**Лабораторная работа по теме № 22. Настройка VPN сервера на Windows Server 2019**

**Цель –** получение навыков настройки ОС семейства Windows в качестве маршрутизатора и VPN-сервера для организации подключений типа «узел-сеть» по протоколу PPTP с авторизацией через Active Directory.

**Теоретическое введение**

VPN (англ. Virtual Private Network «виртуальная частная сеть») — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, Интернет). Несмотря на то, что коммуникации осуществляются по сетям с меньшим или неизвестным уровнем доверия (например, по публичным сетям) уровень доверия к построенной логической сети не зависит от уровня доверия к базовым сетям благодаря использованию средств криптографии.

В зависимости от применяемых протоколов и назначения, VPN может обеспечивать соединения трёх видов: узел-узел, узел-сеть и сеть-сеть.

VPN можно использовать для:

1. организации доступа клиентов из внутренней сети во внешнюю (Интернет) с авторизацией;

2. наоборот – для защищенного доступа через внешнюю сеть с авторизацией к ресурсам внутренней сети.

Описание сетевых карт в ОС Windows Server 2019 при настройке соответствуют варианту 1. Описание ролей сетевых карт, приведенное ниже, соответствует варианту 2.

Для организации VPN нужен VPN-сервер с двумя сетевыми интерфейсами, из которых до установки VPN-соединения клиенту доступен только один, а второй (вместе с доступными через него ресурсами) становится доступным после установки VPN-соединения. Интерфейсам сервера назначаются IP–адреса из различных подсетей.

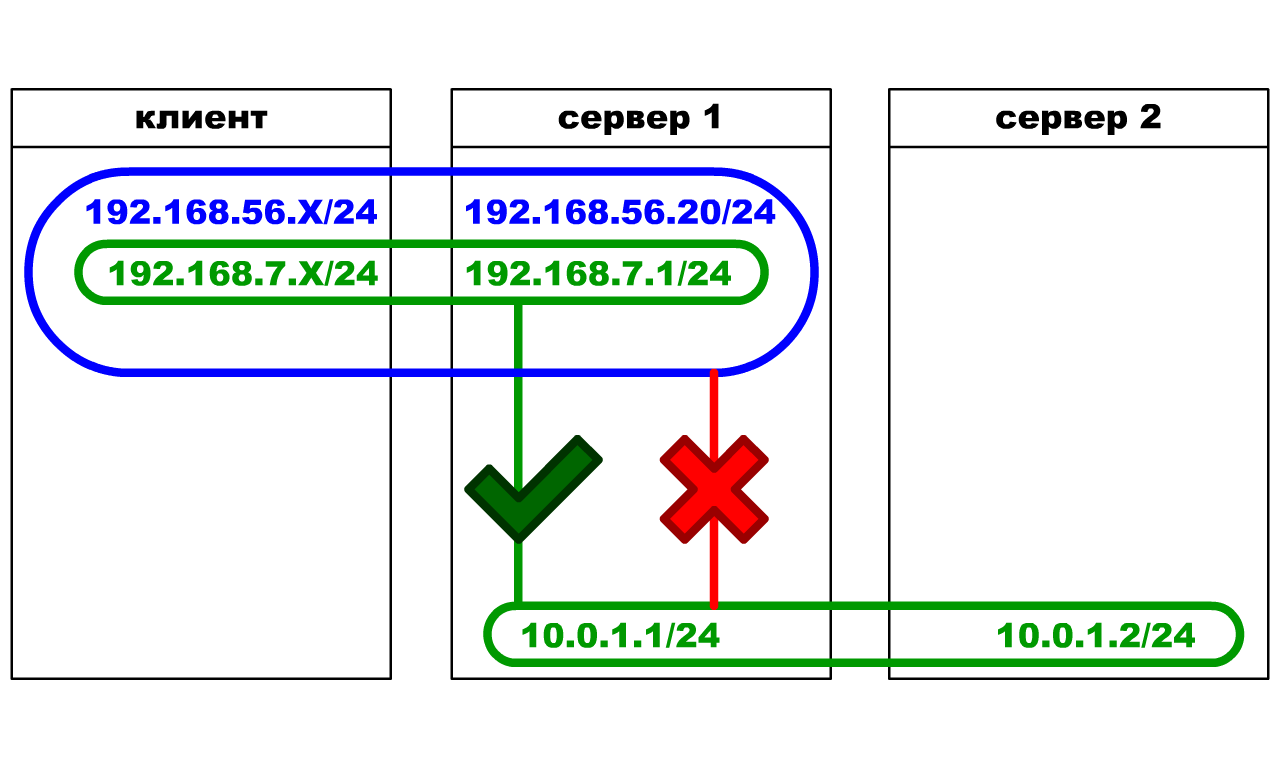
Наша задача – создать две новые сети:

– VPN, в примере ниже – с диапазоном адресов 192.168.7.1–5

– внутреннюю сеть (новая сетевая карта типа «Сетевой мост»), в примере ниже – 10.0.1.0/24.

Старую сеть (условно внешняя) с сетевыми адаптерами типа «Сетевой мост» (в примере ниже – 192.168.56.0/24) будем рассматривать как внешнюю, через которую будут подключаться клиенты.

*Внимание! Не забывайте в дополнительный настройках виртуальных адаптеров выбирать «Неразборчивый режим» «Разрешить все»!*



В роли VPN-сервера и маршрутизатора пакетов между VPN и внутренней сетью организации будет выступать ОС Windows Server 2019. Пример настройки сетевых карт:

*Сетевая карта 1 (наша старая карта типа «Сетевой мост», условно подключенная к внешней сети, к ней подключается клиент):*

***IP: 192.168.56.20/24***

*Сетевая карта 2 (новая сетевая карта типа «Сетевой мост» на ту же физическую карту, что и старая, условно подключена во внутреннюю сеть, недоступна для клиента до установки VPN-соединения):*

***IP: 10.0.1.1/24***

Доступ по протоколам VPN и маршрутизация пакетов между сетями в Windows Server 2019 реализуется на базе роли **Remote Access (RRAS, по-русски – «Удаленный доступ»).**

VPN и маршрутизация позволяют дать клиентам доступ к тем сетям, к которым имеет доступ VPN-сервер. При этом каждый пользователь при удаленном подключении должен будет вводить логин и пароль.

**Порядок выполнения работы**

**Приготовление инфраструктуры**

1. Добавьте новую виртуальную сетевую карту первому серверу и задайте ей IP-адрес сети, которая будет выступать в роли внутренней (в примере – 10.0.1.1/24).

2. Задайте второму серверу на старой сетевой карте еще один IP-адрес сети, которая будет выступать в роли внутренней (в примере – 10.0.1.2/24) и в качестве основного шлюза IP-адрес первого сервера во внутренней сети.

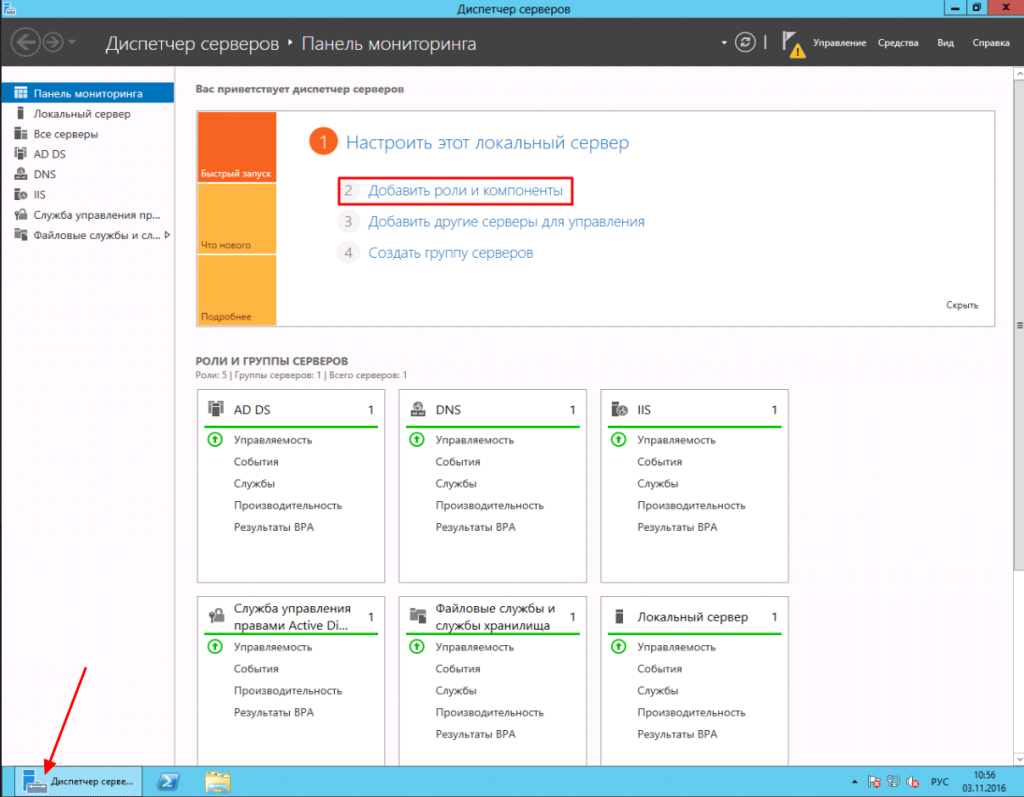
3. Проверьте командой ping обмен пакетами между клиентом и старой сетевой картой первого сервера – должно работать.

4. Проверьте командой ping обмен пакетами между первым сервером и вторым сервером – должно работать.

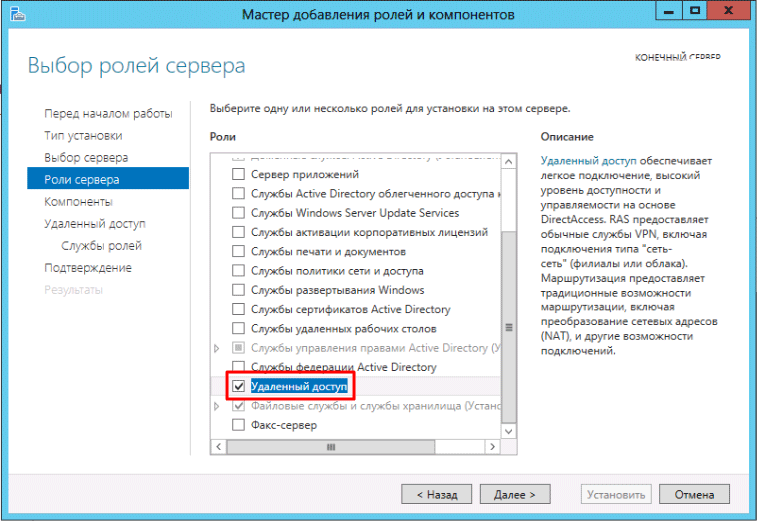
5. Проверьте командой ping обмен пакетами между клиентом и вторым сервером – НЕ должно работать. Должно заработать только в конце лабораторной работы, когда все настроите.

**Установка роли VPN на Server 2019**

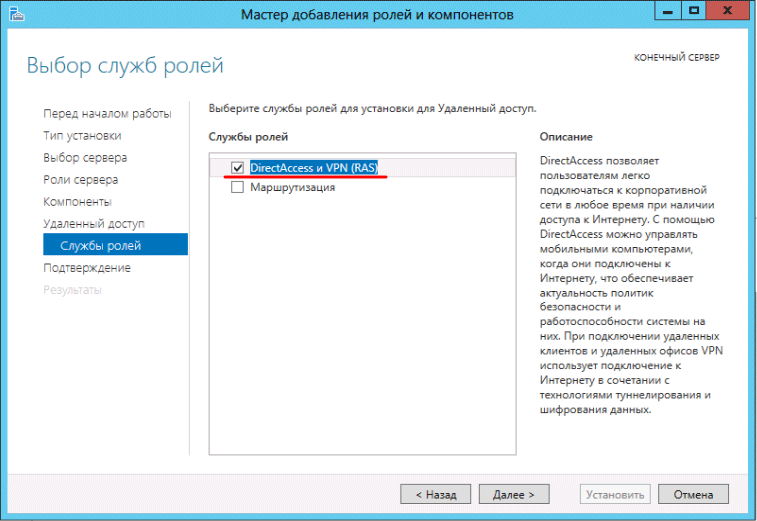
На первом сервере, который с двумя сетевыми картами, откройте «**Диспетчер серверов**» и в открывшимся окне запустите оснастку «**Добавить роли и компоненты**»



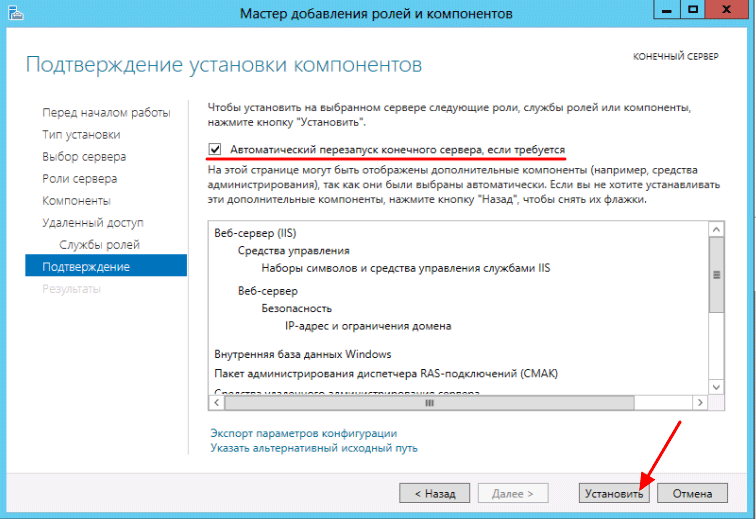
Затем оставляем все по умолчанию и останавливаемся на вкладке «**Роли сервера**» ставим галочку напротив надписи: «**Удаленный доступ**» у вас откроется окно, в котором в котором необходимо кликнуть «**Добавить компоненты**» ну и для продолжения жмем «**Далее**»



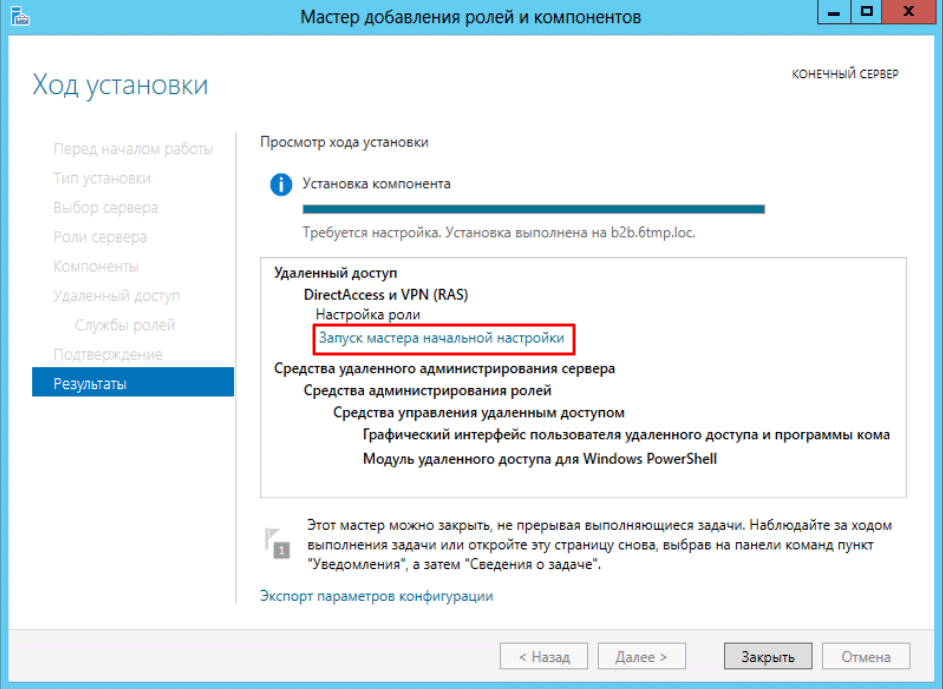
Останавливаемся на вкладке «**Службы ролей**» и убедившись, что выбрана роль «**DirectAccess и VPN (RAS)**» и «**Маршрутизация**» нажимаем «**Далее**»

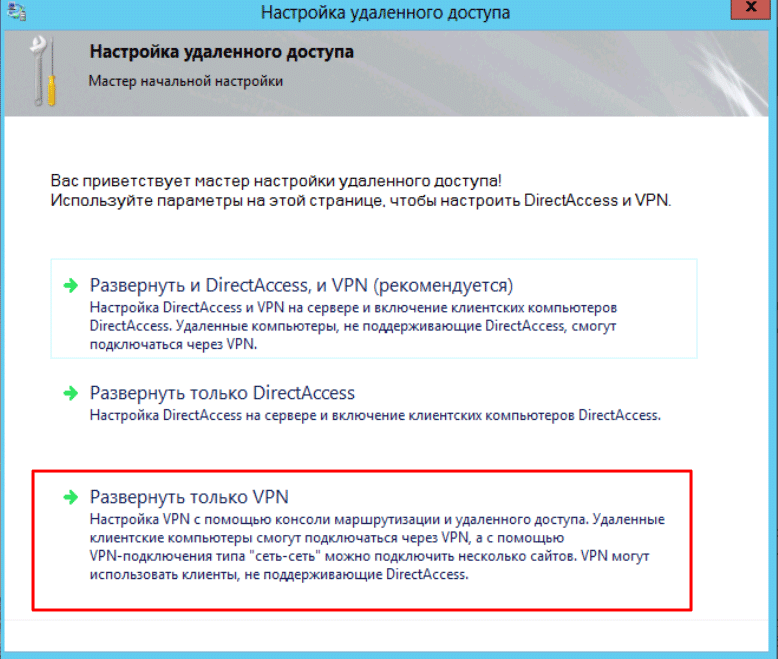
Во вкладке «**Подтверждение**» ставим птичку напротив надписи: «**Автоматический перезапуск конечного сервера, если требуется**» и нажимаем «**Установить**»



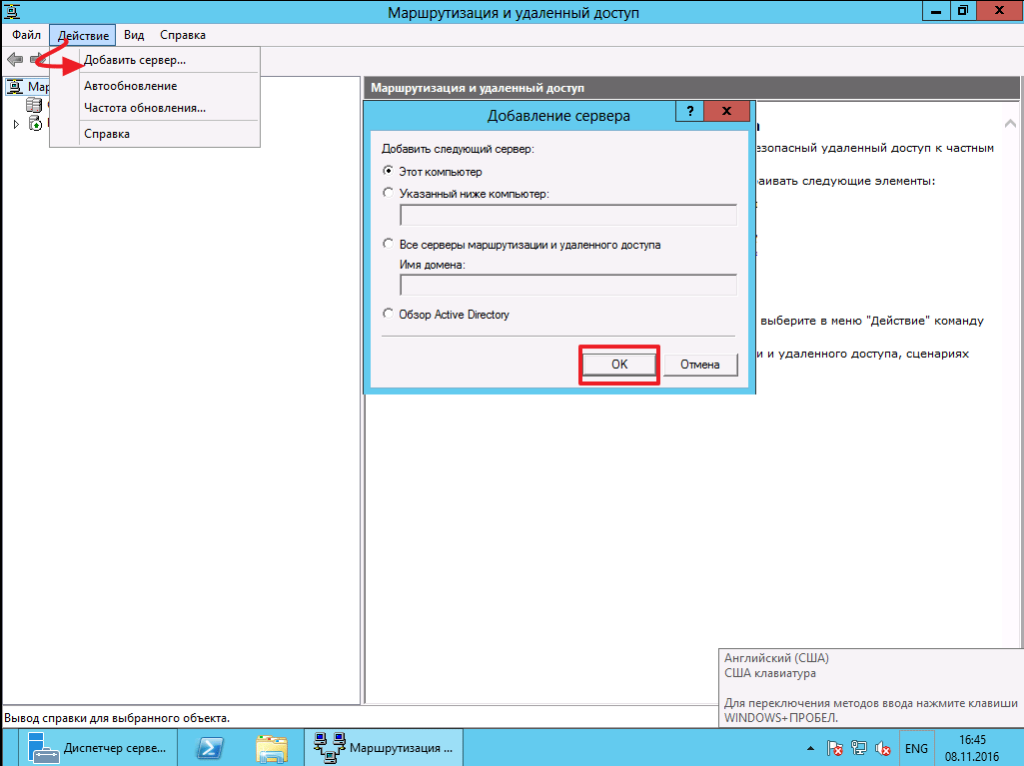
После того как установка роли удаленного доступа завершена, нам потребуется провести начальную настройку, для того что бы это сделать кликните по надписи: «**Запуск мастера начальной настройки**»



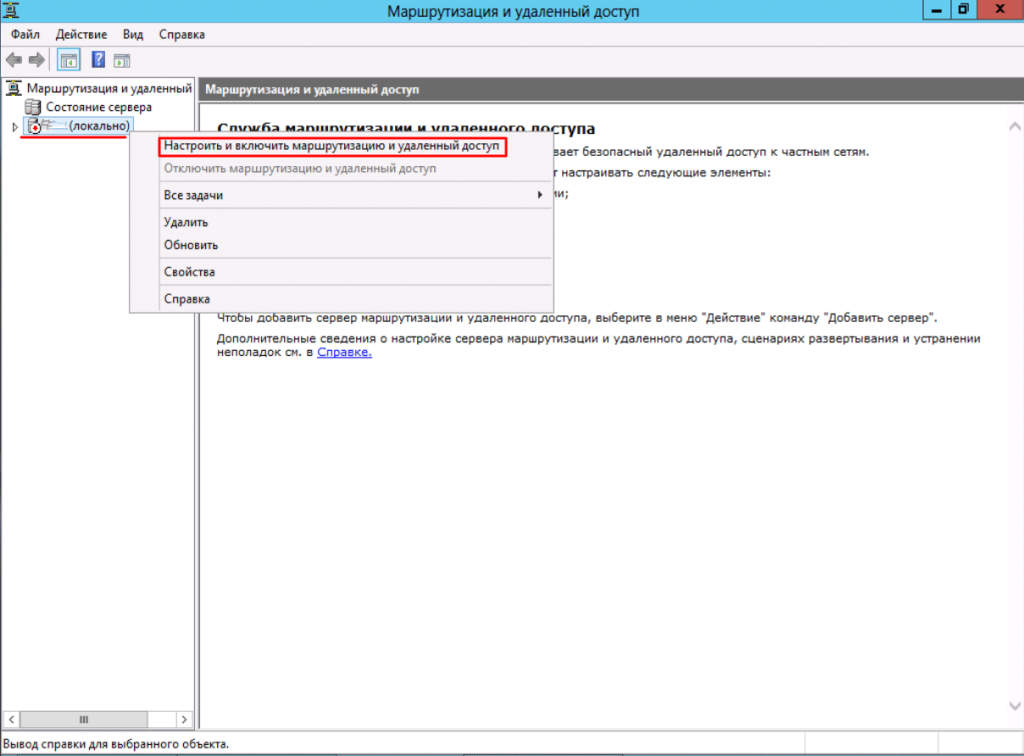
У вас сразу должен открыться мастер начальной настройки удаленного доступа, в нем потребуется выбрать 3-й пункт с названием: «**Развернуть только VPN**»



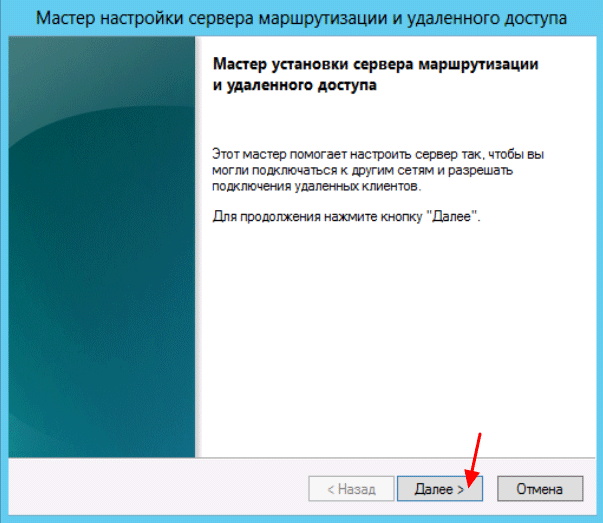
После выполнения вышеуказанных настроек добавьте текущий сервер нажав в верхнем меню «**Действие**» затем «**Добавить сервер**» после чего «**Ок**»



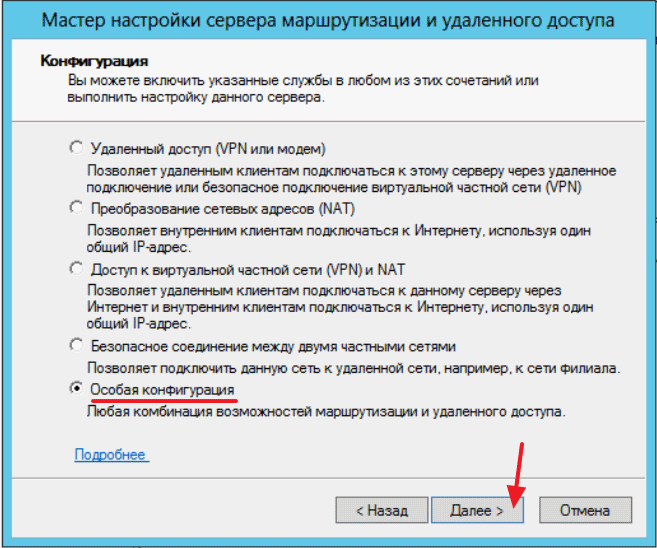
Далее жмите правой кнопкой мыши по серверу, на котором будет сконфигурирована роль VPN и выберите пункт «**Настроить и включить маршрутизацию и удаленный доступ**»



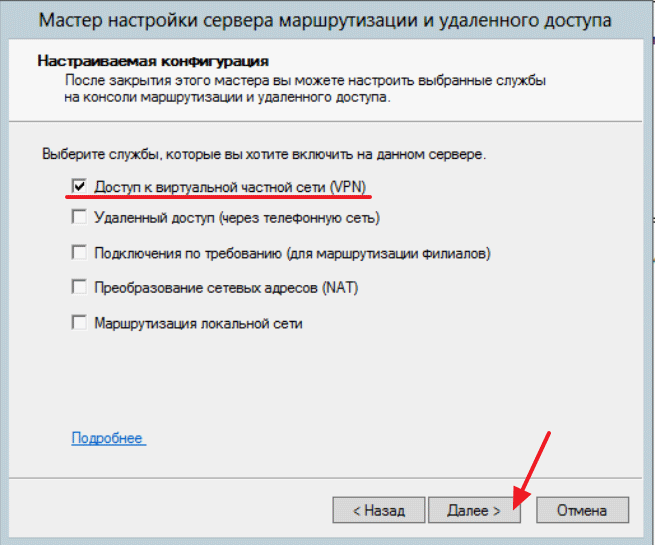
В мастере установки для продолжения конфигурации нажмите «**Далее**»



Затем выберете пункт «**Особая конфигурация**» и снова «**Далее**»



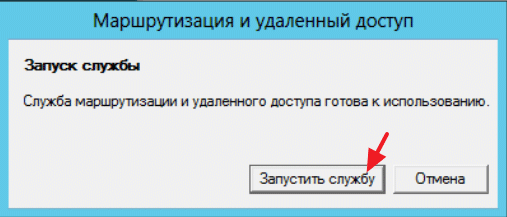
В появившимся окне выбираем службу под названием: «**Доступ к виртуальной частной сети (VPN)**» ну и соответственно «**Далее**»



После чего мастер потребует от вас запуск службы поэтому жмем «**Запустить службу**»

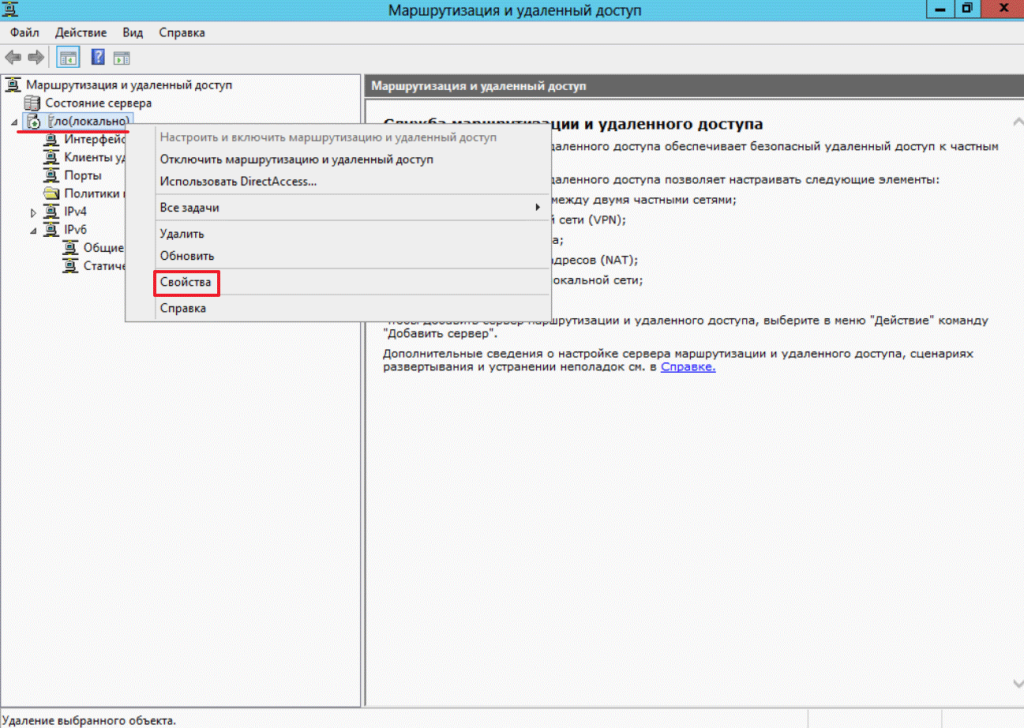
*Примечание: если у вас не открыты порты в брандмауэре, то перед запуском службы у вас всплывет окно с примечанием – игнорируйте его, так как добавлять порты мы*

*будем чуть позже…*

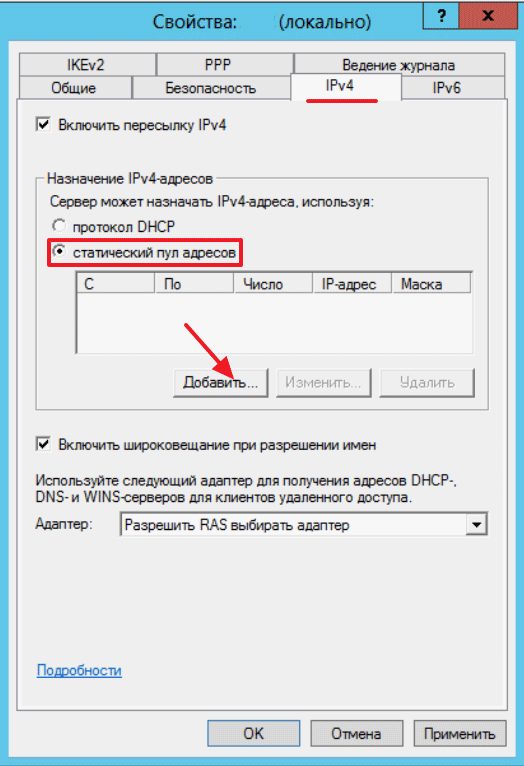


Как вы можете заметить мы почти сконфигурировали наш VPN сервер, дальнейшая настройка будет заключаться в том, чтобы задать статистический пул адресов для пользователей удаленного рабочего стола.

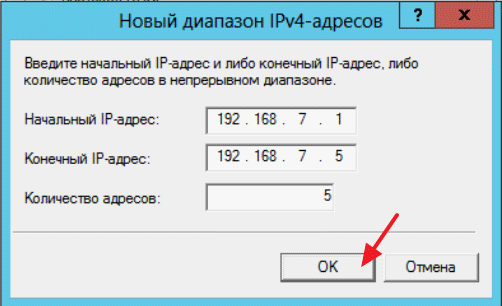
Кликните правой кнопкой мыши по серверу VPN и зайдите в его «**Свойства**»



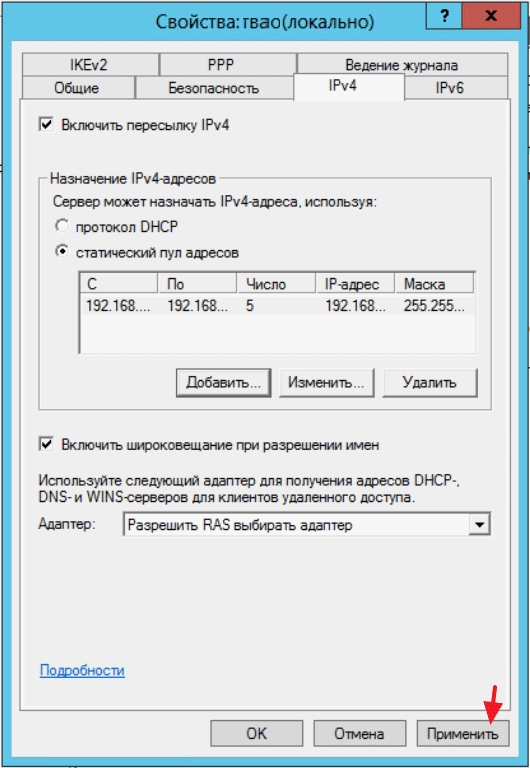
Затем перейдите во вкладку «**iPv4**» выбираем «**Статистический пул адресов**» ну и задаем параметры кнопкой «**Добавить**»



Вбиваем диапазон адресов VPN, в качестве примера я указал эти настройки, вы можете задать любые, после того как вы ввели данные нажмите «**Ок**»



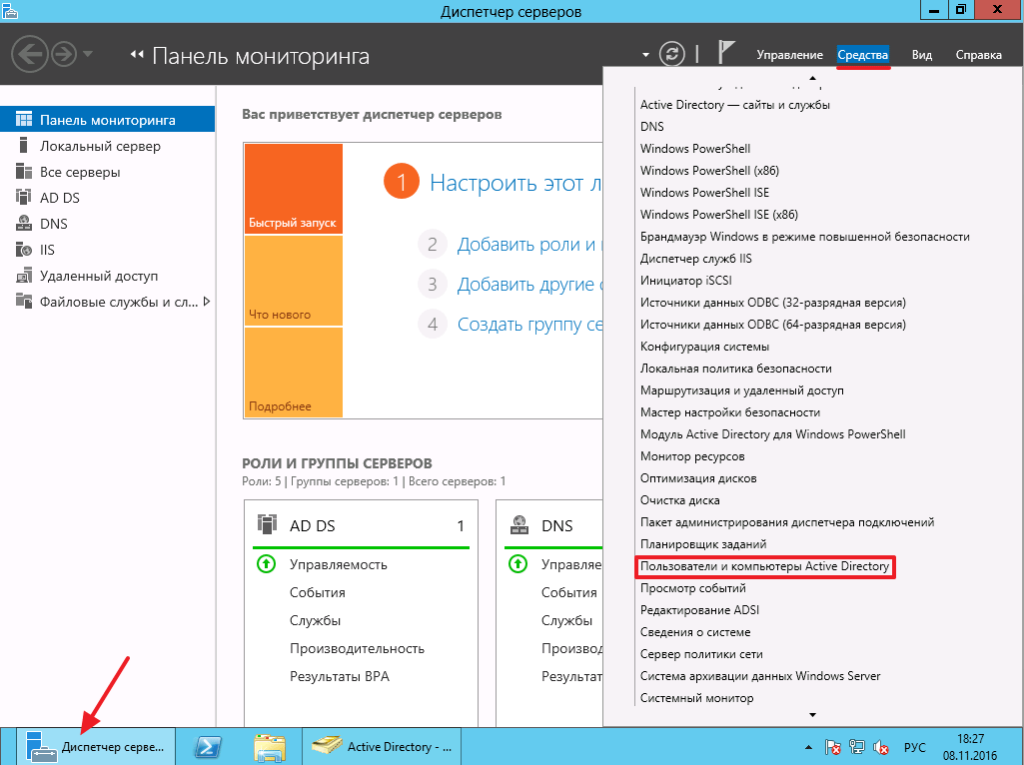
Сохраняем текущую конфигурацию настроек кнопкой «**Применить**»



На данном этапе мы сконфигурировали роль удаленного доступа VPN

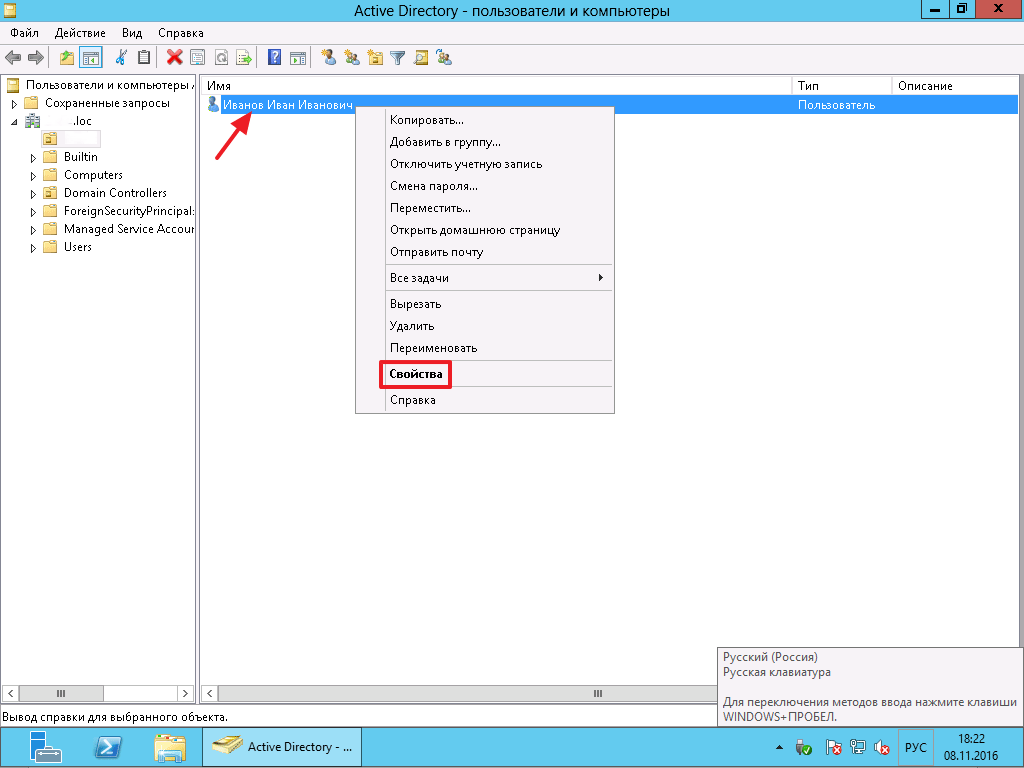
**Разрешение подключения VPN для пользователя домена**

Для начала запустите консоль AD открыв «**Диспетчер серверов**» затем в верхнем меню выберите раздел «**Средства**» и в раскрывающимся списке кликаем по пункту: «**Пользователи и компьютеры Active Directory**»

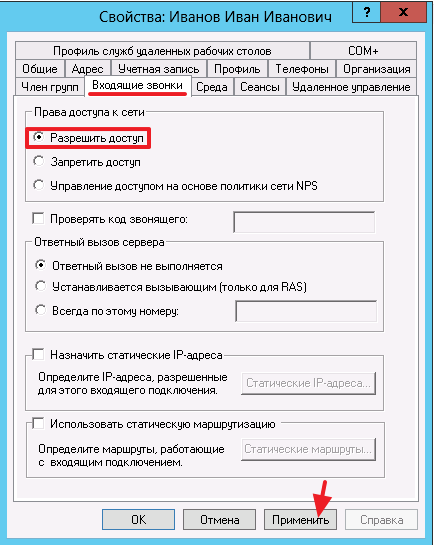


Я создал пользователя с обычными правами, в моем примере это «**Иван**» и именно ему я дам разрешение на удаленное подключение к серверу через VPN.

Сделать это очень просто – кликаем правой кнопкой мыши по данной учетной записи и переходим в «**Свойства**»



В открывшимся окне свойств откройте в верхнем меню раздел «**Входящие звонки**» затем поставьте чекбокс напротив надписи: «**Разрешить доступ**» затем сохраняем изменения нажав «**Применить**» - этим действием мы разрешили доступ по VPN

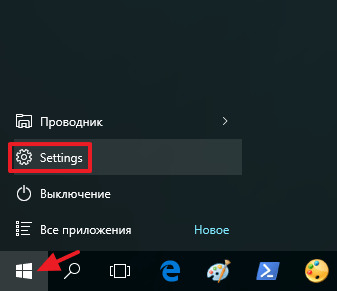


На этом настройка VPN на Server 2019 завершена, теперь необходимо протестировать все на клиенте.

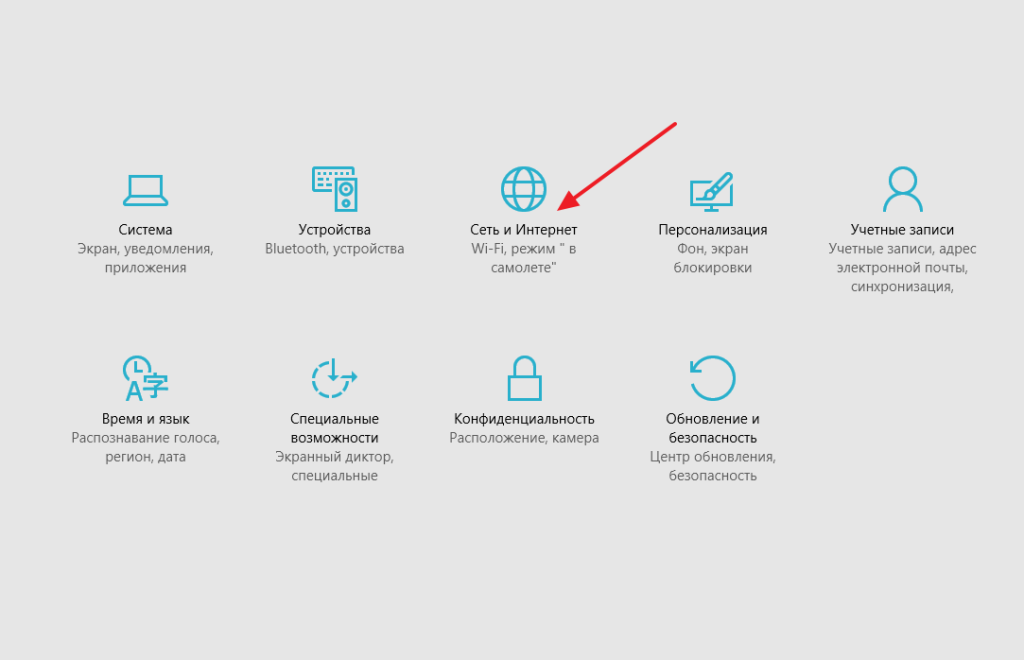
**Установка подключения VPN с клиентской ОС**

Для того что бы протестировать подключение VPN к серверу на Windows 10 необходимо создать VPN-подключение.

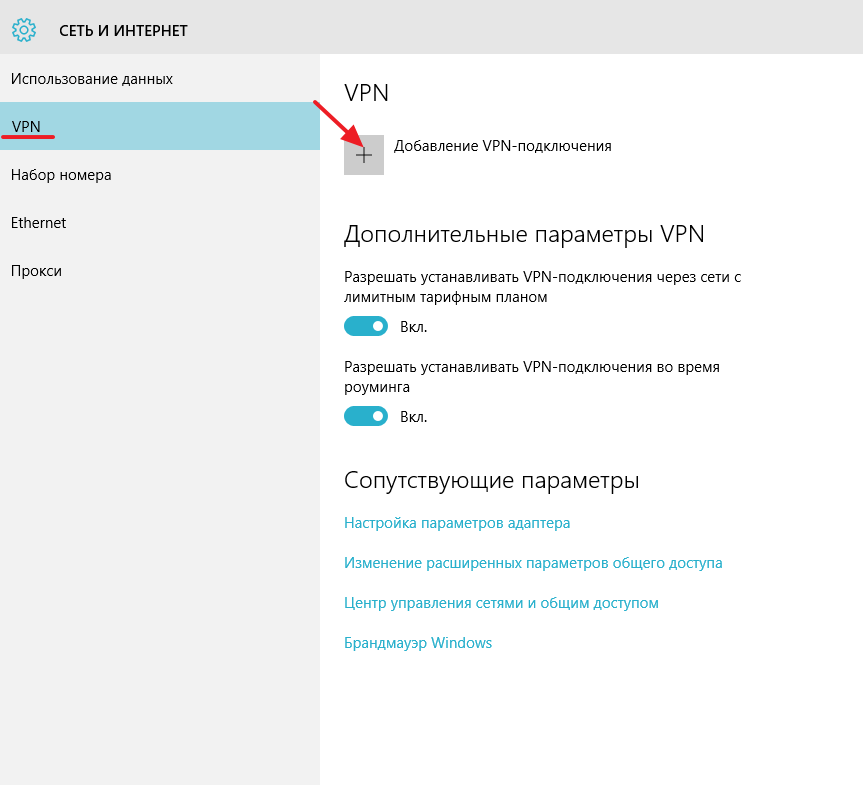
Откройте «**Меню пуск**» затем выберите вкладку «**Параметры (Settings)**»



В открывшимся окне кликаем по значку: «**Сеть и Интернет**»



В левом меню переходим на вкладку «**VPN**» в отразившихся параметрах нам необходимо добавить новое VPN подключение для этого жмем «**Добавление VPN - подключения**»



Перед нами появилось окно настроек нового VPN – подключения для Windows 10, как вы уже поняли наверно нам необходимо ввести в соответствующие столбцы параметры:

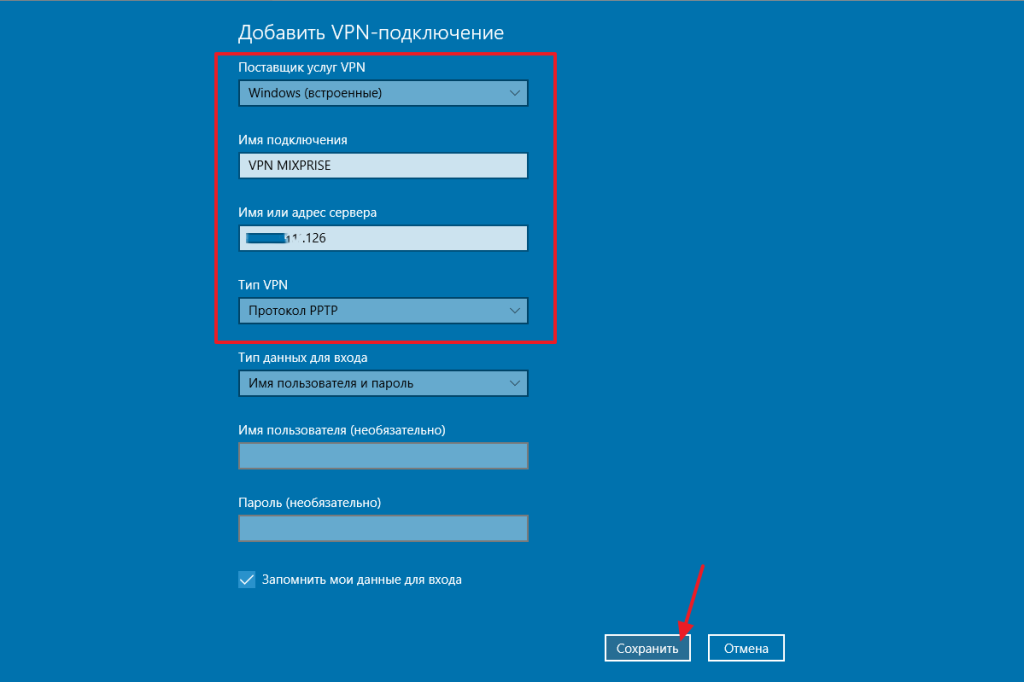
1. В окне под названием: «**Постановщик услуг VPN**» выберите параметр по умолчанию из раскрывающегося списка

2. В окне «**Имя подключения**» придумайте название вашему новому подключению

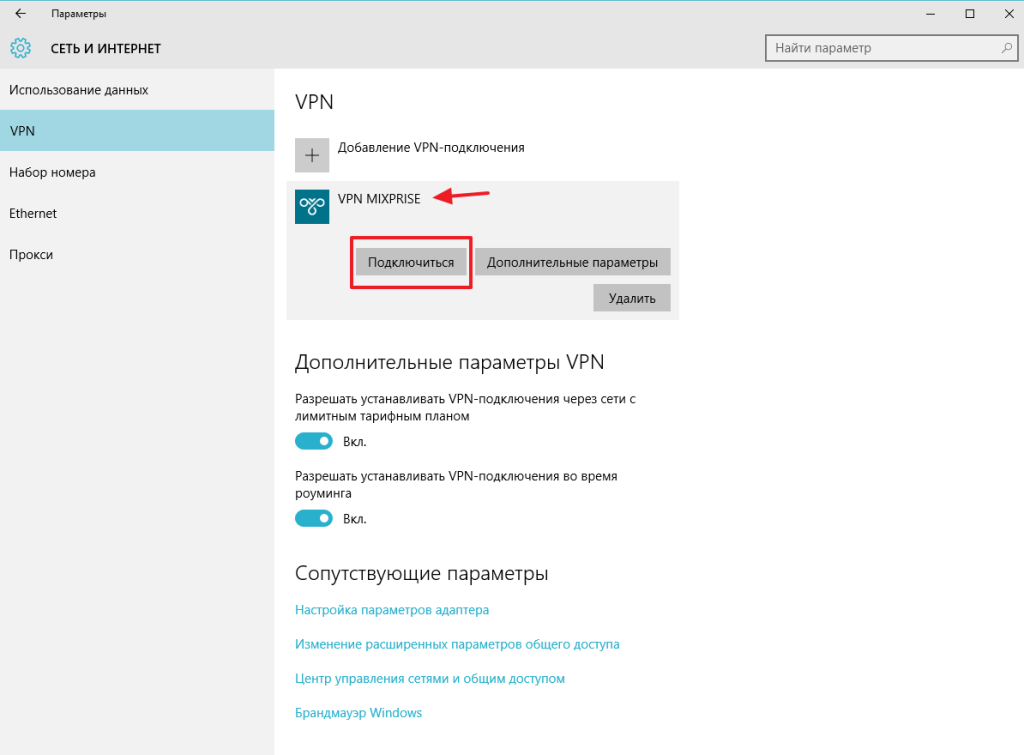
3. В следующем окне «**Имя или адрес сервера**» указываем адрес сервера в сети Интернет (в нашем случае – с сетевого адаптера типа «Сетевой мост») или же его доменное имя.

4. Переходим к следующему шагу, а именно выбору «**Тип VPN**» в соответствии с настройками, которые мы производили выше, из раскрывающегося списка выбираем «**Протокол PPTP**».

5. Нажимаем «**Сохранить**».

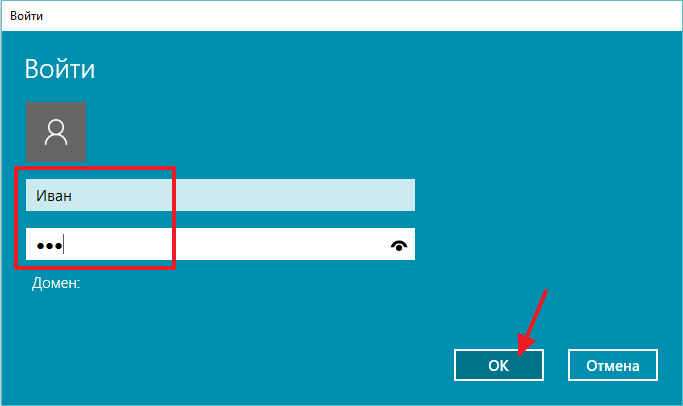


Теперь давайте запустим вновь созданное VPN подключение на Windows 10, для этого вновь откройте раздел «**Сеть и интернет**» и подключите текущее VPN соединение нажав «**Подключиться**»



Для того что бы подключиться необходимо ввести «**Имя пользователя**» и «**Пароль**» пользователю Active Directory, которому ранее давали разрешение на подключение к серверу.

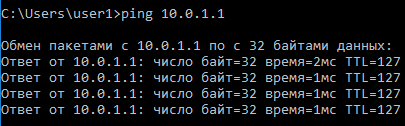
После ввода данных нажмите «**Ок**»



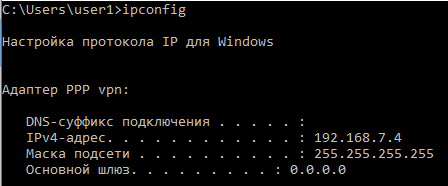
Если данные введены верно, то VPN подключение должно быть в статусе ***ПОДКЛЮЧЕНО***



После этого для проверки связи с внутренней сетью на клиенте запустите командную строку и выполните команду ping к IP-адресам серверов во внутренней сети:



Командой ipconfig посмотрите, что для VPN-подключения создался новый виртуальный сетевой адаптер с IP-адресом из диапазона VPN (192.168.7.1-5):



В окне параметров нажмите кнопку «Отключиться» и убедитесь командой ping, что соединение с внутренней сетью исчезло:

