**НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «СИНЕРГИЯ»**

|  |  |  |
| --- | --- | --- |
| **Факультет/Институт** |  | Информационных технологий |
|  |  | (наименование факультета/ Института) |
| **Направление/специальность** |  | Разработка, сопровождение и обеспечение безопасности информационных систем |
| **подготовки:** |  | (код и наименование направления /специальности подготовки) |
| **Форма обучения:** |  | очная |
|  |  | (очная, очно-заочная, заочная) |
|  |  |  |

**Лабораторный практикум № 3**

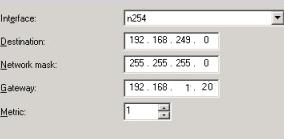
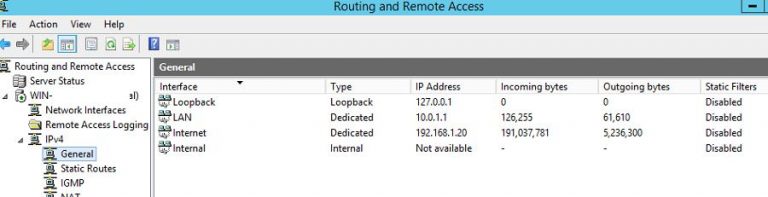
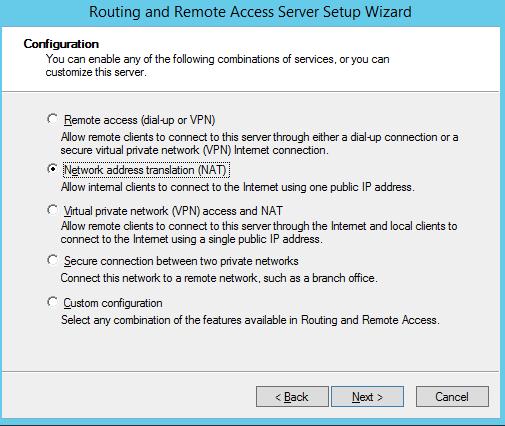
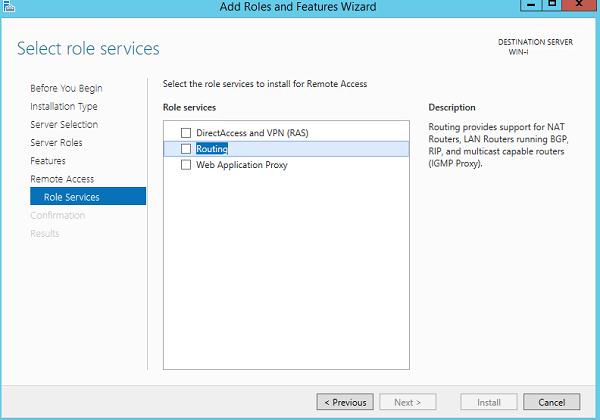
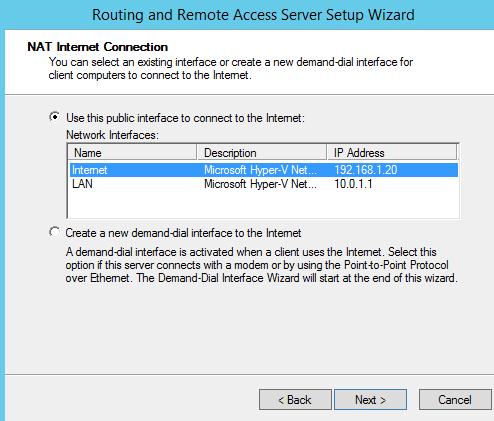
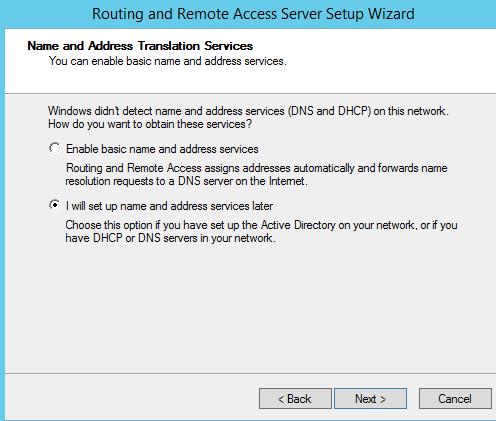
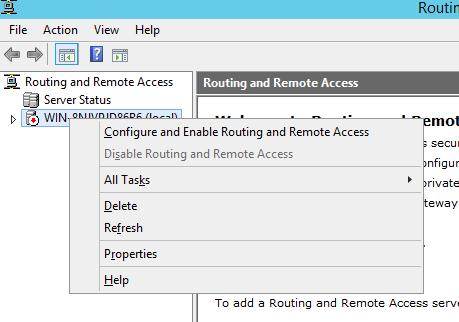
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **по дисциплине** |  | Администрирование информационных систем | | |
|  | | |  | (наименование дисциплины) |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Обучающийся** |  | **Клепиков Сергей Григорьевич** |  |  |
|  |  | (ФИО) |  | (подпись) |
| **Группа** |  | **Вбио - 304 рсоб** |  |
|  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Преподаватель** |  | Сибирев Иван Валерьевич |  |  |
|  |  | (ФИО) |  | (подпись) |

**Москва 2024 г**

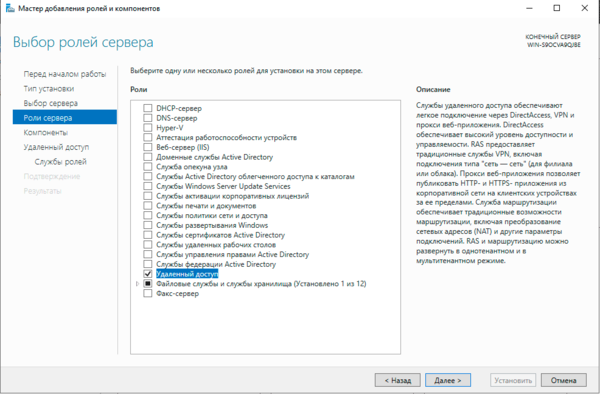
1. Провести настройку средств администрирования служб маршрутизации в Microsoft RRAS Microsoft Windows Server 2012 R2.

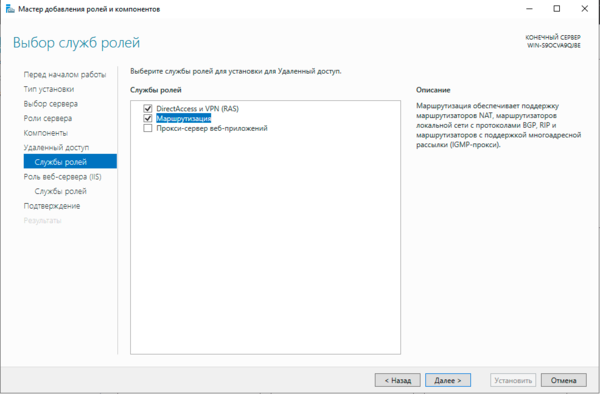


2. Провести настройку средств удаленного доступа в Microsoft RRAS Microsoft Windows Server 2012 R2.

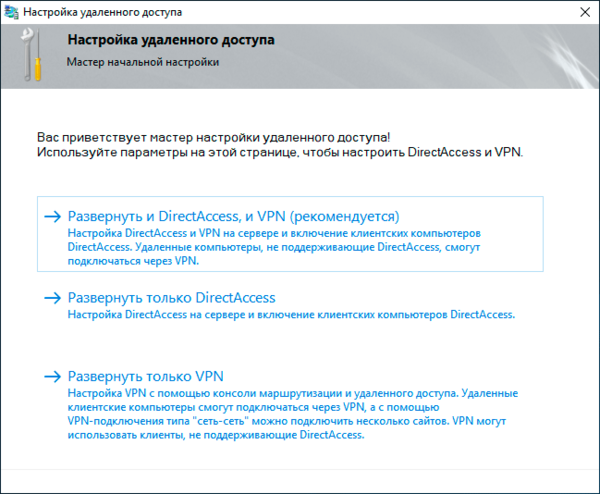
### Установка и настройка службы маршрутизации и удаленного доступа

Для начала работы с VPN в среде Windows Server потребуется установить роль **Удаленный доступ**

[](https://interface31.ru/tech_it/assets_c/2020/11/PPTP-L2TP-VPN-Windows-RRAS-001-12296.html)В **Службах ролей** выбираем **Маршрутизация**, роль**DirectAccess и VPN (RAS)** будет добавлена автоматически.

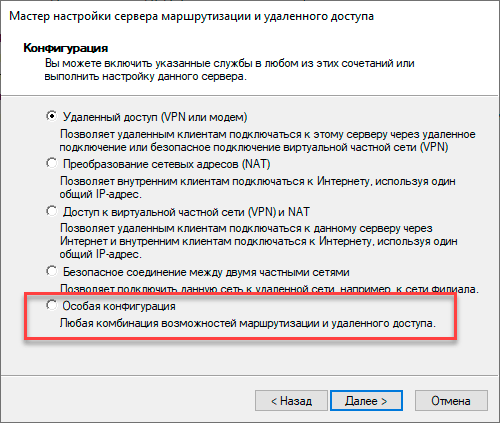
[](https://interface31.ru/tech_it/assets_c/2020/11/PPTP-L2TP-VPN-Windows-RRAS-002-12299.html)После установки роли **Удаленный доступ** ее следует настроить, проще всего это сделать, нажав на значок с желтым треугольником в **Диспетчере серверов** и выбрать в появившемся списке пункт **Запуск мастера начальной настройки**.

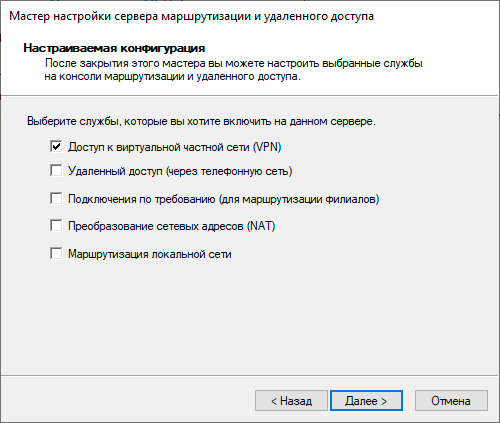
В появившемся окне выбираем пункт **Развернуть только VPN**.

[](https://interface31.ru/tech_it/assets_c/2020/11/PPTP-L2TP-VPN-Windows-RRAS-004-12305.html)

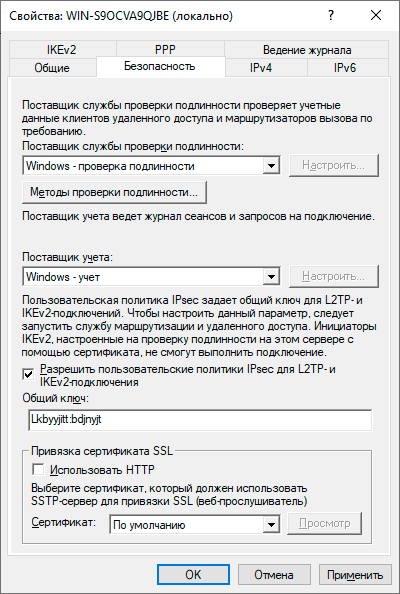
Затем в оснастке **Маршрутизация и удаленный доступ** щелкаем правой кнопкой мыши по строке с сервером и выбираем в выпадающем меню **Настроить и включить маршрутизацию и удаленный доступ**.

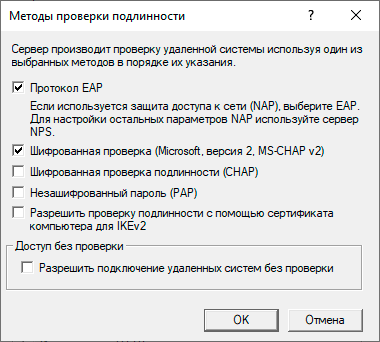
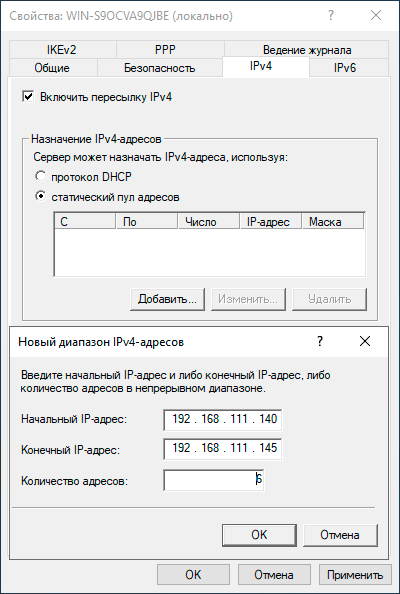
[](https://interface31.ru/tech_it/assets_c/2020/11/PPTP-L2TP-VPN-Windows-RRAS-005-12308.html)После чего появится хорошо знакомое окно мастера настройки, предлагающее сразу несколько типовых конфигураций

В следующем окне достаточно поставить галочку **Доступ к виртуальной частной сети (VPN)** и завершить работу мастера.

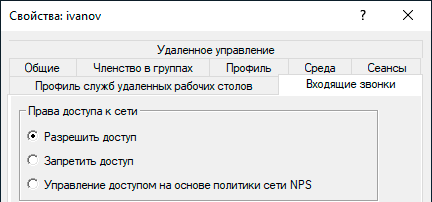
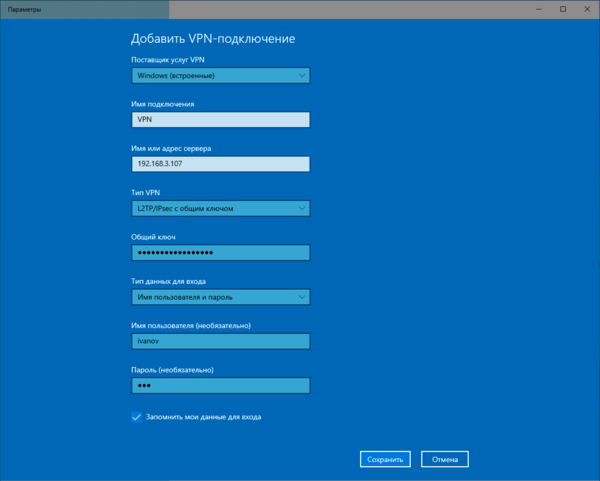
После завершения работы мастера служба **Маршрутизации и удаленного доступа будет запущена** и можно приступить к настройке сервера удаленного доступа.

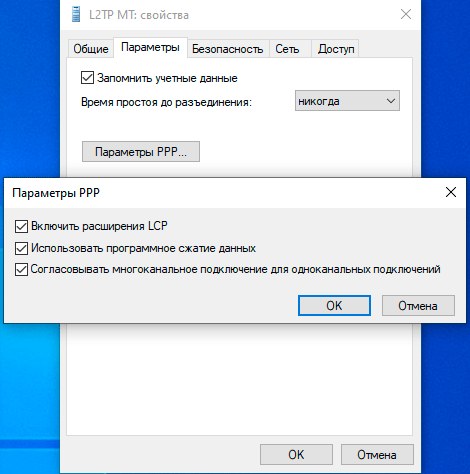
### PPTP-L2TP-VPN-Windows-RRAS-008.png

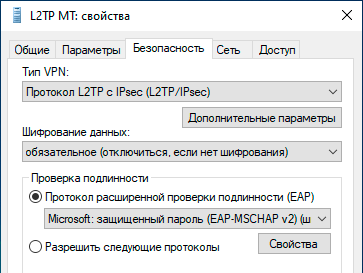
Нажав на кнопку **Методы проверки подлинности** откроем окно, в котором выберем только **Протокол EAP** и **Шифрованная проверка (Microsoft, версия 2, MS-CHAP v2)**, остальные протоколы не являются безопасными и должны быть отключены.

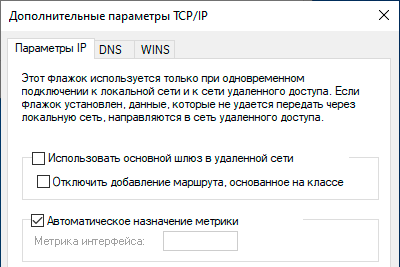
 

На этом настройка сервера может считаться законченной, следующим шагом следует разрешить подключения нужным пользователям

[](https://interface31.ru/tech_it/assets_c/2020/12/PPTP-L2TP-VPN-Windows-RRAS-014-12323.html)

Затем на закладке **Безопасность** установите в **Шифрование данных**-**обязательное**, а в пункте **Проверка подлинности** выберите **Протокол расширенной проверки подлинности (EAP)**.

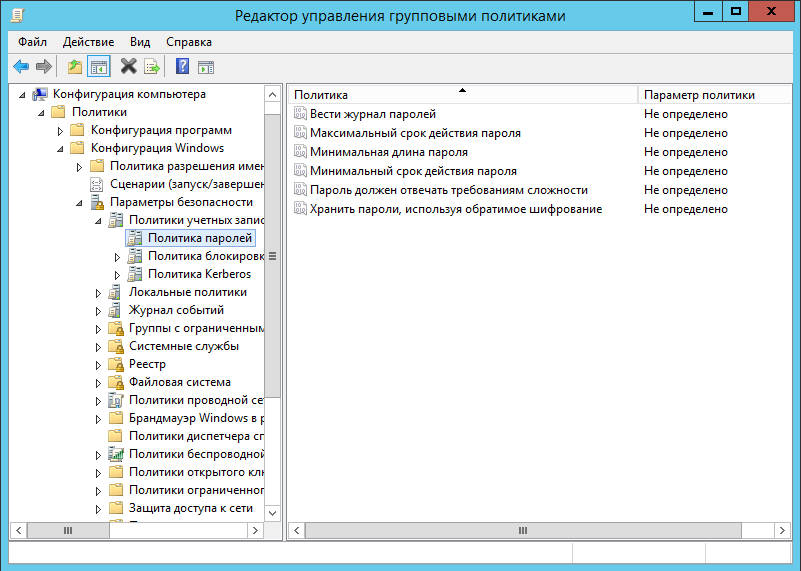
И наконец на закладке**Сеть** перейдите в свойства протокола **IP версии 4 (TCP/IP 4)** и нажмите **Дополнительно**, в открывшемся окне снимите флаг **Использовать основной шлюз в удаленной сети**, в противном случае весь исходящий трафик будет направлен в туннель.

После чего можем подключаться и пробовать получить доступ к ресурсам удаленной сети, если вы все сделали правильно, то проблем возникнуть не должно.

3. Настроить параметры политики безопасности Windows 2012 Server.

Установка параметров безопасности

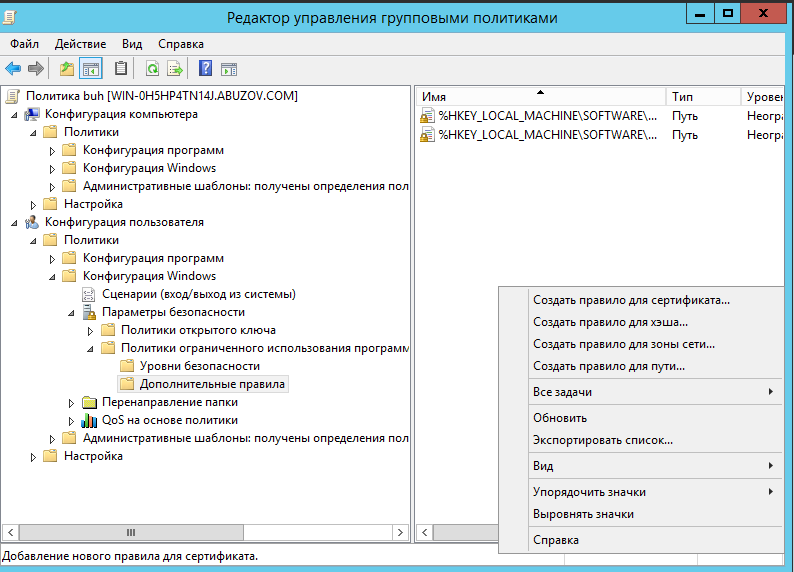
Ограничения парольной защиты

Конфигурация Windows –> Параметры безопасности –> Политики учетных записей –> Политика паролей.  


В данном разделе объекта групповой политики определяются следующие параметры:

1. «Минимальный срок действия пароля» задает периодичность смены пароля.
2. «Минимальная длина пароля» определяет минимальное количество знаков пароля.
3. «Максимальный срок действия пароля» определяет интервал времени, через который разрешается менять пароль.
4. «Пароль должен отвечать требованиям сложности» определяет требования к составу групп знаков, которые должен включать пароль.
5. «Хранить пароли, используя обратимое шифрование» задает способ хранения пароля в базе данных учетных записей.
6. «Вести журнал паролей» определяет количество хранимых устаревших паролей пользователя.

Запретим использовать командную строку на клиентском компьютере.

  
Запрет запуска командной строки (cmd.exe).  
