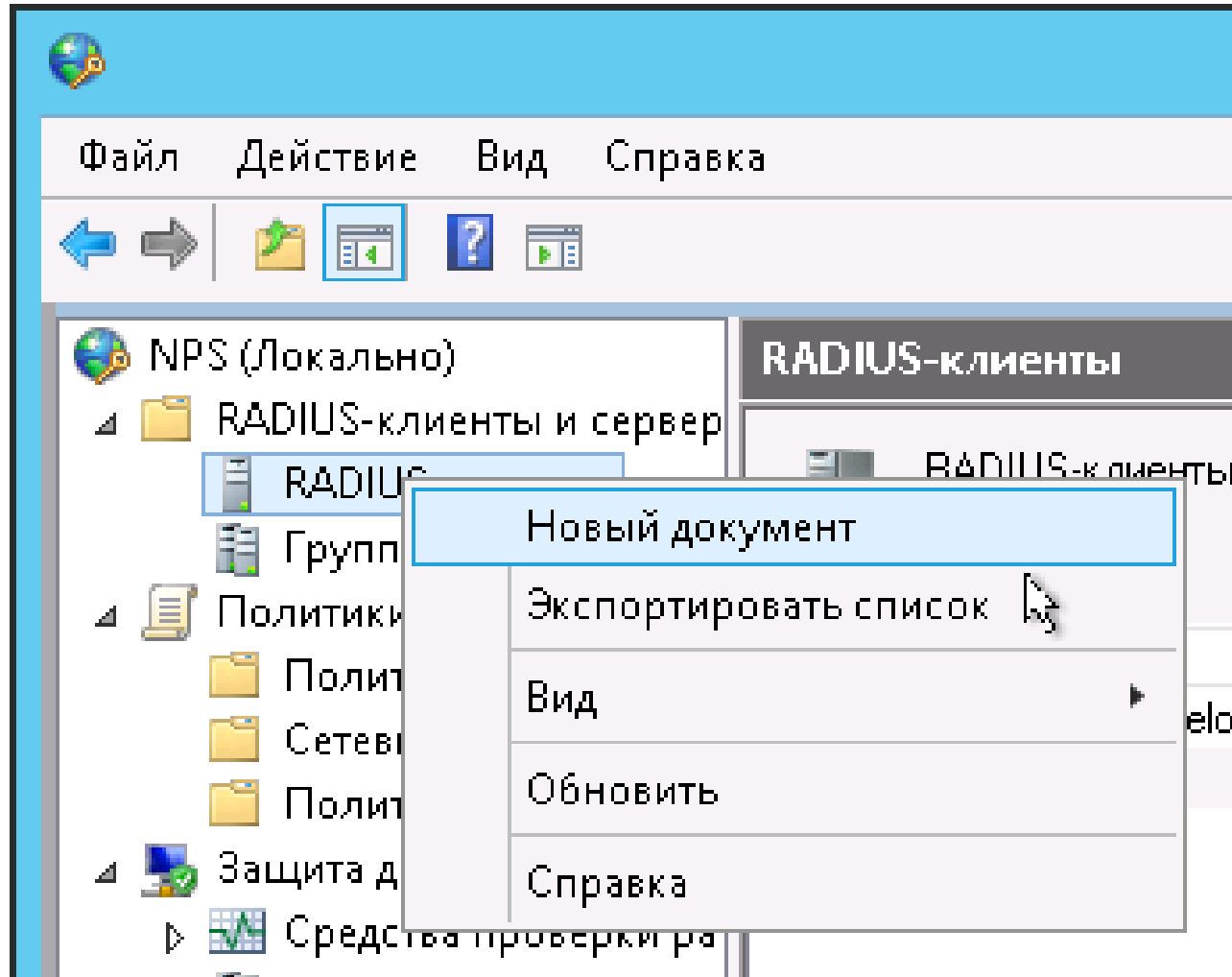
OK
Cancel
Apply

Настройка RADIUS сервера

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



Добавляем radius клиента (наш MikroTik)



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

Свойства mikrotik_capsman

Параметры | Дополнительно

Включить этот RADIUS-клиент

Выберите существующий шаблон:

Имя и адрес

Понятное имя:
mikrotik_capsman

Адрес (IP или DNS):
192.168.91.57

Общий секрет

Выберите существующий шаблон общих секретов:
Отсутствует

Чтобы ввести общий секрет вручную, щелкните "Вручную". Чтобы автоматически создать общий секрет, щелкните "Создать". Необходимо настроить RADIUS-клиент с введенным здесь общим секретом. В общих секретах учитывается регистр символов.

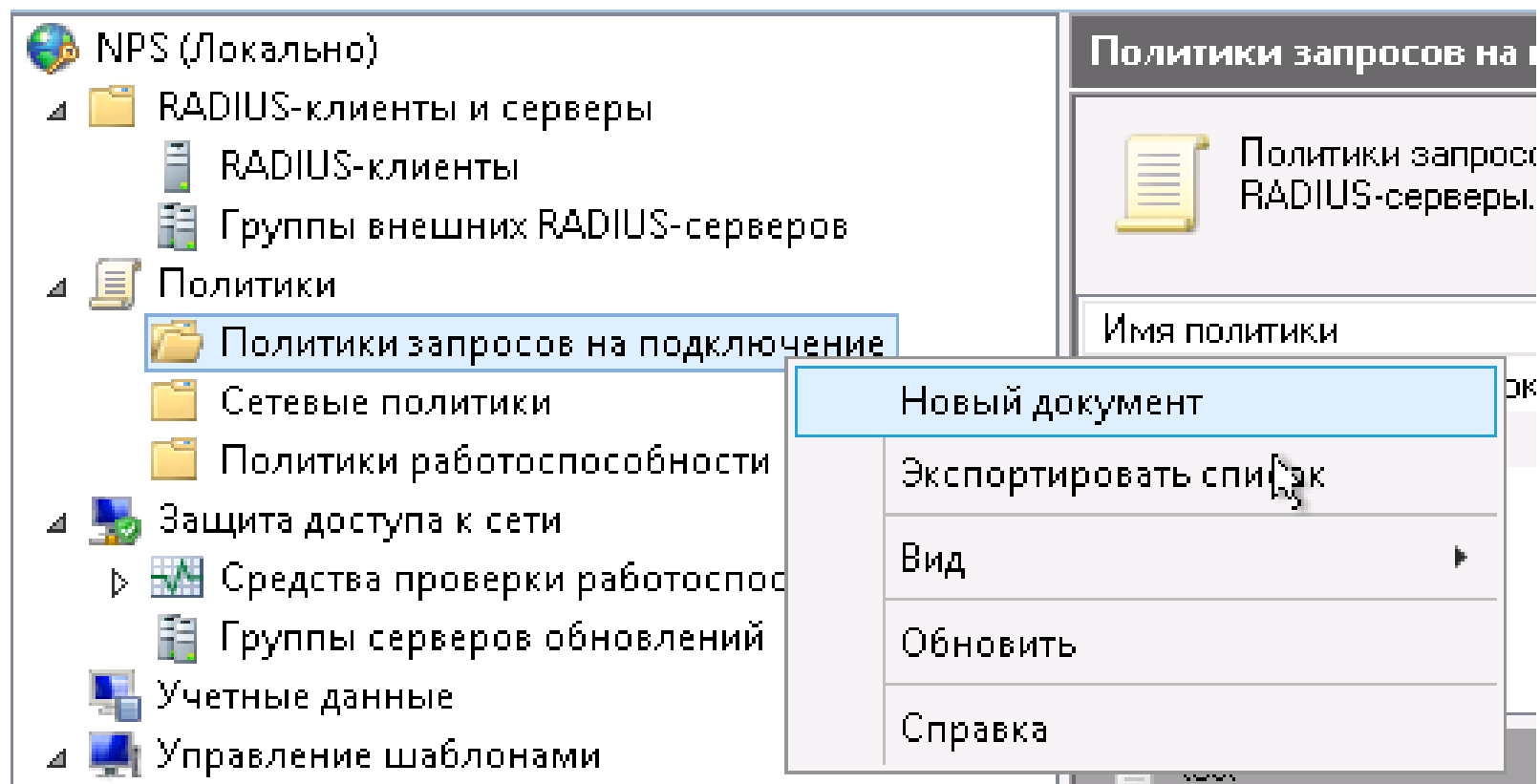
Вручную Создать

Общий секрет:
.....

Подтверждение общего секрета:
.....

OK Отмена Применить

Создаём политику запросов, одну на carspan



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

Свойства test

Обзор Условия Параметры

Имя политики: test

Состояние политики
Если включена, сервер сетевых политик проверяет эту политику при обработке запроса на подключение. Если отключена, сервер сетевых политик не проверяет эту политику.

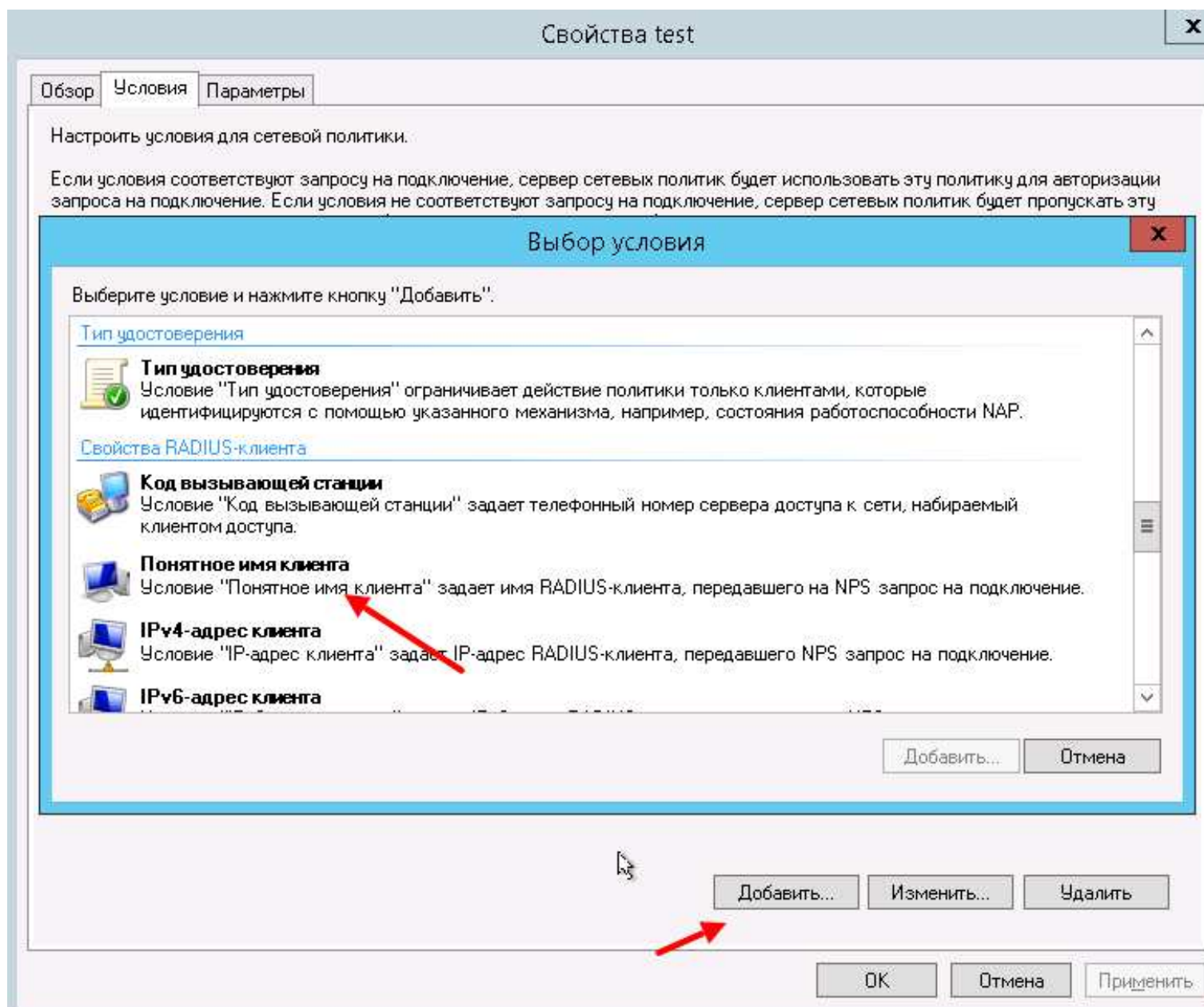
Политика включена

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". Если в качестве сервера сетевых политик используется коммутатор 802.1X или беспроводная точка доступа, выберите "Не указано".

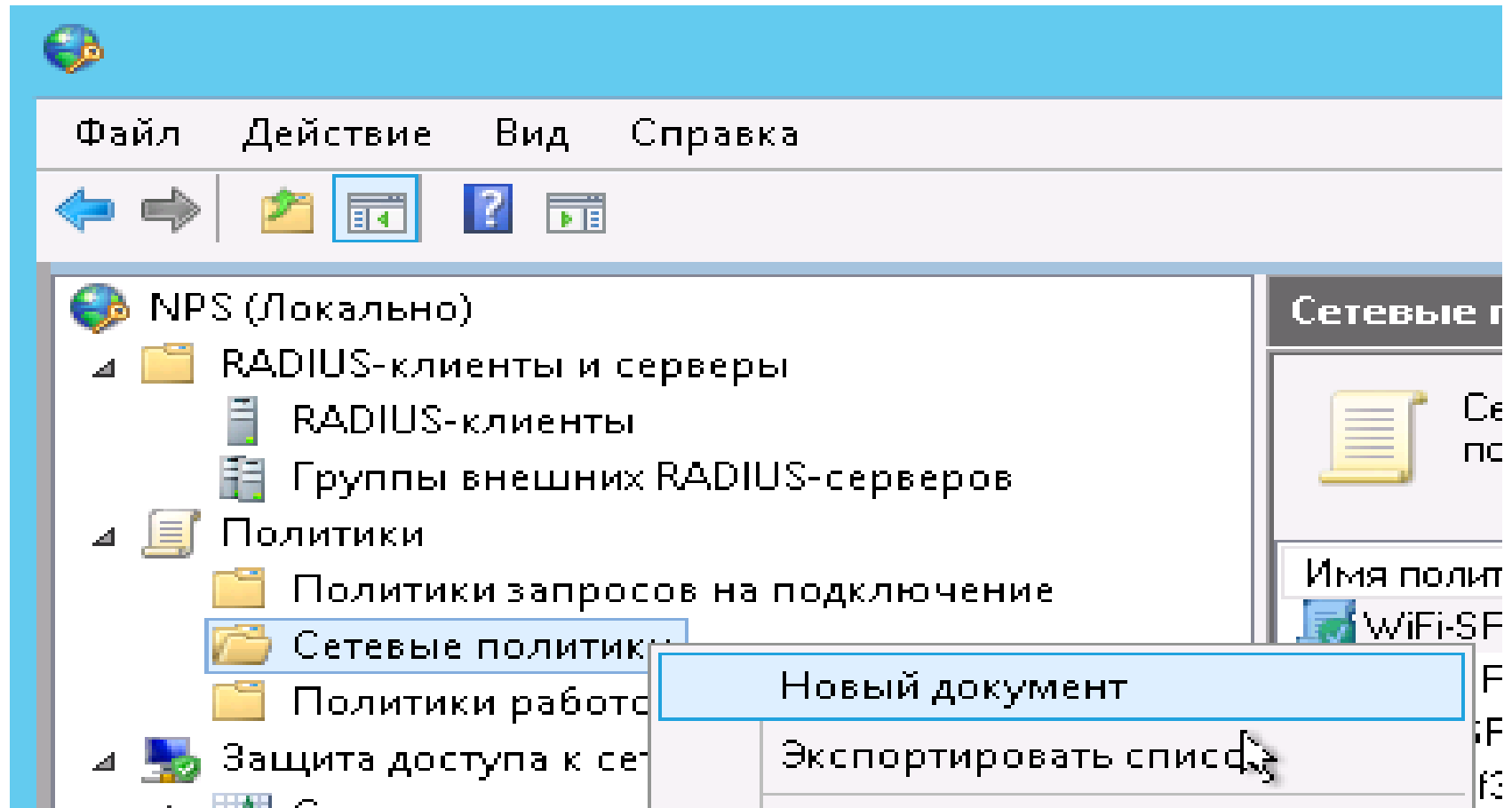
Тип сервера доступа к сети:
Не указано

Зависящие от поставщика:
10

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

Новая политика сети X

 **Укажите имя политики сети и тип подключения**

Вы можете 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:

Указываем условия.

- Если у нас планируется использование нескольких radius клиентов (сартсан`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 многотонавая модуляция)
- ISDL – 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

██████████\WifiOffice

Добавить группы...

Удалить

OK

Отмена

...компьютер должен принадлежать к одной

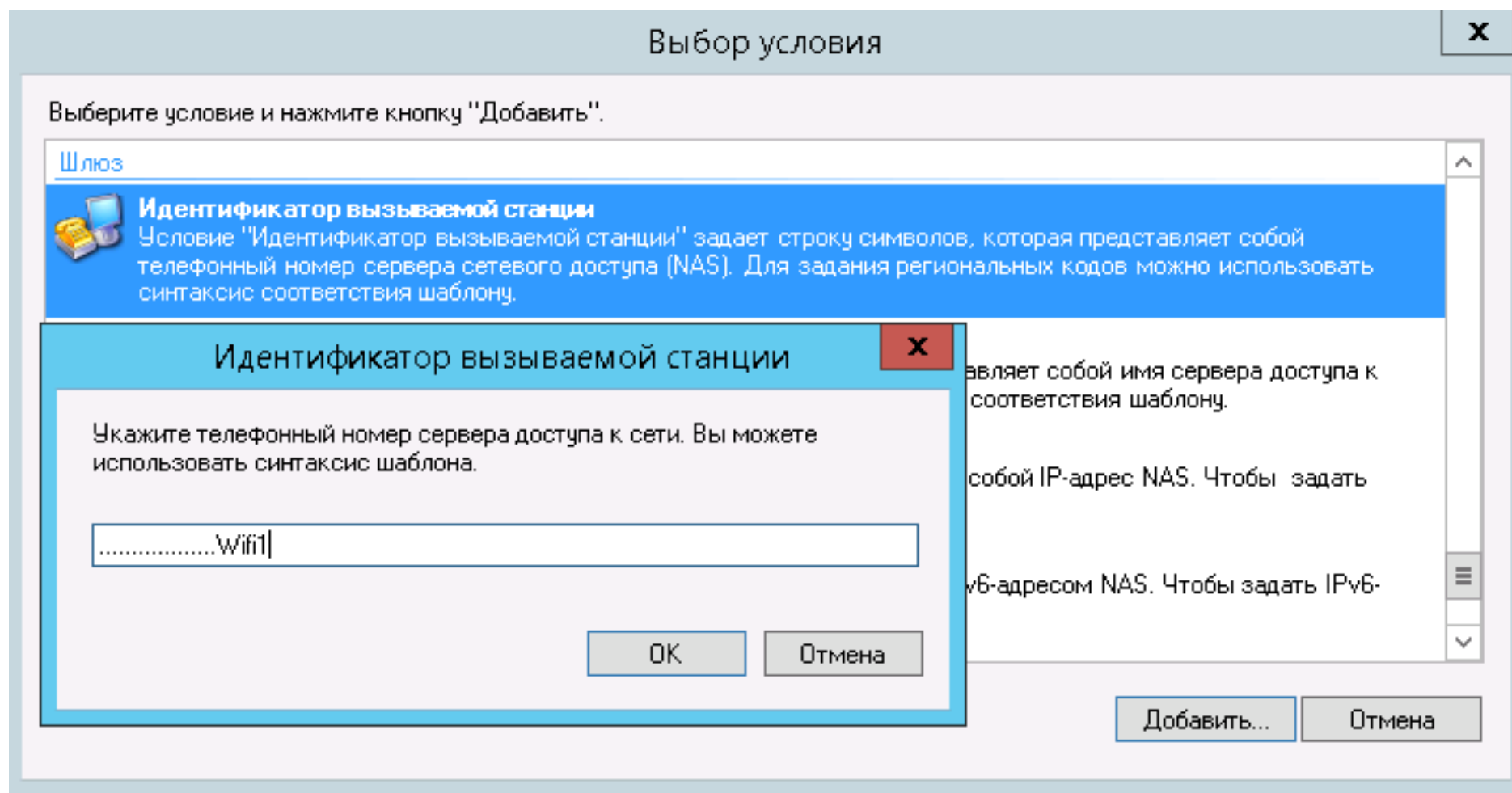
...пользователь должен принадлежать к

...протокола авторизации учетных данных
...R используется для взаимодействия
...использованием данного условия

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 сетиWifi1 (18 точек, потом имя сети).







Получаем такой список условий

Новая политика сети X

 **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	HOMEME\WifiOffice
 Тип порта NAS	Беспроводная – IEEE 802.11
 Понятное имя клиента	mikrotik_capsman
 Идентификатор вызываемой станцииWifi1

На следующей вкладке задаём действие (разрешаем доступ)

Новая политика сети X

 **Укажите разрешение доступа**

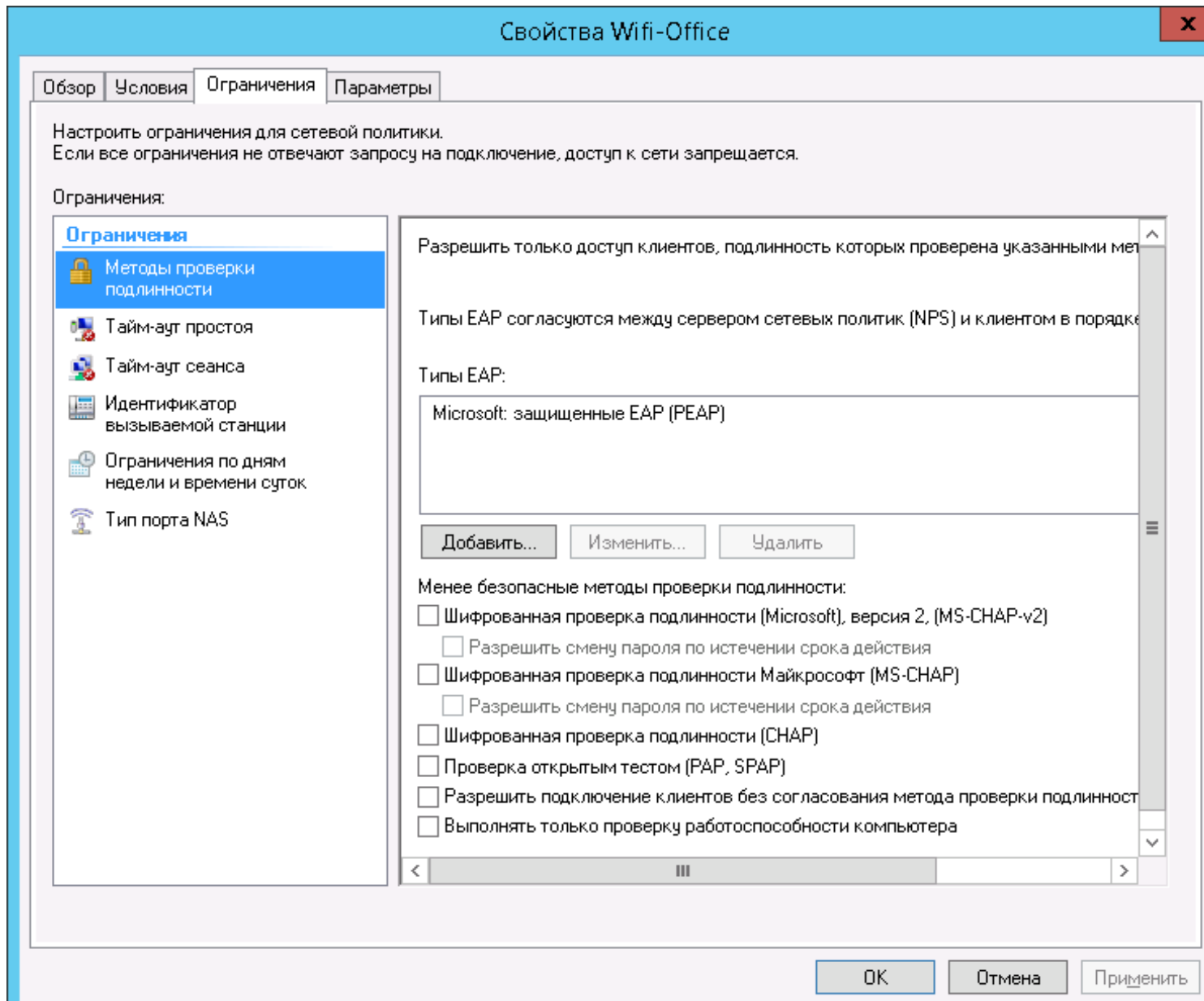
Укажите, предоставлять или запрещать сетевой доступ, если запрос на подключение соответствует данной политике.

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.

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.

Новая политика сети

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
- Тайм-аут сеанса
- Идентификатор вызываемой станции
- Ограничения по дням недели и времени суток
- Тип порта NAS

Укажите в минутах максимальное время простоя сервера до прерывания подключения

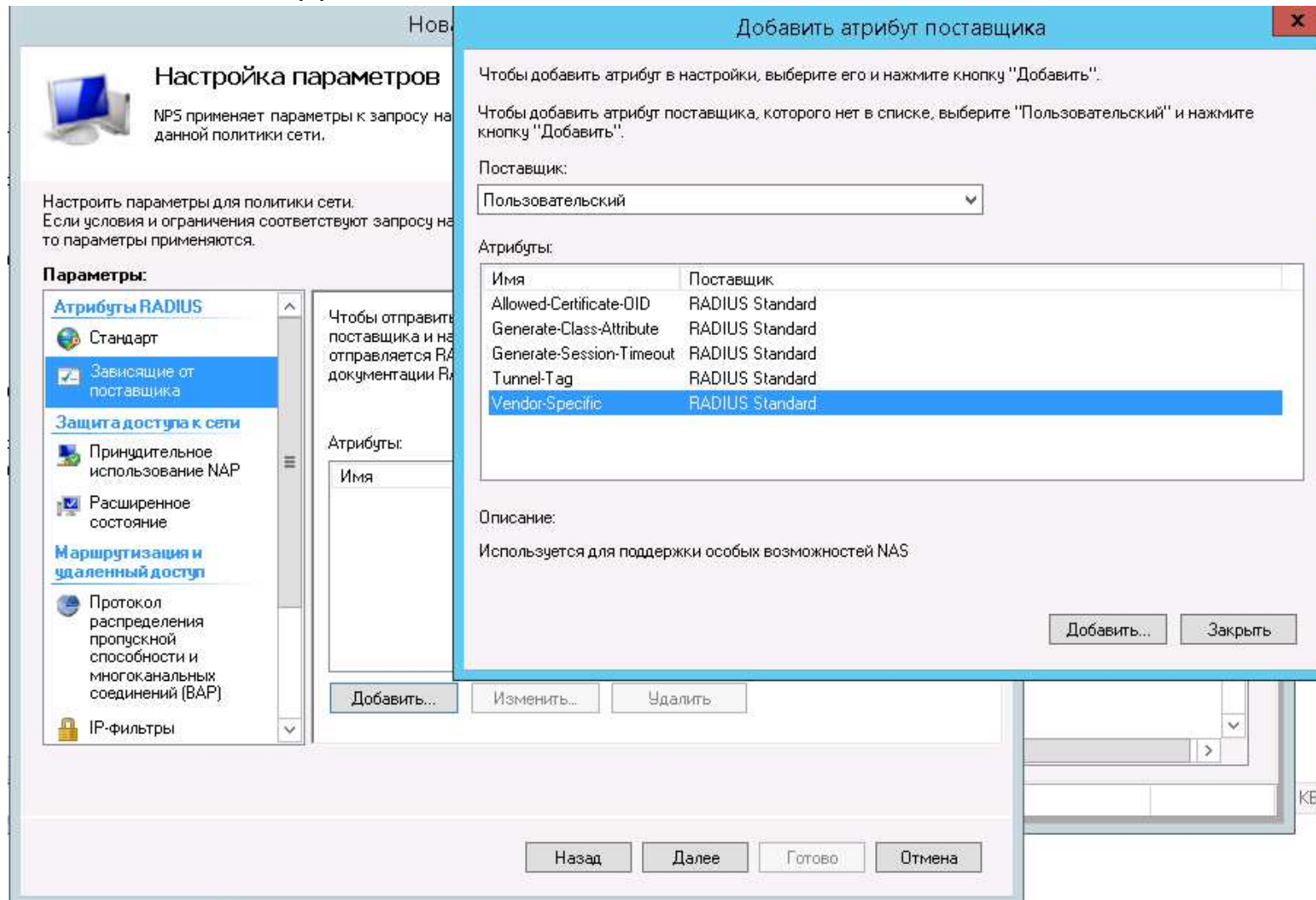
Максимальное время простоя до отключения

1

Назад Далее Готово Отмена

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"

Сведения об атрибуте поставщика

Имя атрибута:
Зависящие от поставщика

Поставщик сервера удаленного доступа.

Выбрать из списка: RADIUS Standard

Ввести код поставщика: 14988

Укажите, соответствует ли атрибут спецификации RADIUS RFC атрибутам поставщиков.

Да, Соответствует

Нет, не соответствует

Настройка атрибута...

OK Отмена

Нажимаем кнопку "Настройка атрибута..."

Вводим "Назначенный поставщиком номер атрибута" 26

Формат атрибута выбираем десятичный

В поле значение атрибута проставляем нужный нам vlan

Настройка VSA (в соответствии с RFC) X

Назначенный поставщиком номер атрибута:

26

Формат атрибута:

Десятичный

Значение атрибута:

1

OK Отмена

Закрываем окно и видим результат

Сведения об атрибуте ✕

Имя атрибута:
Vendor-Specific

Номер атрибута:
26

Формат атрибута:
OctetString

Значения атрибута:


Поставщик	Значение
Код поставщика: 14988	1

Добавить...
Изменить...
Удалить
Вверх
Вниз

OK Отмена

В итоге получили настроенную политику

Новая политика сети x

 **Завершение создания политики сети**

Успешно создана следующая политика сети:

Wifi-Office


Условия политики:

Условие	Значение
Группы Windows	HOMEME\WifiOffice
Тип порта NAS	Беспроводная - IEEE 802.11
Понятное имя клиента	mikrotik_capsman
Идентификатор вызываемой станцииWifi1

Параметры политики:

Условие	Значение
Метод проверки подлинности	EAP OR (ИЛИ) MS-CHAP v1 OR (ИЛИ) MS-CHAP v1 (Разре...
Права доступа	Разрешение доступа к узлу
Обновить несовместимые клиенты	True (истина)
Принудительное использование NAP	Разрешить полный доступ к сети
Framed-Protocol	PPP
Service-Type	Framed





Для завершения мастера нажмите кнопку "Готово".



Назад Далее Готово Отмена

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.

Сетевые политики			
 Сетевые политики позволяют указать, кто авторизован для подключений к сети, и обстоятельства, при которых можно или нельзя подключаться.			
Имя политики	Состояние	Порядок обработки	Тип доступа
 Wifi-Office	Включено	1	Разрешение доступа к узлу
 Wifi-Guest	Включено	2	Разрешение доступа к узлу
 wifi-region	Включено	3	Разрешение доступа к узлу

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