# JaCarta PKI и VPN-тоннели в Microsoft Windows Server 2016

## Руководство по настройке

Листов: 37

Автор: Dmitry Shuralev

# Аннотация

Настоящий документ содержит сведения о настройке двухфакторной аутентификации по электронным ключам **JaCarta PKI** к защищённому **VPN-соединению** для безопасного доступа из вне или во внутреннюю сеть предприятия.

# Оглавление

О технологии VPN 4
О JaCarta 4
Описание демо-стенда 4
Ход настройки 5
Установка роли IIS (web-сервер) и запрос сертификата для IIS сервера 5
Установка роли IIS (web-сервер) 5
Запрос сертификата для сервера IIS 12
Установка и настройка компонентов Удалённый доступ и Маршрутизация 14
Установка роли удалённый доступ и службы политики сети и доступа 14
Настройка маршрутизации 20
Назначение пользователю прав на использование VPN-подключения 27
Проверка работоспособности 29
Создание подключения 29
Подключение к шлюзу 31
Контакты, техническая поддержка 35
Регистрация изменений 36

# О технологии VPN

**VPN (Virtual Private Network)** — 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 (шифрования, аутентификации, инфраструктуры открытых ключей, средств для защиты от повторов и изменений, передаваемых по логической сети сообщений).

Компания Microsoft имеет собственную реализацию VPN-технологии в рамках ОС Windows Server, а компания "Аладдин Р.Д." предоставляет реализацию двухфакторной аутентификации на VPN-шлюзе. Это обеспечивает дополнительную безопасность пользователей, работающих в виртуальной сети.

Сотрудников, желающих использовать личные устройства, такие как ноутбуки, портативные ПК и планшеты, для подключения к корпоративным сетям, когда они не присоединены к домену, становится с каждый днем всё больше и крайне важно обеспечить защиту подключений в корпоративную сеть извне. Возможность подключения к виртуальной частной сети (VPN), открывающей удалённый доступ к корпоративной сети, предусмотрена для всех устройств на базе ОС Windows. Настоящий документ в полном объёме описывает настройку VPN-шлюза и доступа в защищённую сеть с использованием электронного ключа **JaCarta PKI.**

# О JaCarta

Для аутентификации на VPN-шлюзе подойдёт вся линейка электронных ключей **JaCarta PKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где в дополнение или вместо ввода PIN-кода в качестве фактора аутентификации используется отпечаток пальца. .


> JaCarta PKI — USB-, MicroUSB-токен или смарт-карта для строгой двухфакторной аутентификации пользователей при доступе к защищённым информационным ресурсам предприятия, безопасного хранения ключей, ключевых контейнеров программных СКЗИ с использованием инфраструктуры открытых ключей (PKI) на основе зарубежных криптоалгоритмов.

# Описание демо-стенда

Демо-стенд состоит из следующих компонентов.

### Сервер

**Windows Server 2016 Datacenter** с установленным программным обеспечением **Единый Клиент JaCarta** и настроенными ролями серверов **Active Directory** и **Active Directory Certificate Services**.

> Роль шлюза VPN будет настроена на этом же сервере в рамках настоящего документа. Опционально можно установить на отдельный от AD и CS сервер.
>
> Подробное руководство об установке и настройке **Active Directory Certificate Services** доступно в документе — "**JaCarta PKI для аутентификации в домене Windows Server 2016**", который размещен на официальном сайте "Аладдин Р.Д.", в разделе "Интеграционные инструкции" — https://www.aladdin-rd.ru/support/guides.

### Клиент

**Невходящая в домен рабочая станция — Windows 10,** с установленным программным обеспечением **Единый Клиент JaCarta.**

# Ход настройки

Настройка происходит на сервере и клиенте, делится на следующие этапы.

**На сервере:**

- установка роли IIS (web-сервер);
- запрос сертификата для IIS сервера;
- установка и настройка компонентов Удалённый доступ, Маршрутизация;
- назначение прав на удалённый доступ для пользователей.

**На клиенте:**

- создание VPN-подключения;
- проверка работоспособности.

# Установка роли IIS (web-сервер) и запрос сертификата для IIS сервера

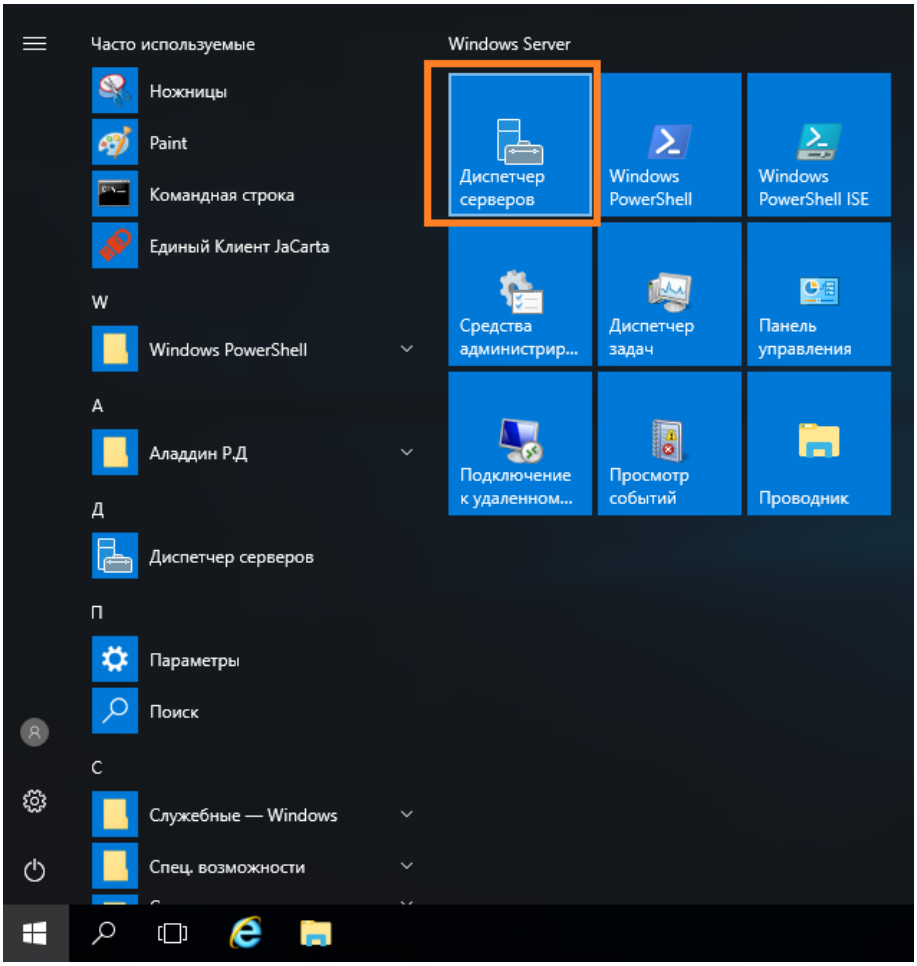
Для организации VPN-соединения с аутентификацией по смарт-картам необходима роль Web-сервера и сертификат для этого сервера.

> Важно, чтобы сертификат был выпущен до установки и настройки
>
> маршрутизации, политик сети и доступа.

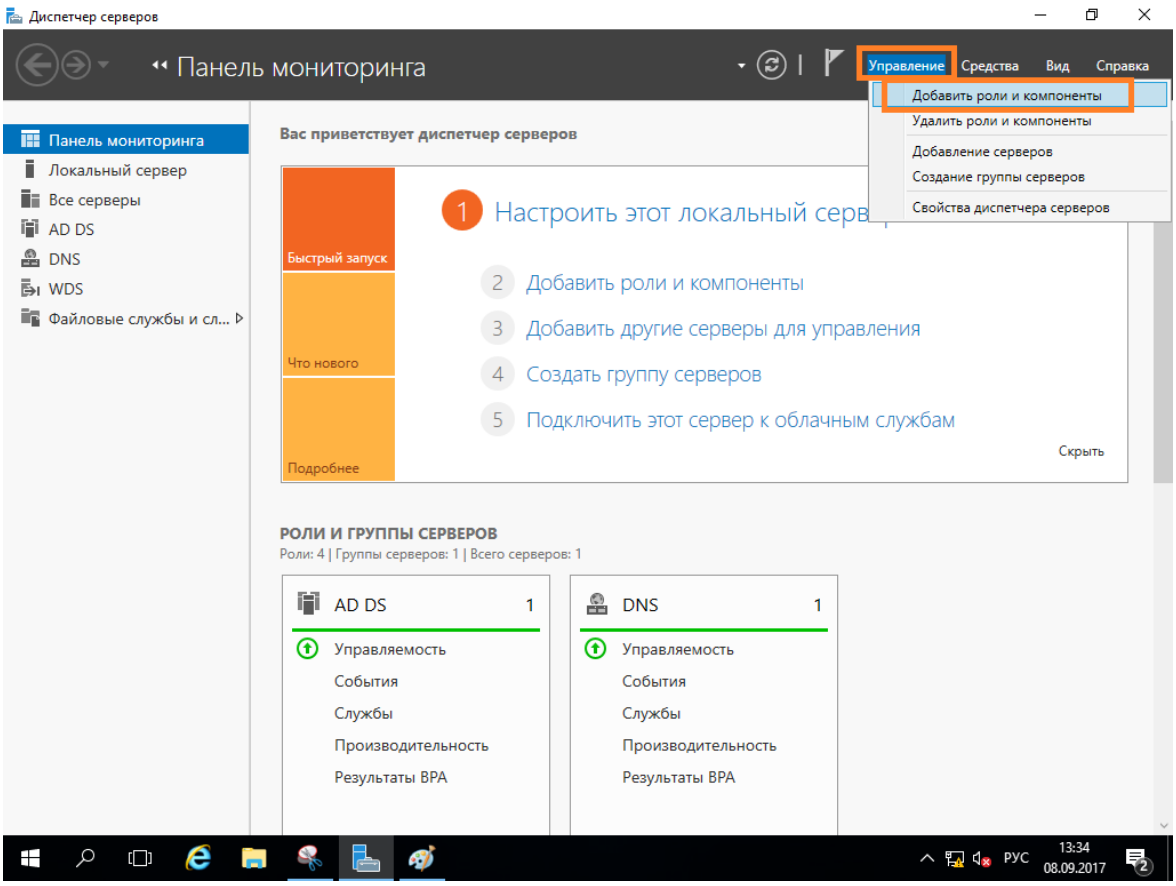
## Установка роли IIS (web-сервер)

Если ранее на сервере была установлена роль IIS, перейдите к следующему разделу. В противном случае, установите компонент. Для этого выполните следующие действия.

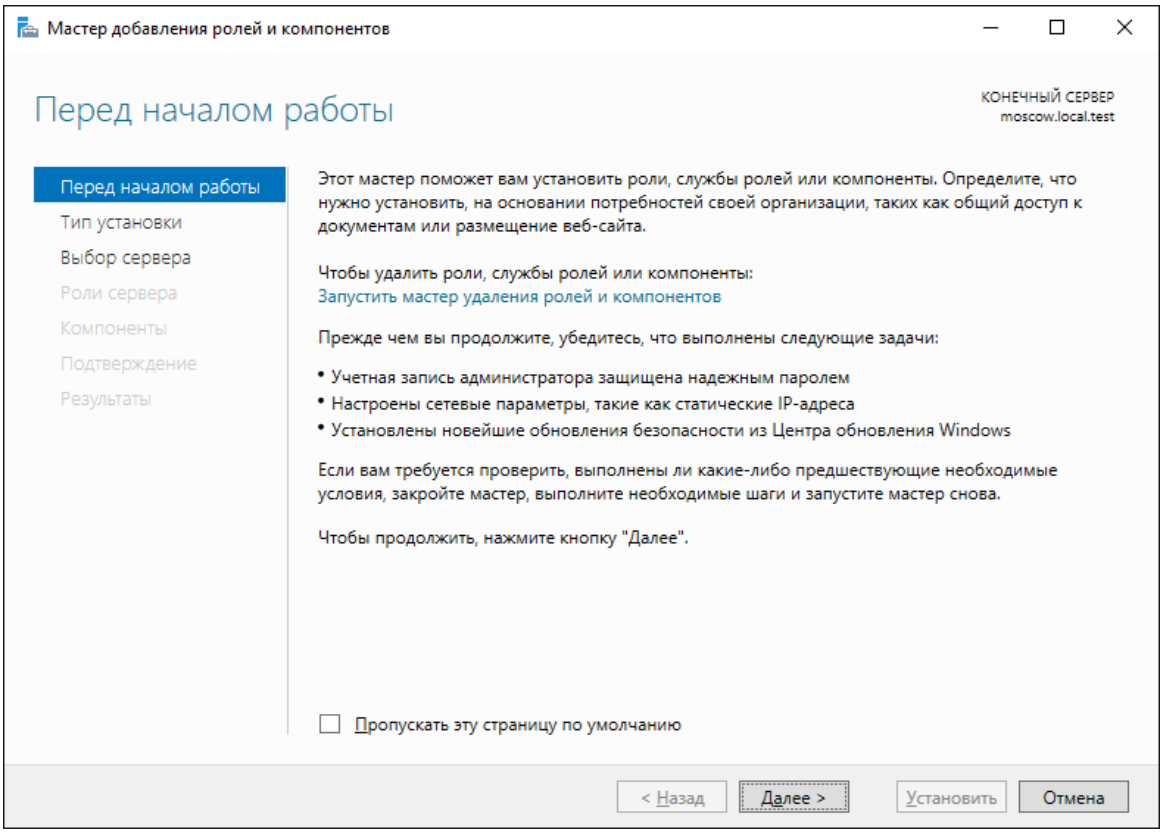
Нажмите **Пуск -> Диспетчер серверов.**



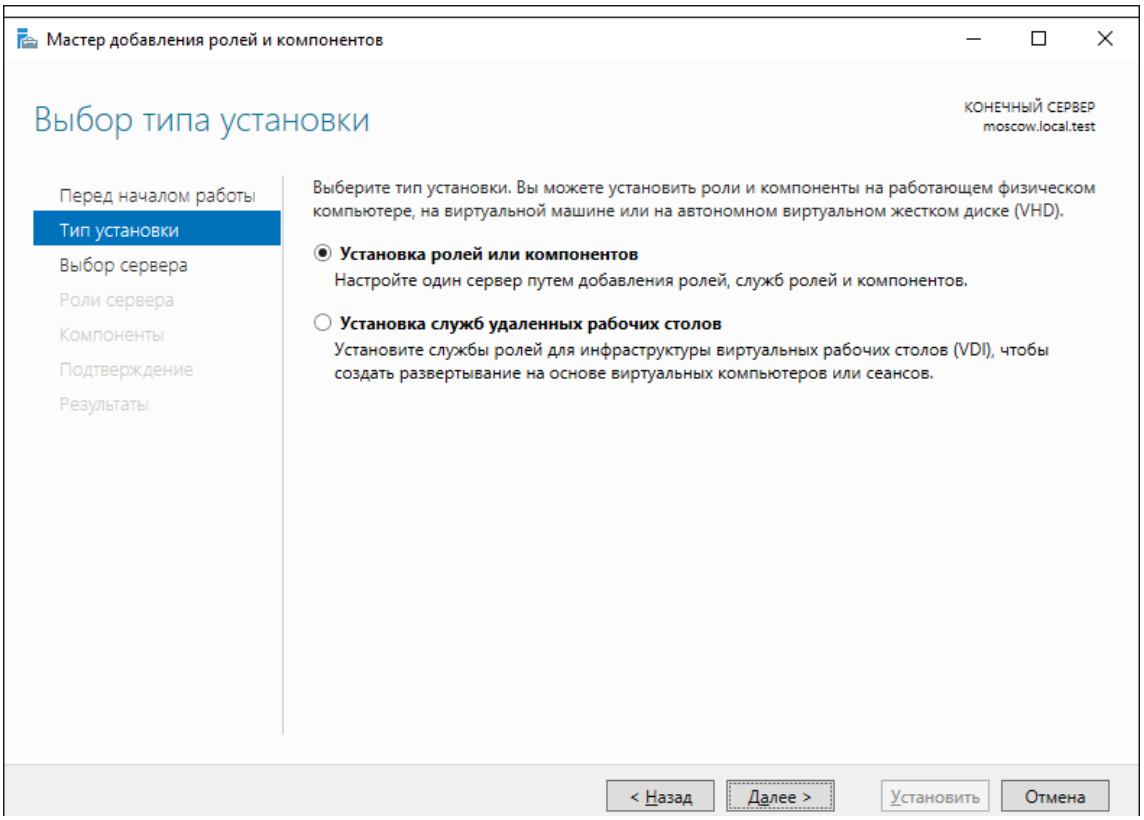
В отобразившемся окне выберите **Управление -> Добавить роли и компоненты.**



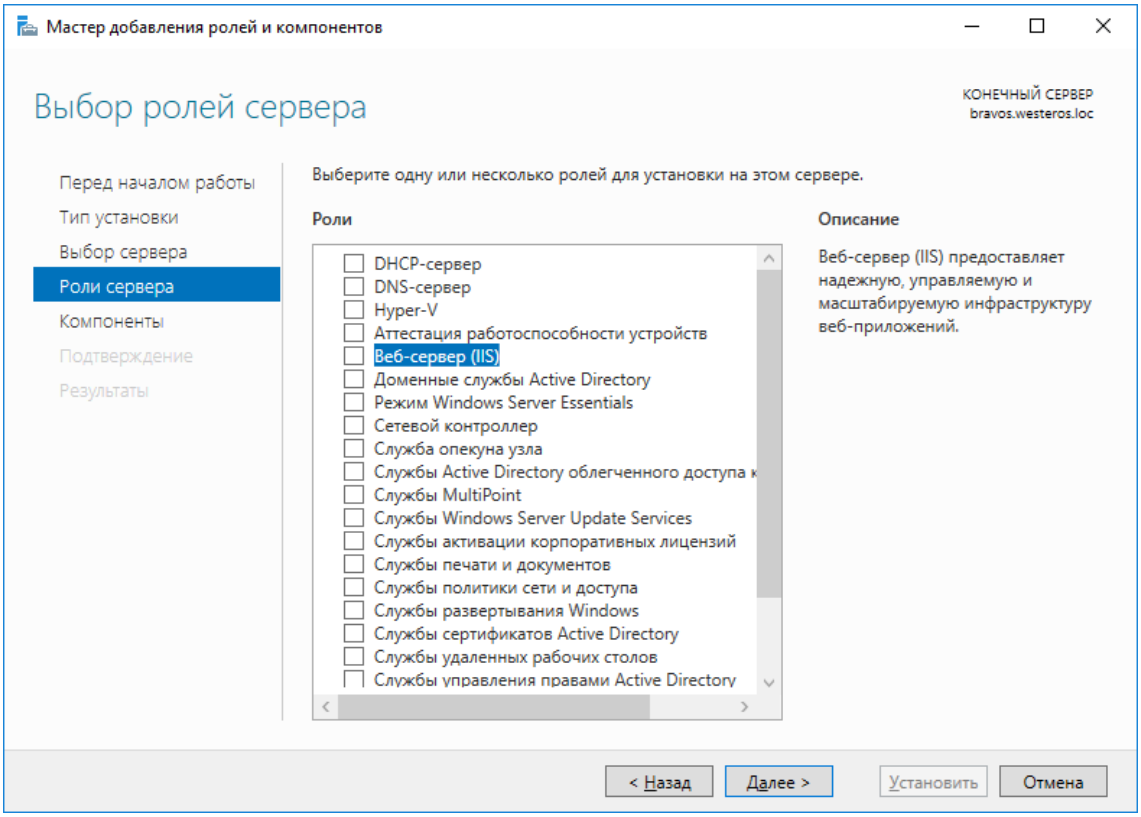
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее.**



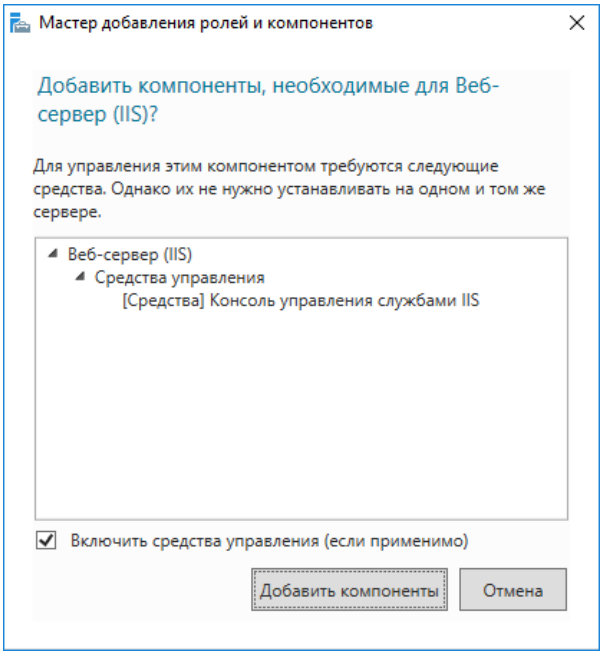
В следующем окне выберите **Установка ролей и компонентов.**



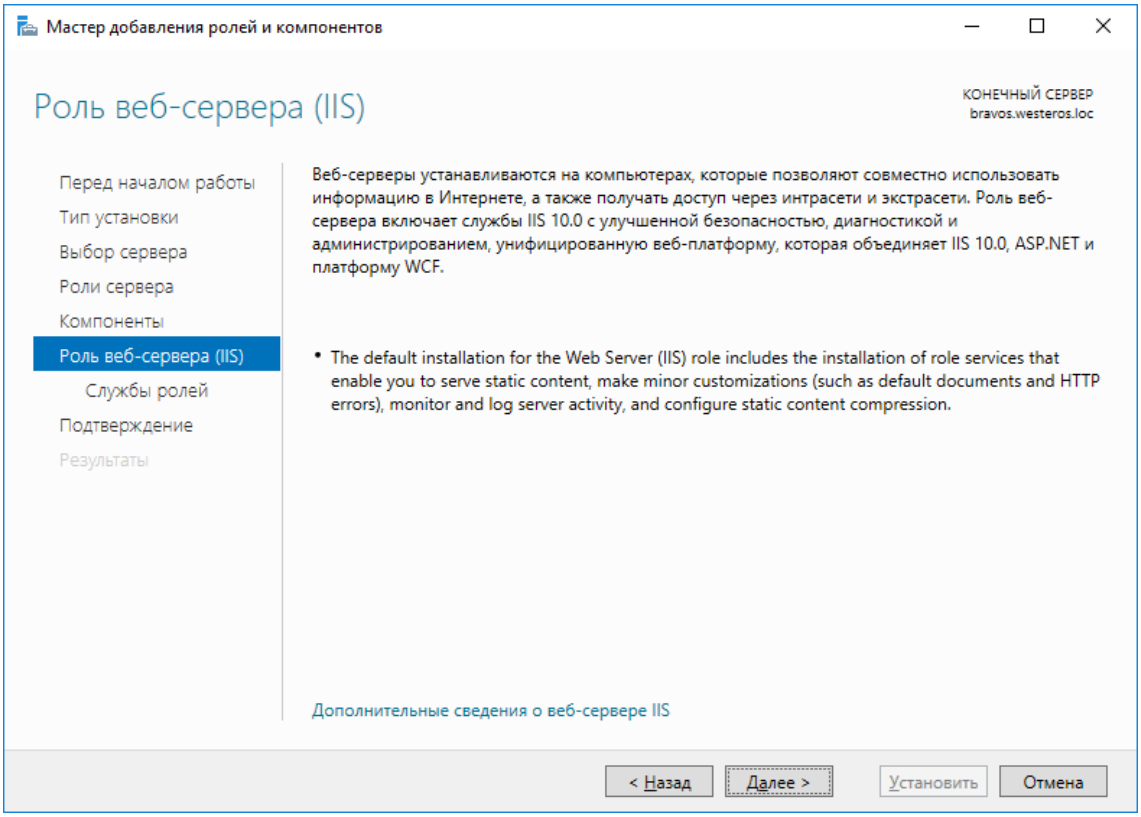

Отобразится окно добавления новых ролей, выберите **Веб-сервер (IIS)** и нажмите **Далее.**



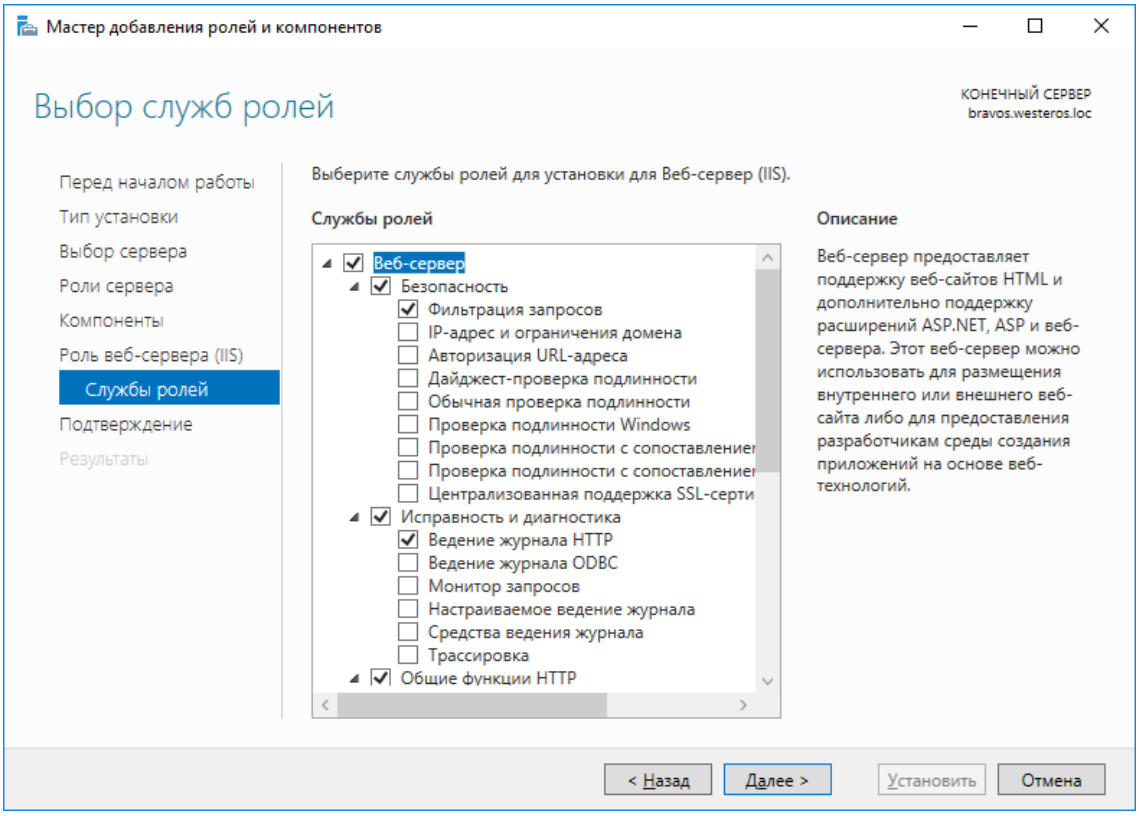

В отобразившемся окне нажмите **Добавить компоненты.**



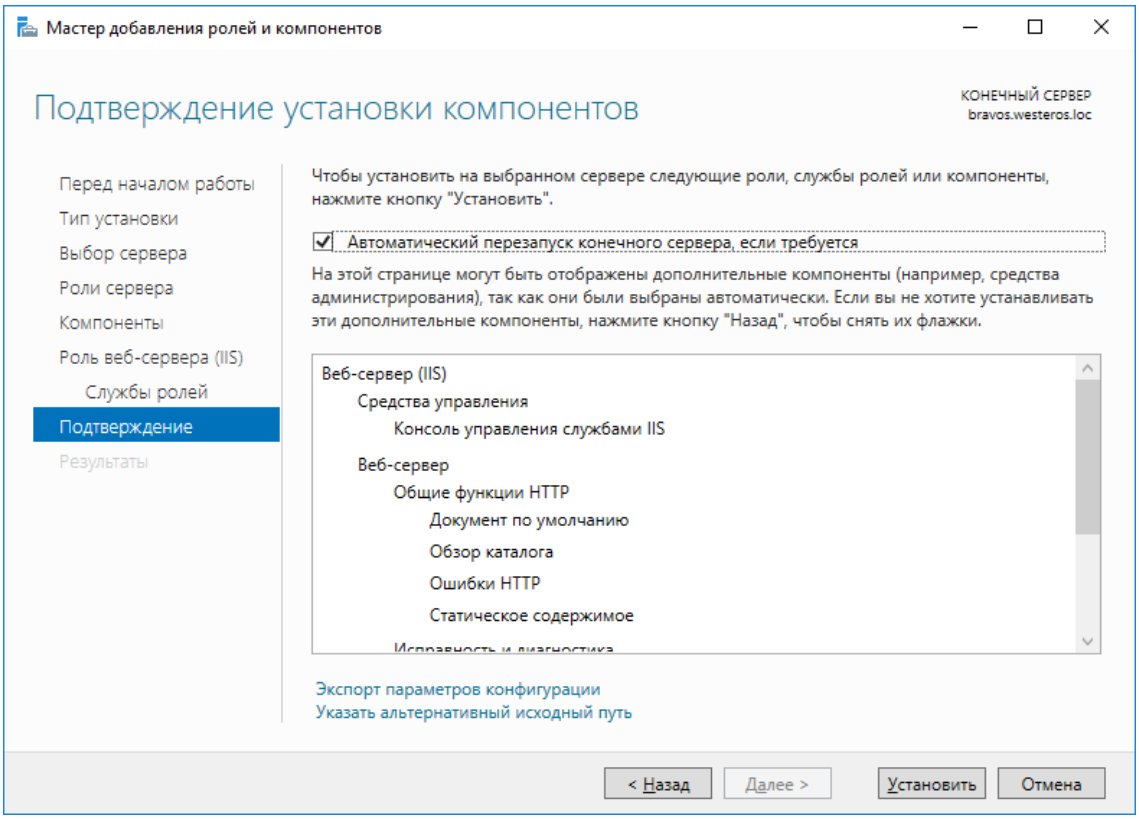

В отобразившемся окне нажмите **Далее.**




В отобразившемся окне **Службы ролей** выбранные параметры можно оставить по умолчанию. Нажмите **Далее.**



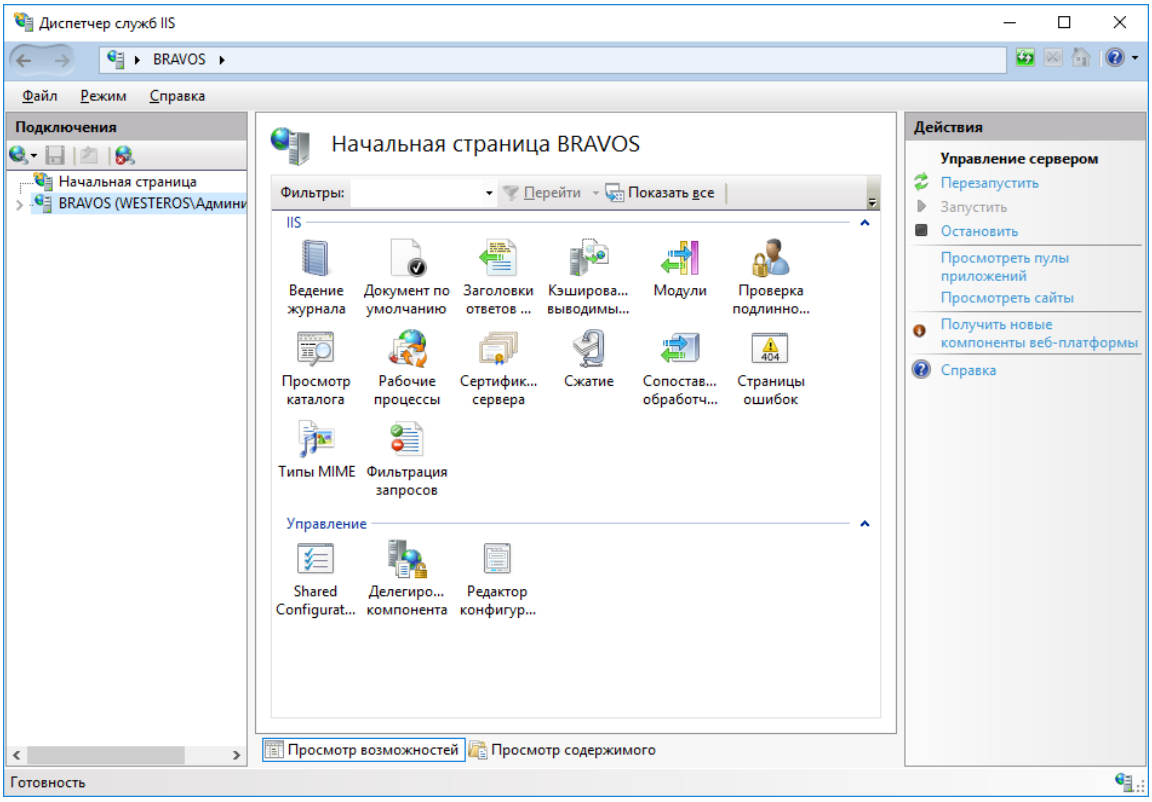

Отметьте **Автоматический перезапуск конечного сервера** и нажмите **Установить.**



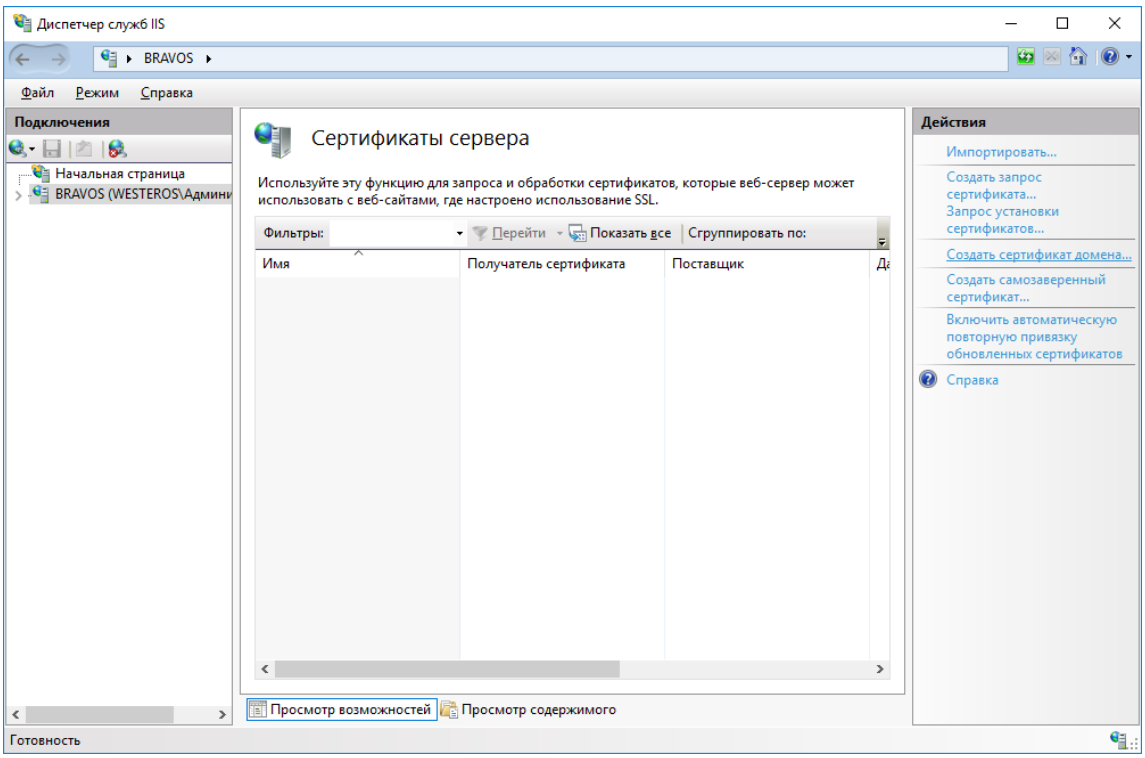

Окно мастера теперь можно закрыть.

# Запрос сертификата для сервера IIS

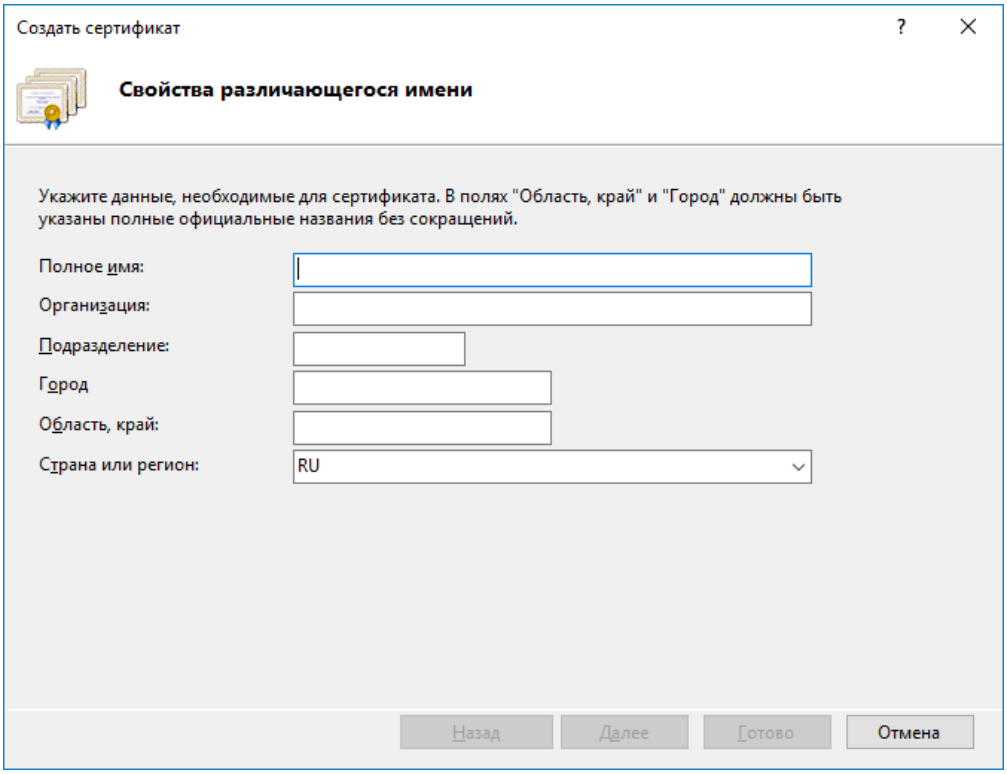
Откройте **диспетчер служб IIS** через **Пуск -> Средства администрирования.** В основном меню, в центре, выберите **Сертификаты сервера.**



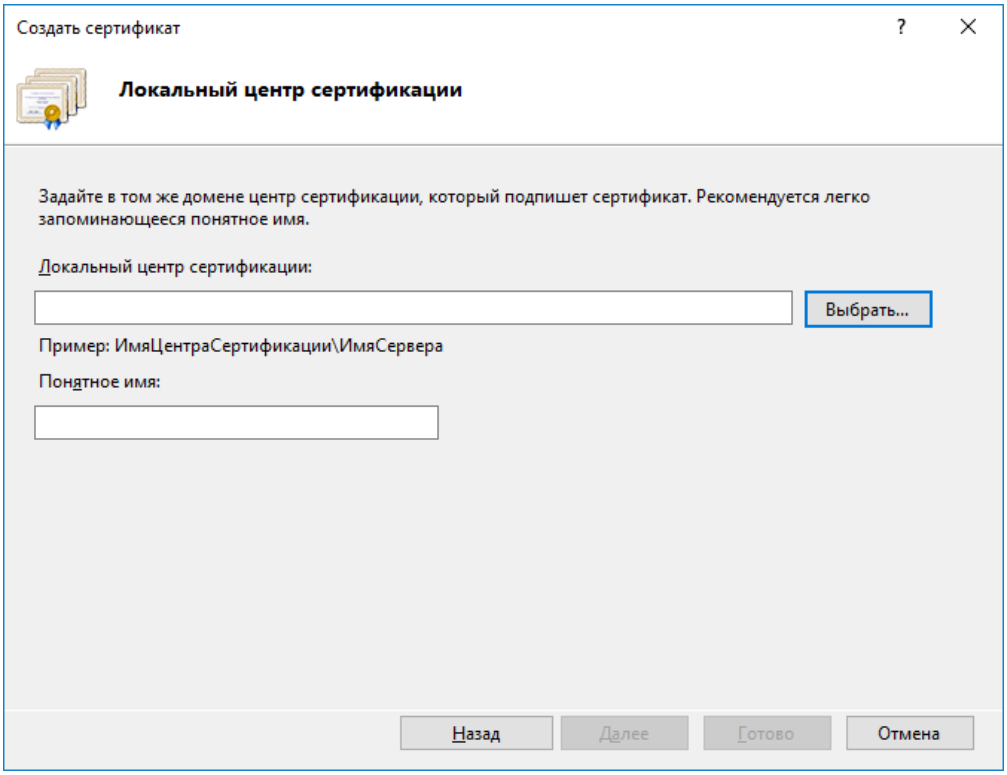

В меню **Действия,** справа выберите **Создать сертификат домена.**



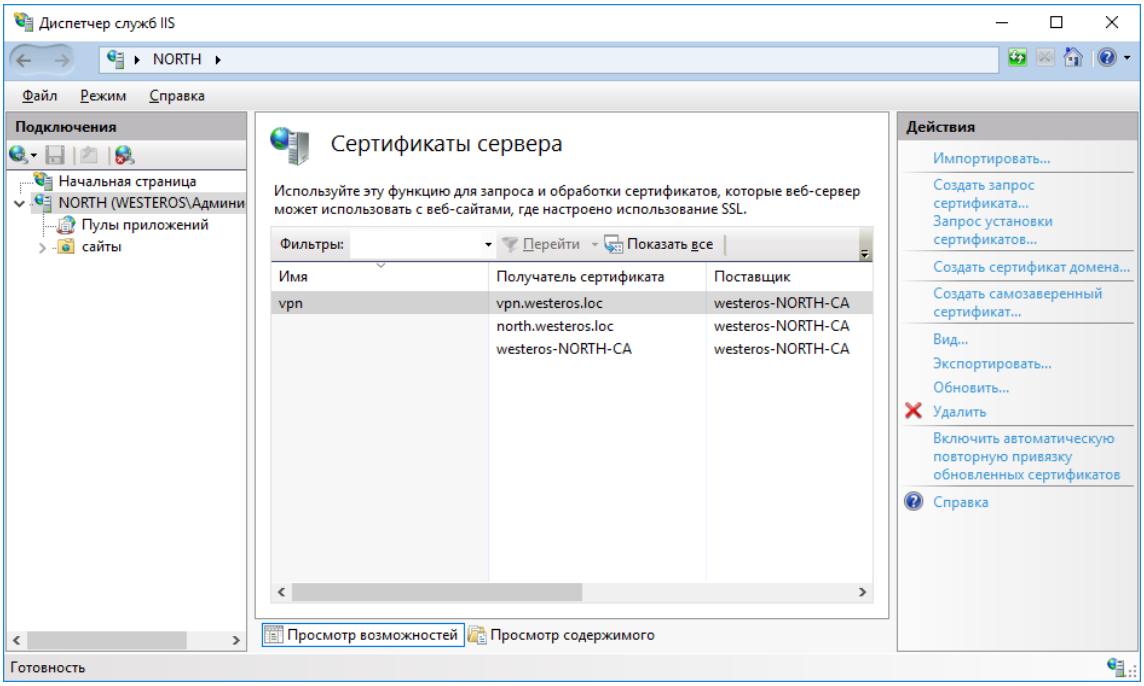

В полном имени укажите имя будущего VPN-соединения и заполните остальные поля так, как это требуется.




В поле **Центр сертификации** нажмите **Выбрать** и укажите центр сертификации. В поле **Понятное имя** укажите короткое имя сертификата, которое будет отображаться в поле **Имя**, в диспетчере IIS. В настоящем примере имя — VPN.



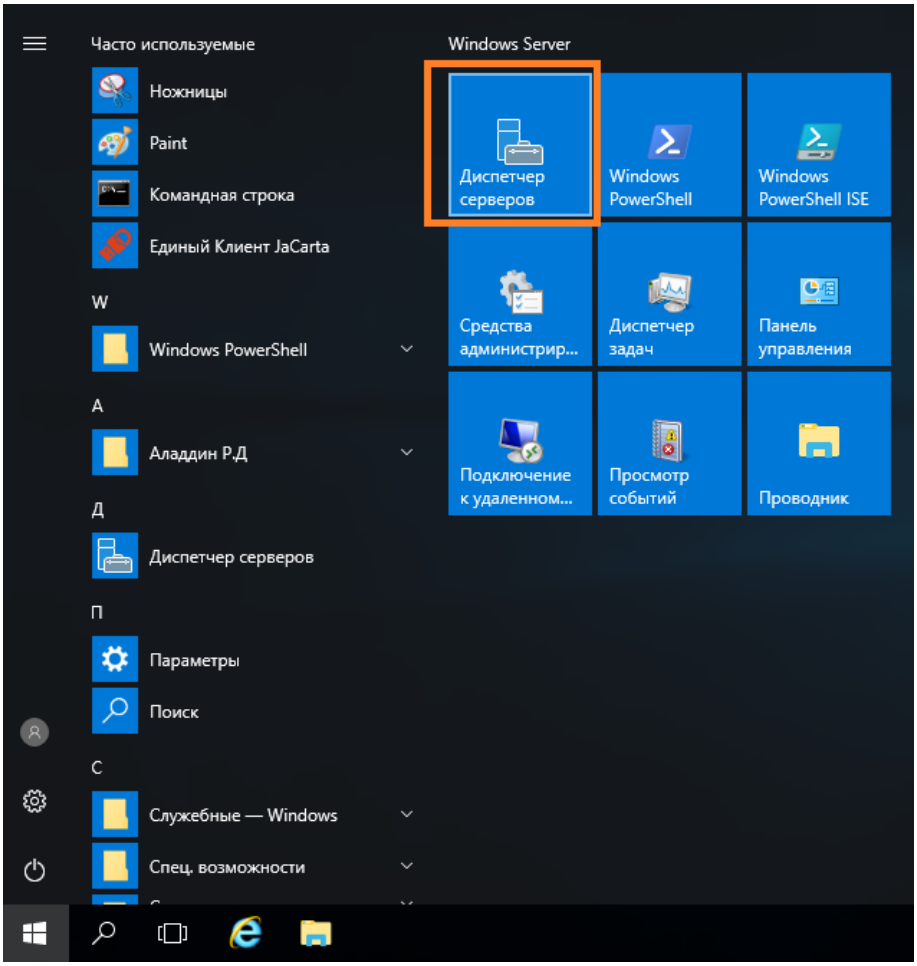

Убедитесь, что сертификат создан.



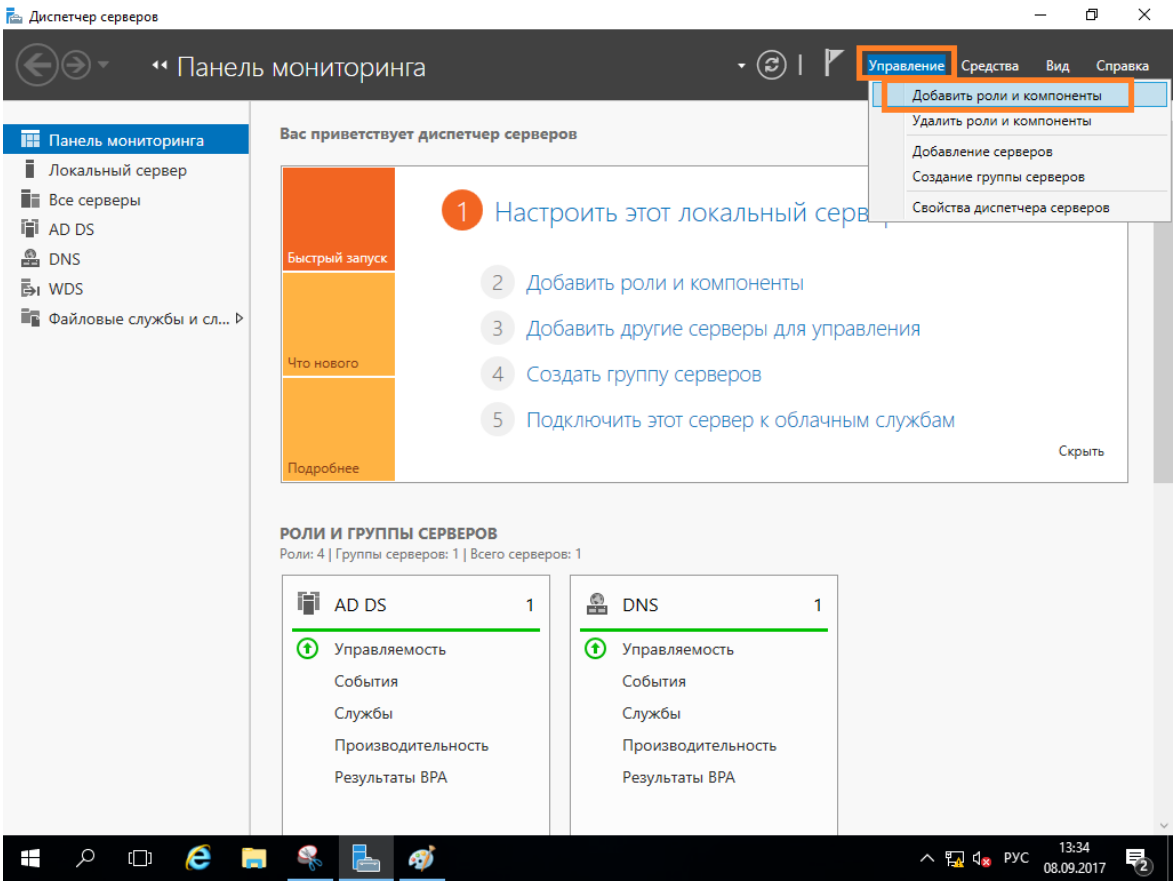

# Установка и настройка компонентов Удалённый доступ и Маршрутизация

## Установка роли удалённый доступ и службы политики сети и доступа

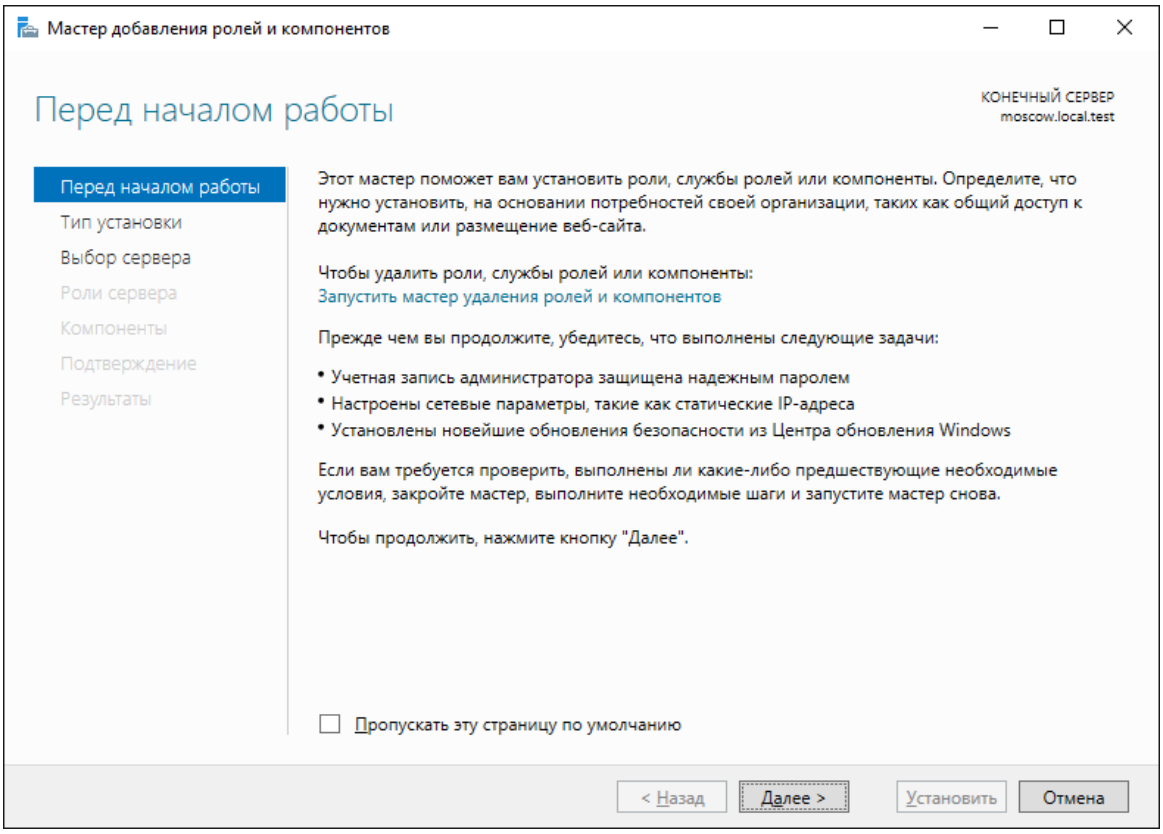
Нажмите **Пуск -> Диспетчер серверов.**


Часто используемые
Ножницы
Paint
Командная строка
Единый Клиент JaCarta
W
Windows PowerShell
A
Аладдин Р.Д
Д
Диспетчер серверов
П
Параметры
Поиск
С
Служебные — Windows
Спец. возможности
Windows Server
Диспетчер серверов
Windows PowerShell
Windows PowerShell ISE
Средства администрир...
Диспетчер задач
Панель управления
Подключение к удаленном...
Просмотр событий
Проводник

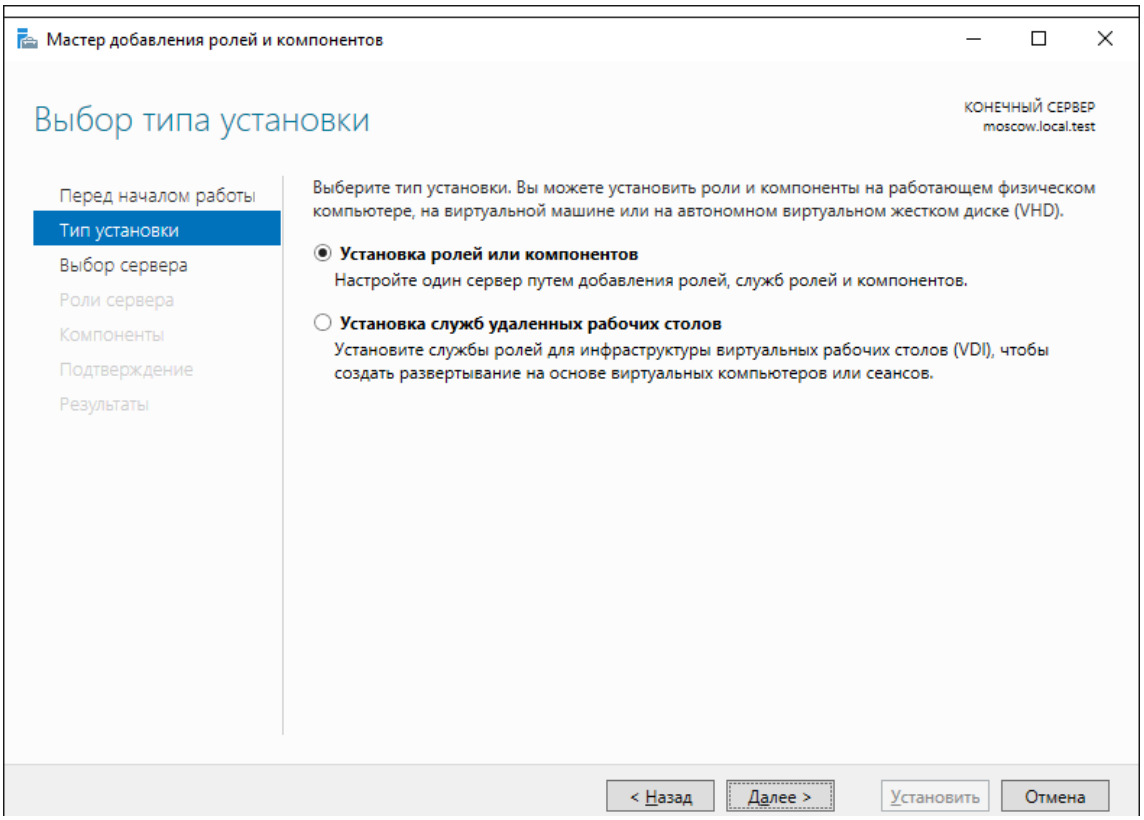
В отобразившемся окне выберите **Управление -> Добавить роли и компоненты.**



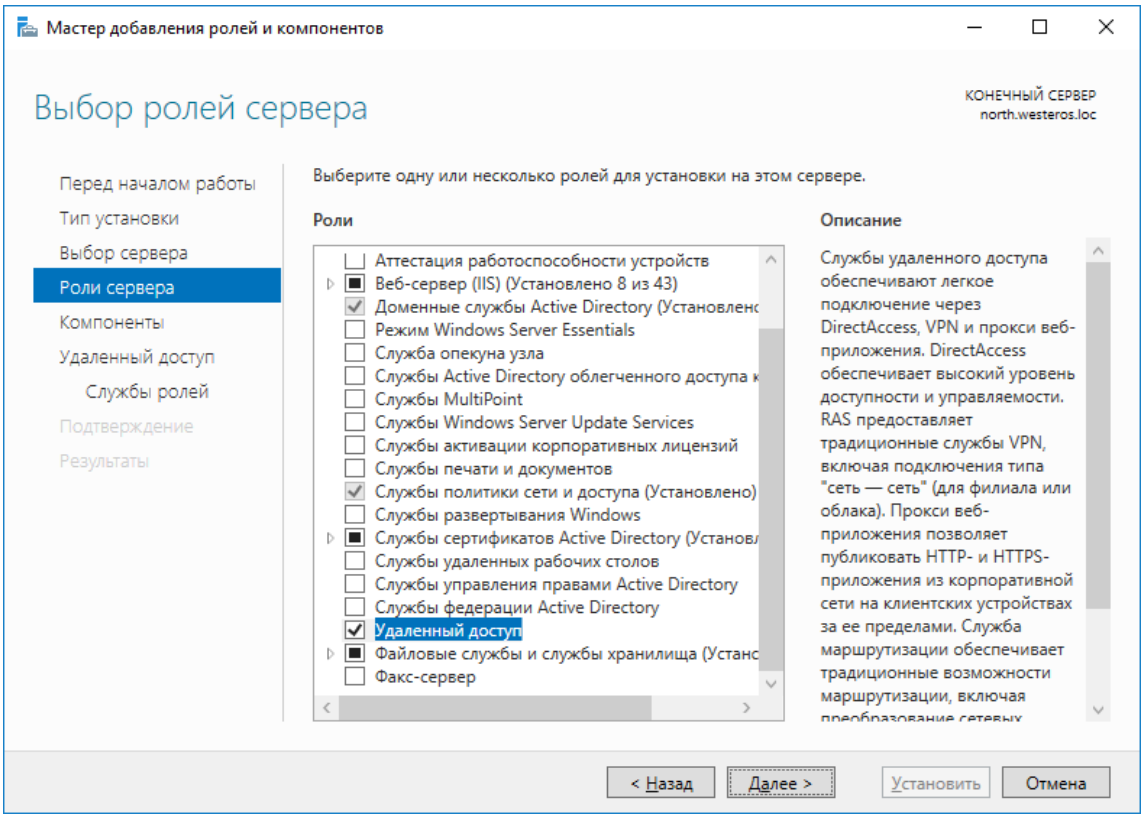
Отобразится окно мастера добавления ролей и компонентов, для продолжения нажмите **Далее.**



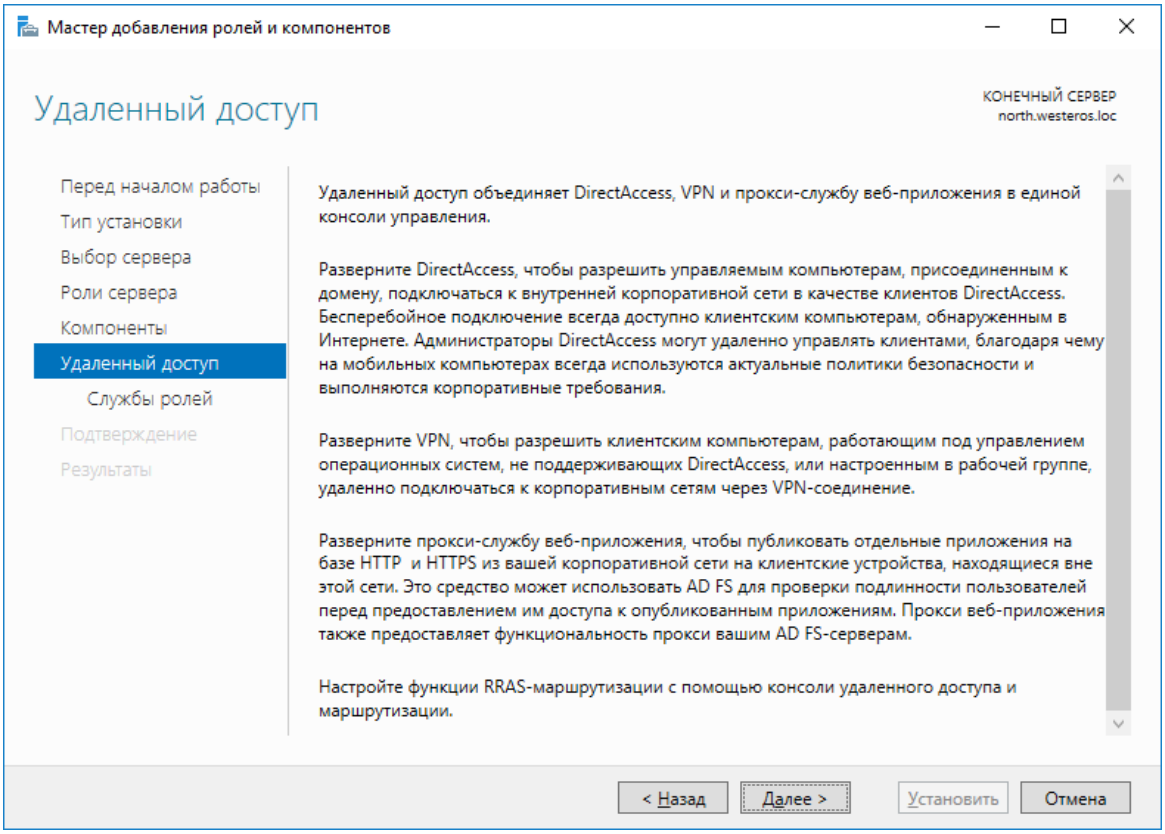
В следующем окне выберите **Установка ролей и компонентов.**



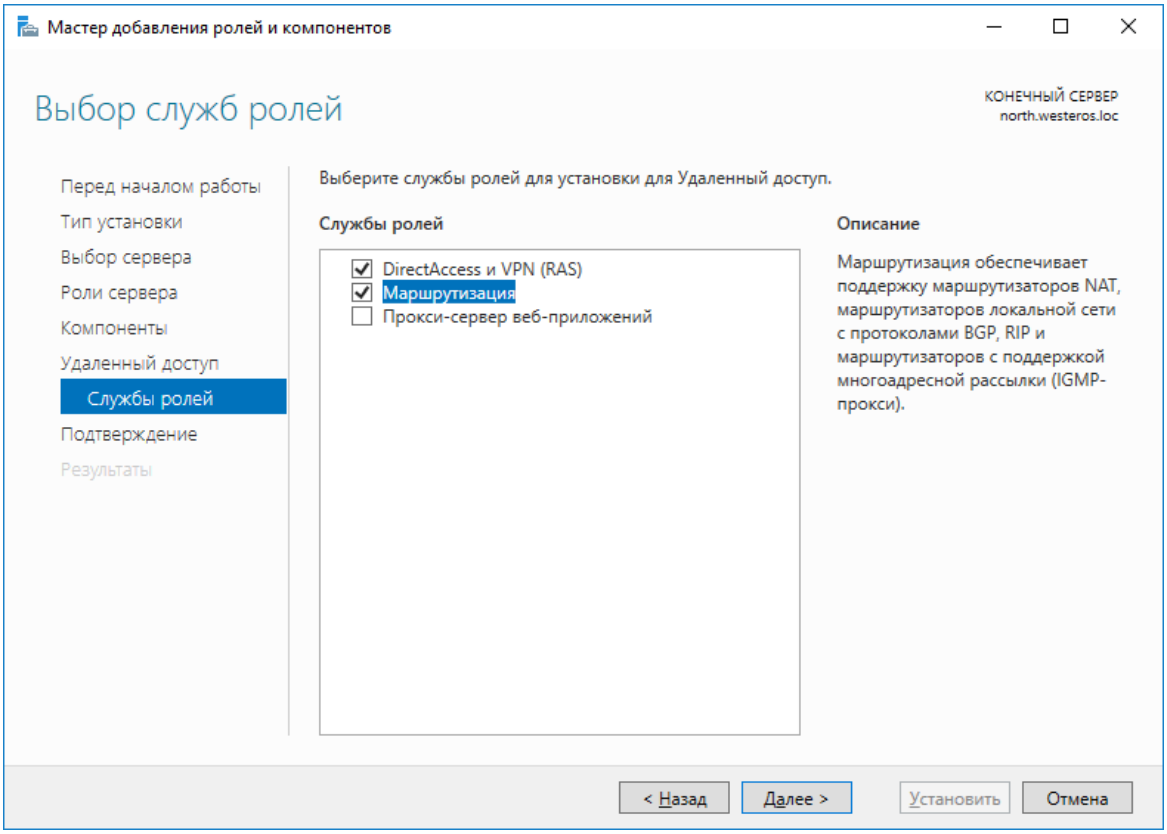

Отобразится окно добавления новых ролей, выберите **Удалённый доступ** и **Службы политики сети и доступа** (если не установлено ранее) и нажмите **Далее.**



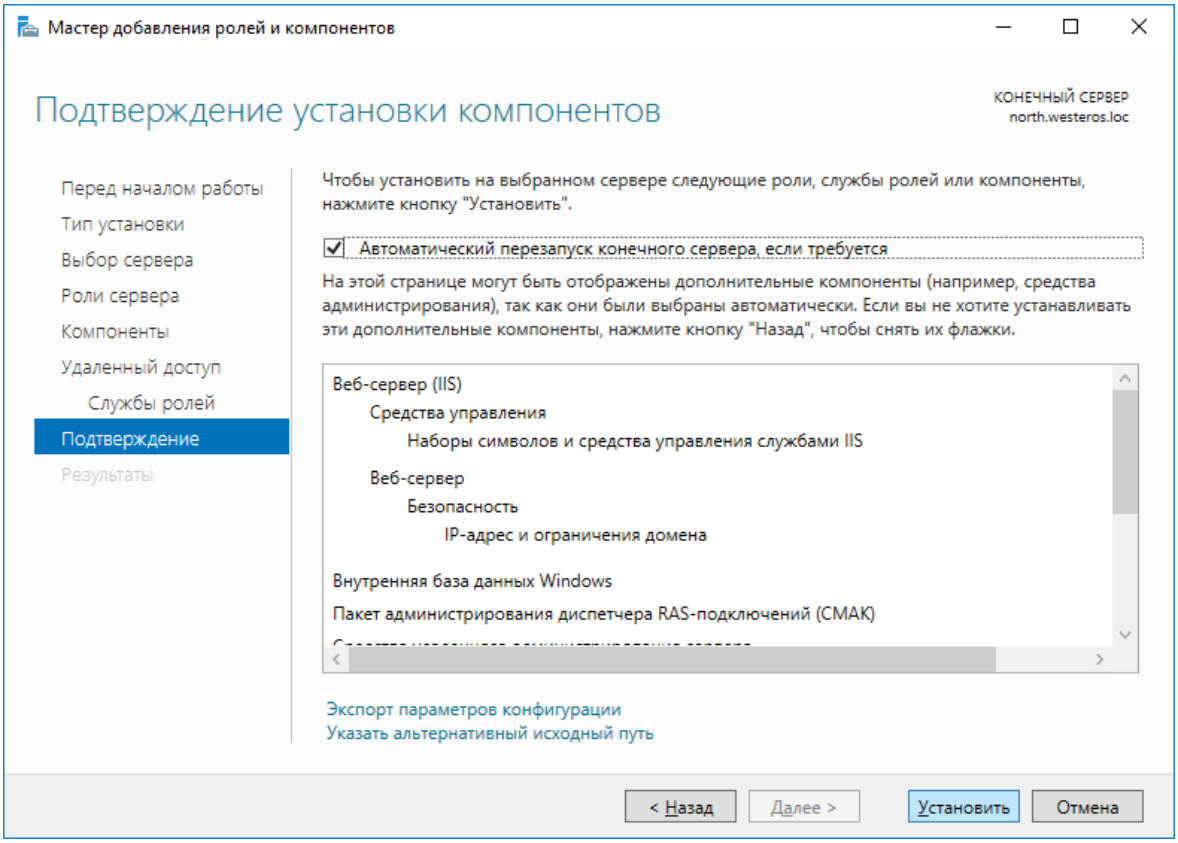

В отобразившемся окне нажмите **Далее.**




В отобразившихся службах ролей выберите **DirectAccess VPN** и **Маршрутизация,** нажмите **Далее.**



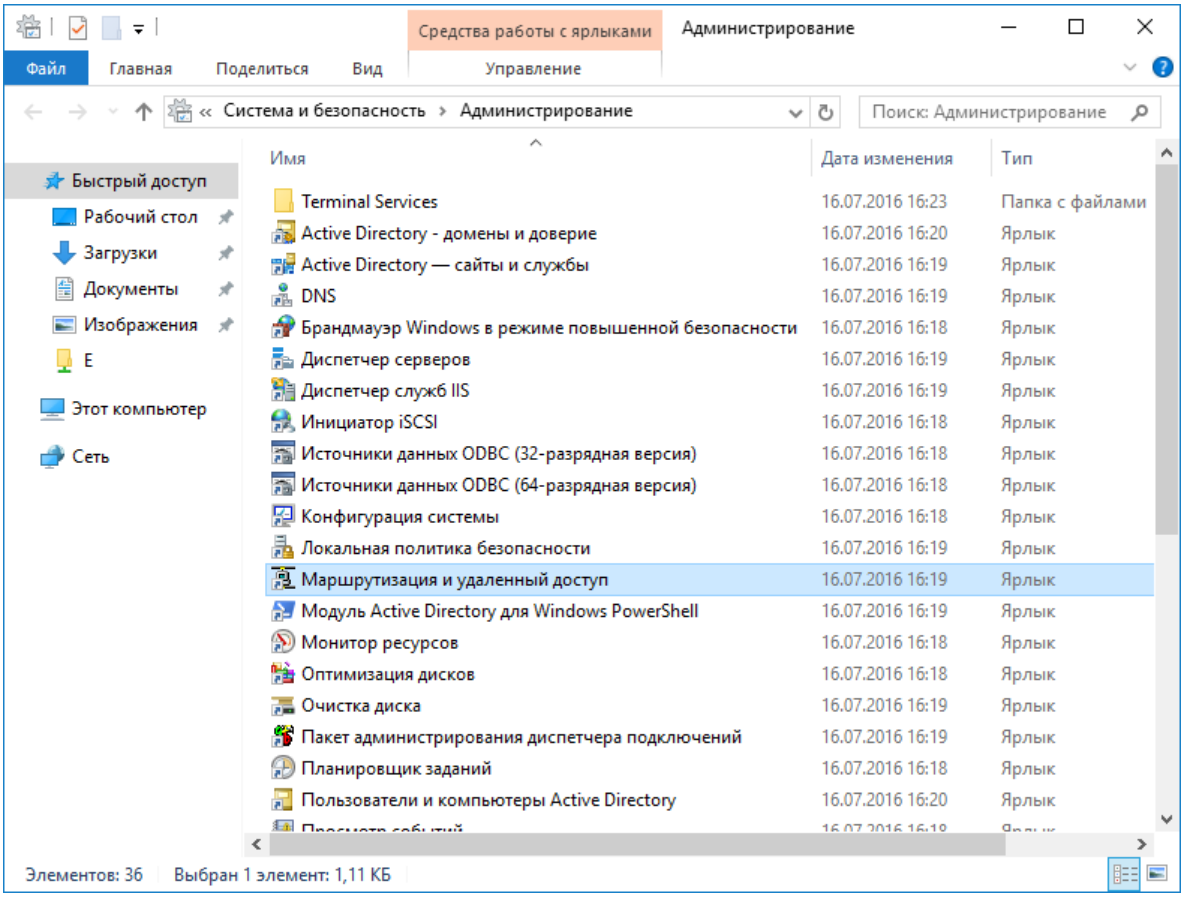

Отметьте **Автоматический перезапуск конечного сервера** и нажмите **Установить.**



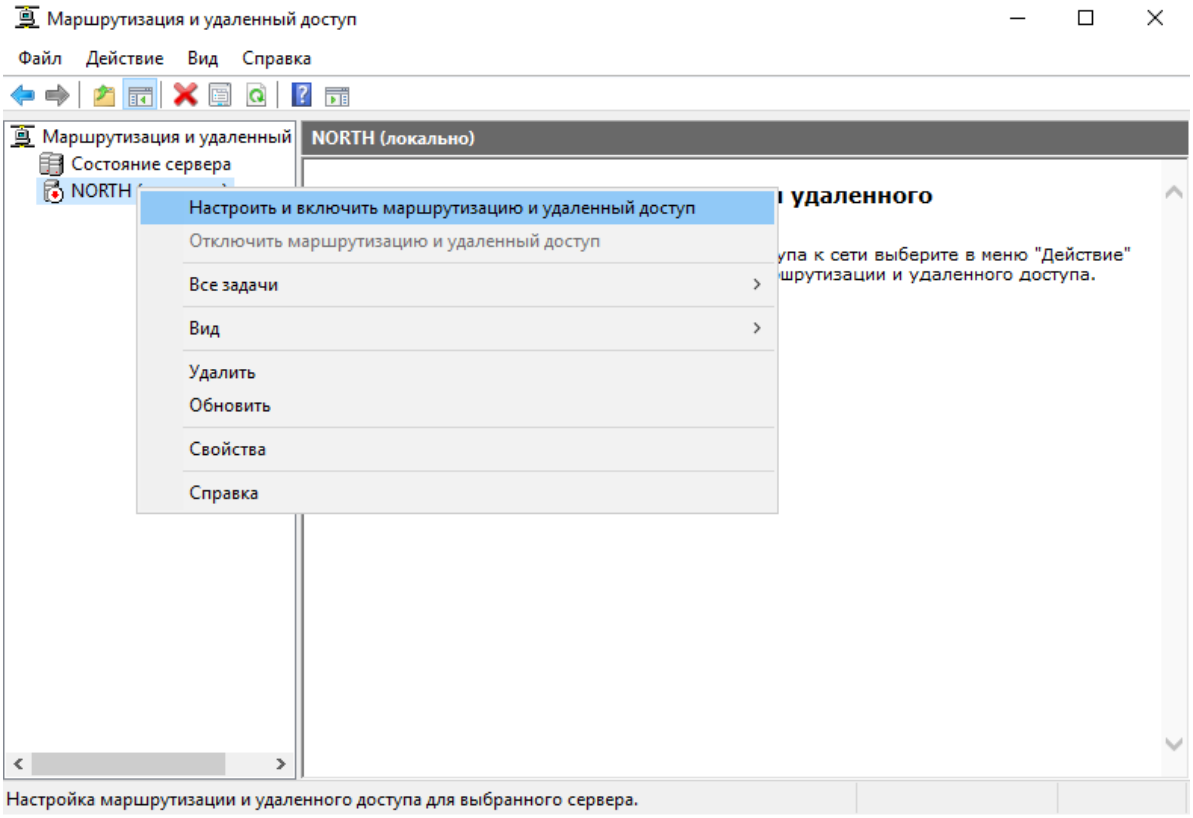

На этом мастер добавления ролей можно закрыть.

# Настройка маршрутизации

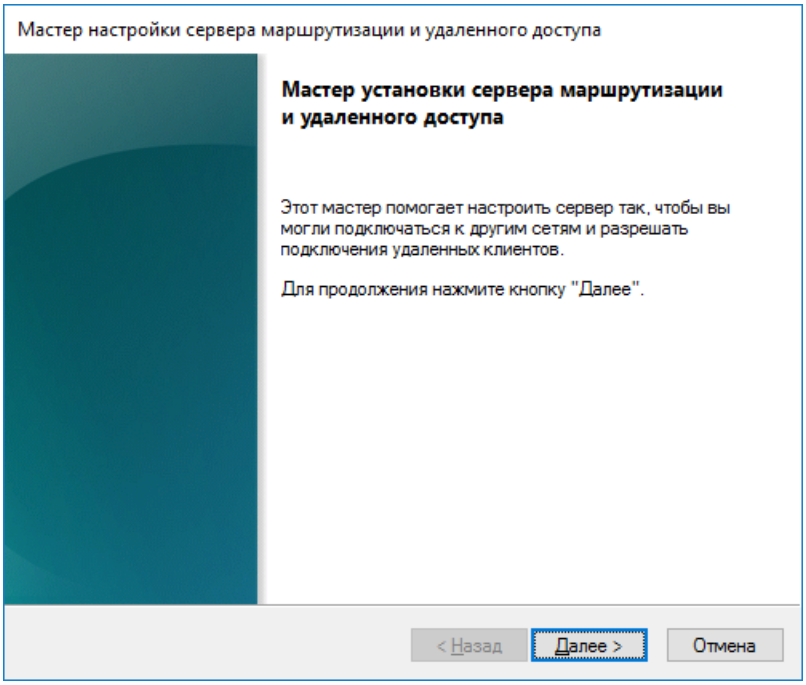
Откройте оснастку **Маршрутизация и удалённый доступ** через **Пуск -> Средства администрирования.**



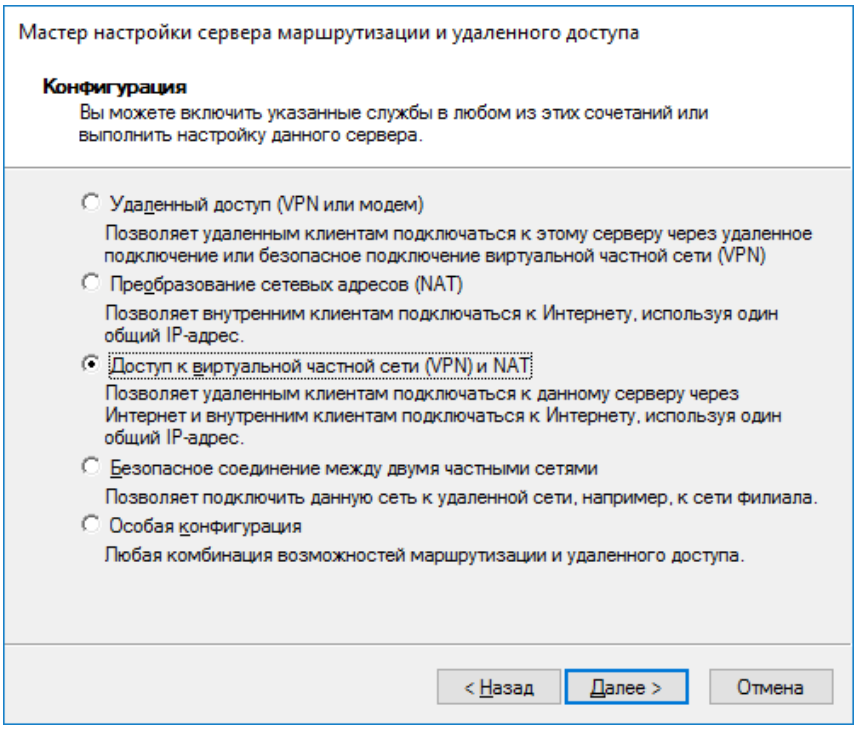

В отобразившейся оснастке в левом меню кликните правой кнопкой нужный сервер и нажмите **Настроить и включить маршрутизацию и удалённый доступ.**




Отобразится мастер установки сервера маршрутизации и удалённого доступа. Нажмите **Далее.**

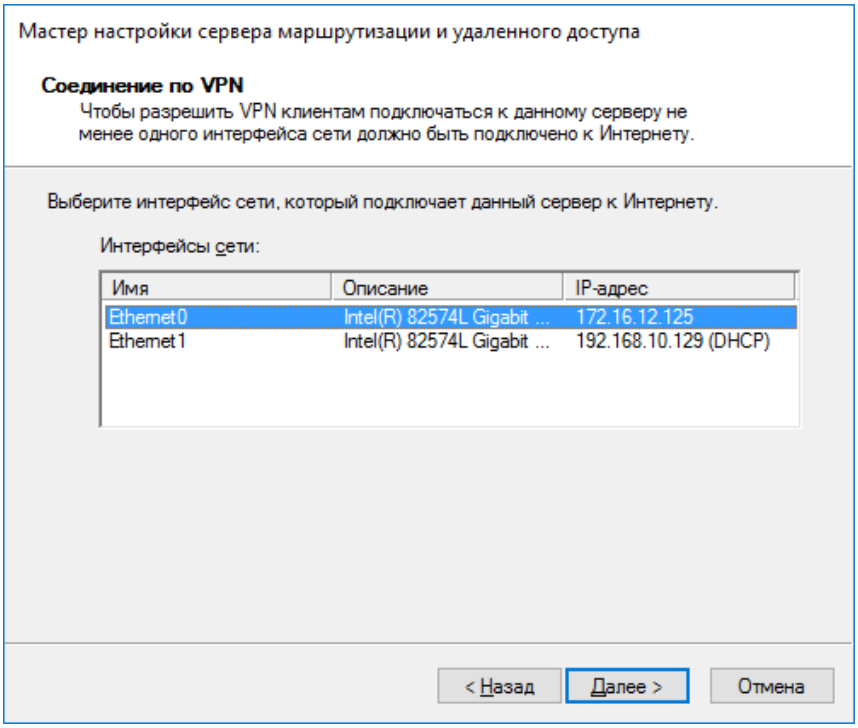



Выберите **Доступ к виртуальной частной сети (VPN) и NAT.**

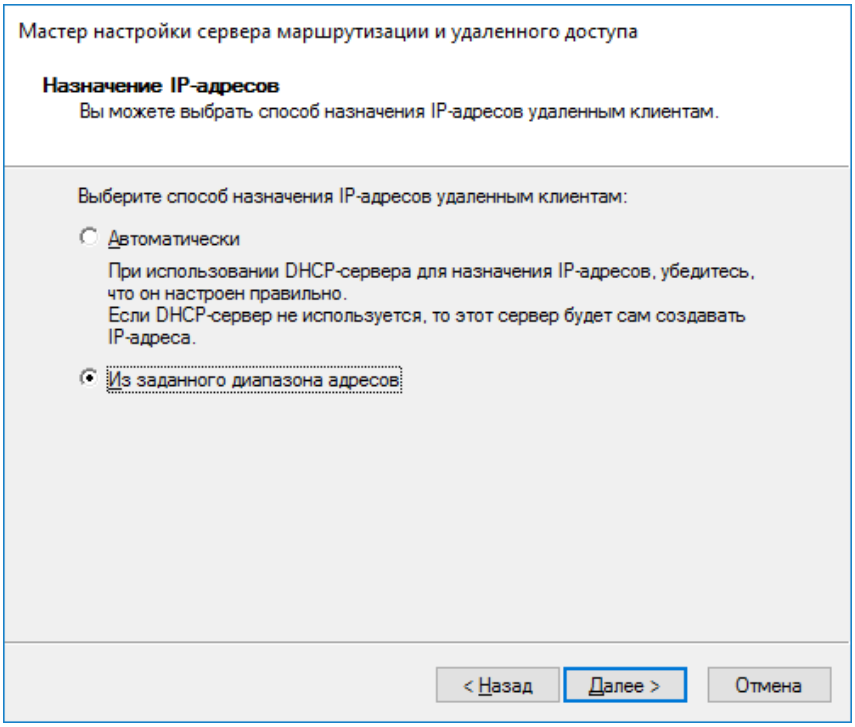



Выберите интерфейс сети, который подключает данный шлюз к сети.

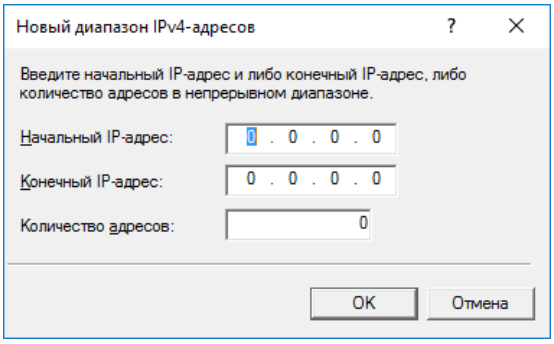
Для реализации VPN на сервере должно быть, как минимум 2 сетевых интерфейса.



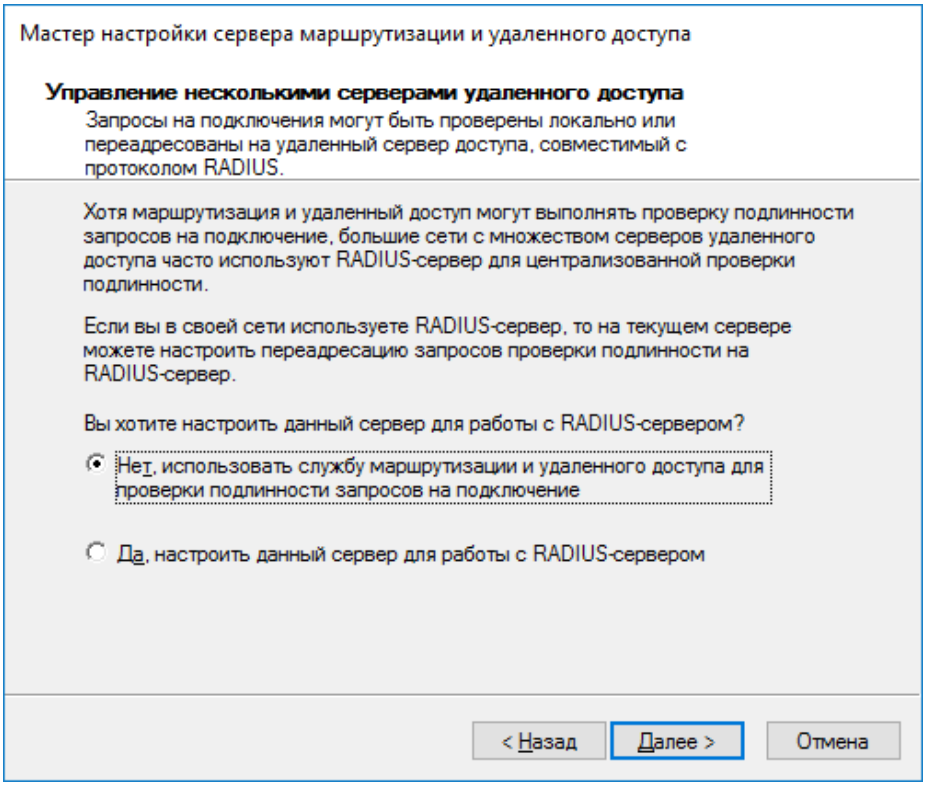

В следующем окне выберите способ назначения IP-адресов — автоматически или из заданного диапазона.



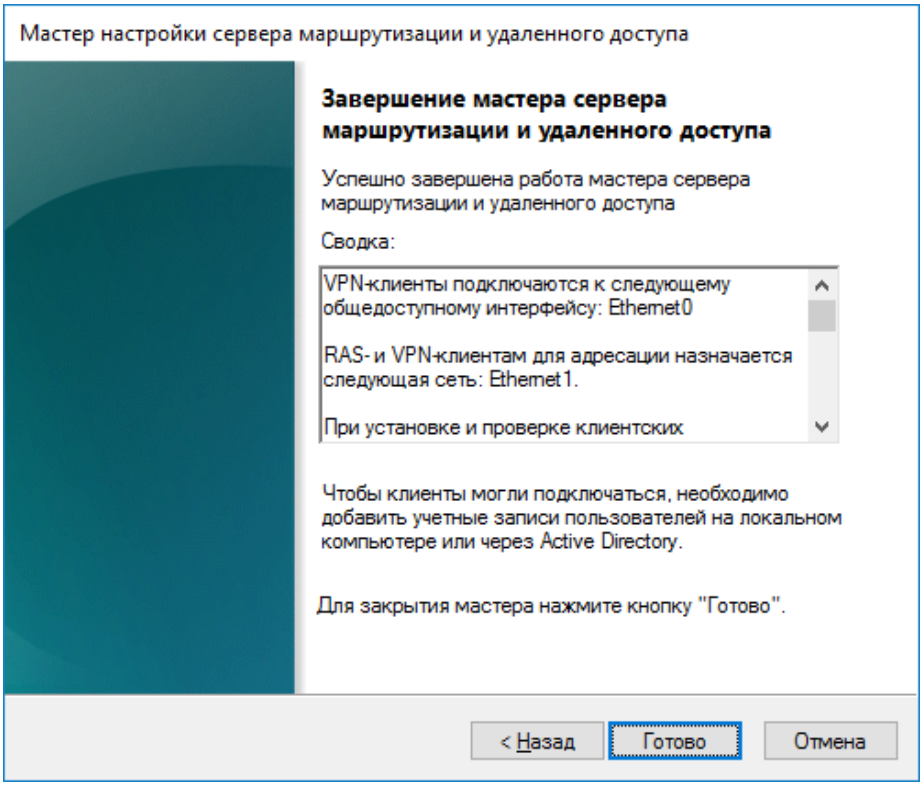

В настоящем примере используется заданный диапазон.



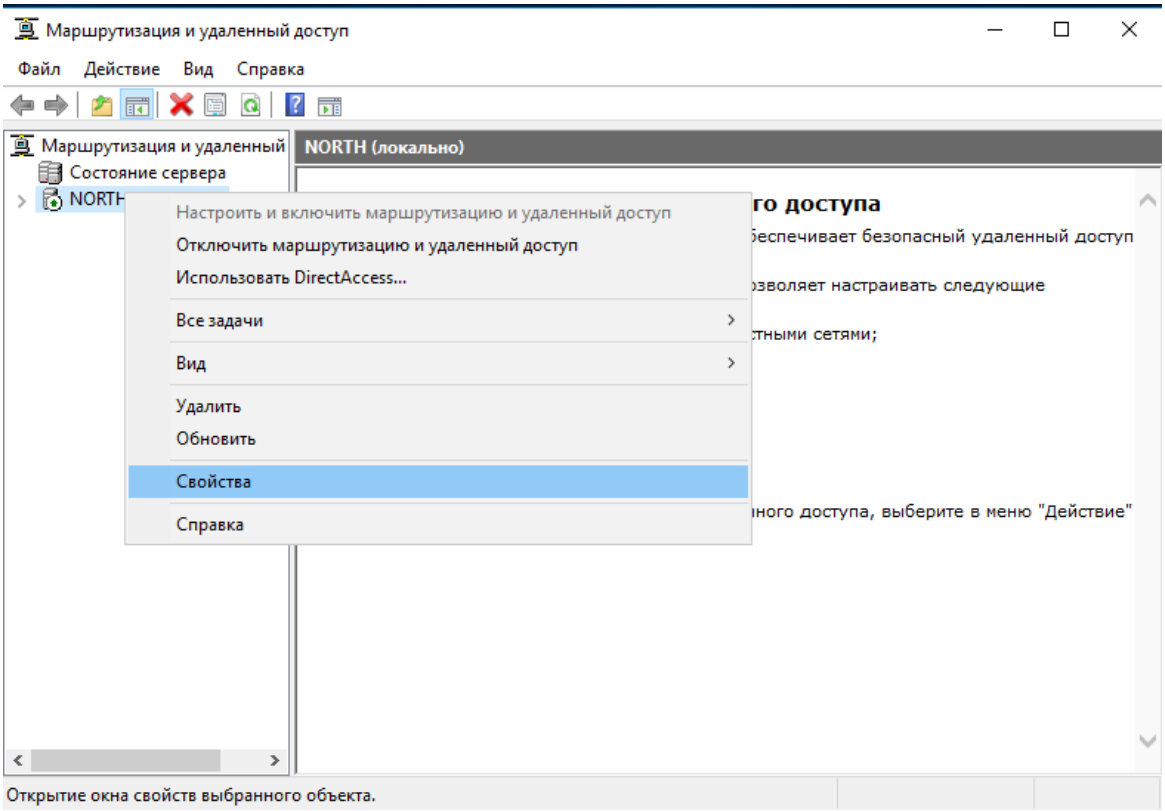

Выберете требуется ли данному серверу работать с RADIUS, в настоящем примере это не требуется, выберите **Нет.**



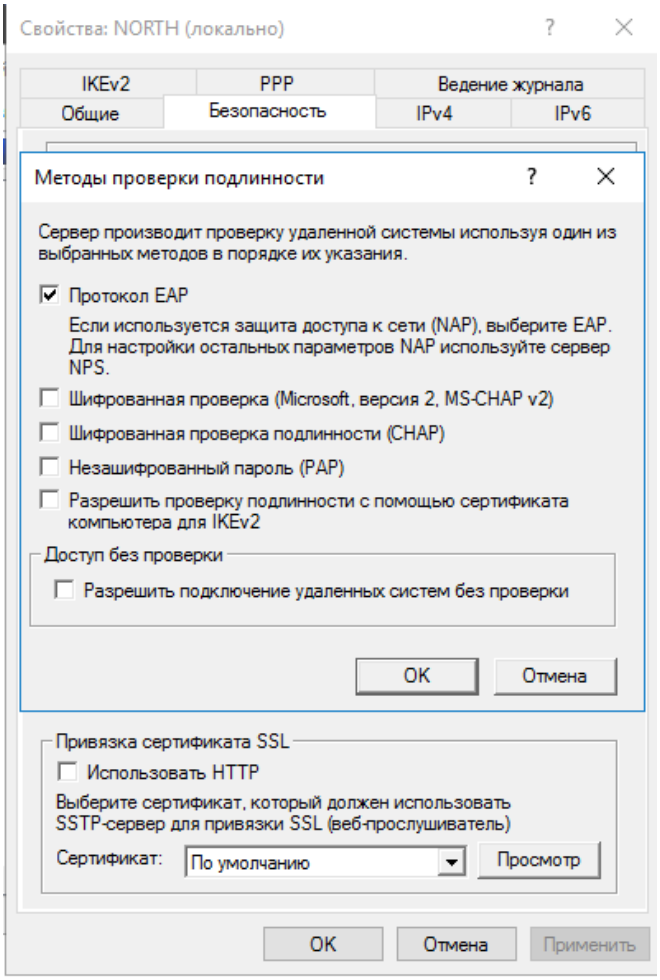

По завершении нажмите **Готово.**



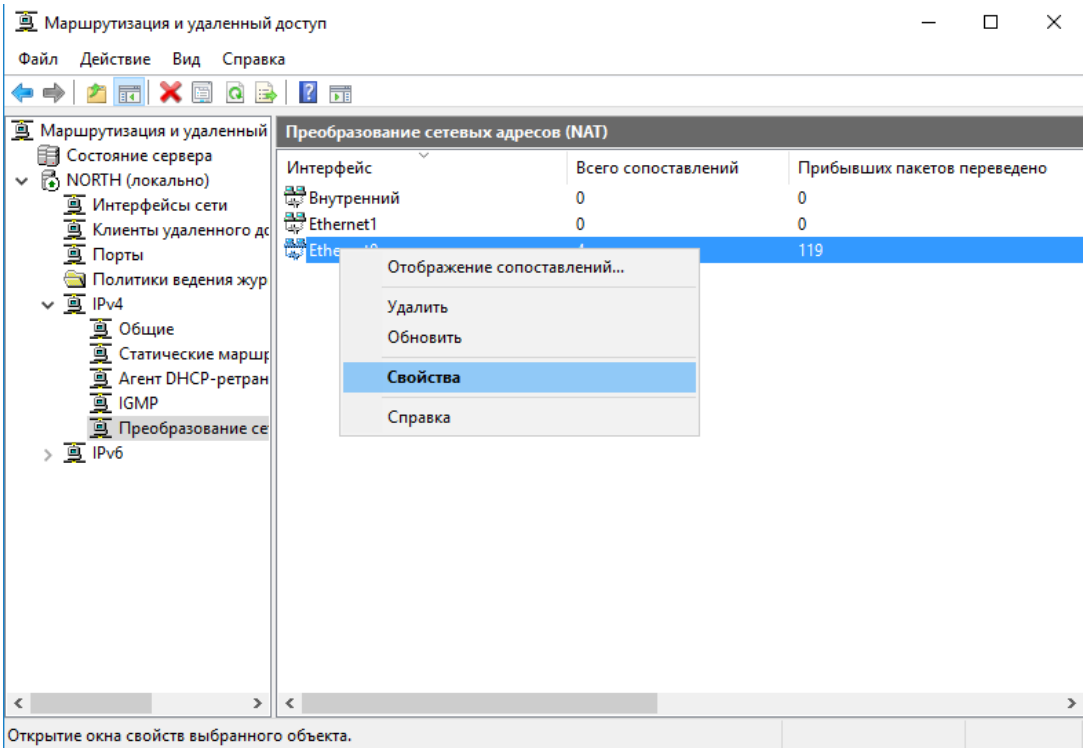

Перейдите в оснастку **Маршрутизация и удалённый доступ,** откройте свойства сервера.



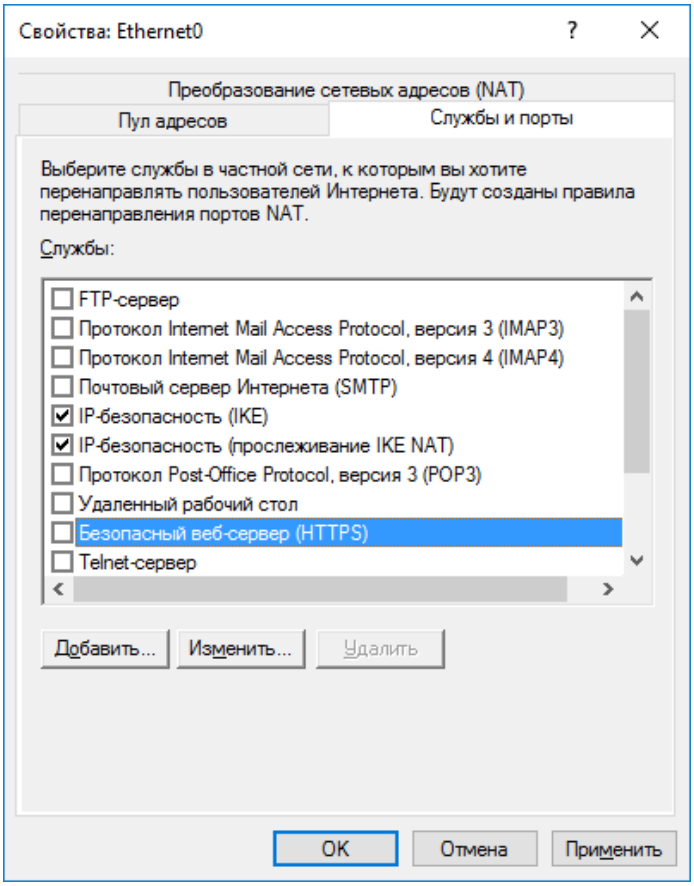

Перейдите во вкладку **Безопасность -> методы проверки подлинности**, отметьте **Протокол EAP,** остальное оставьте пустым. Нажмите **ОК,** нажмите **Применить.**




В оснастке Маршрутизация и удалённый доступ выберите **Сервер-> IPv4 -> Преобразование сетевых адресов (NAT).** В отобразившемся окне откройте свойства сетевого интерфейса, который ранее указывался в мастере настройки маршрутизации.



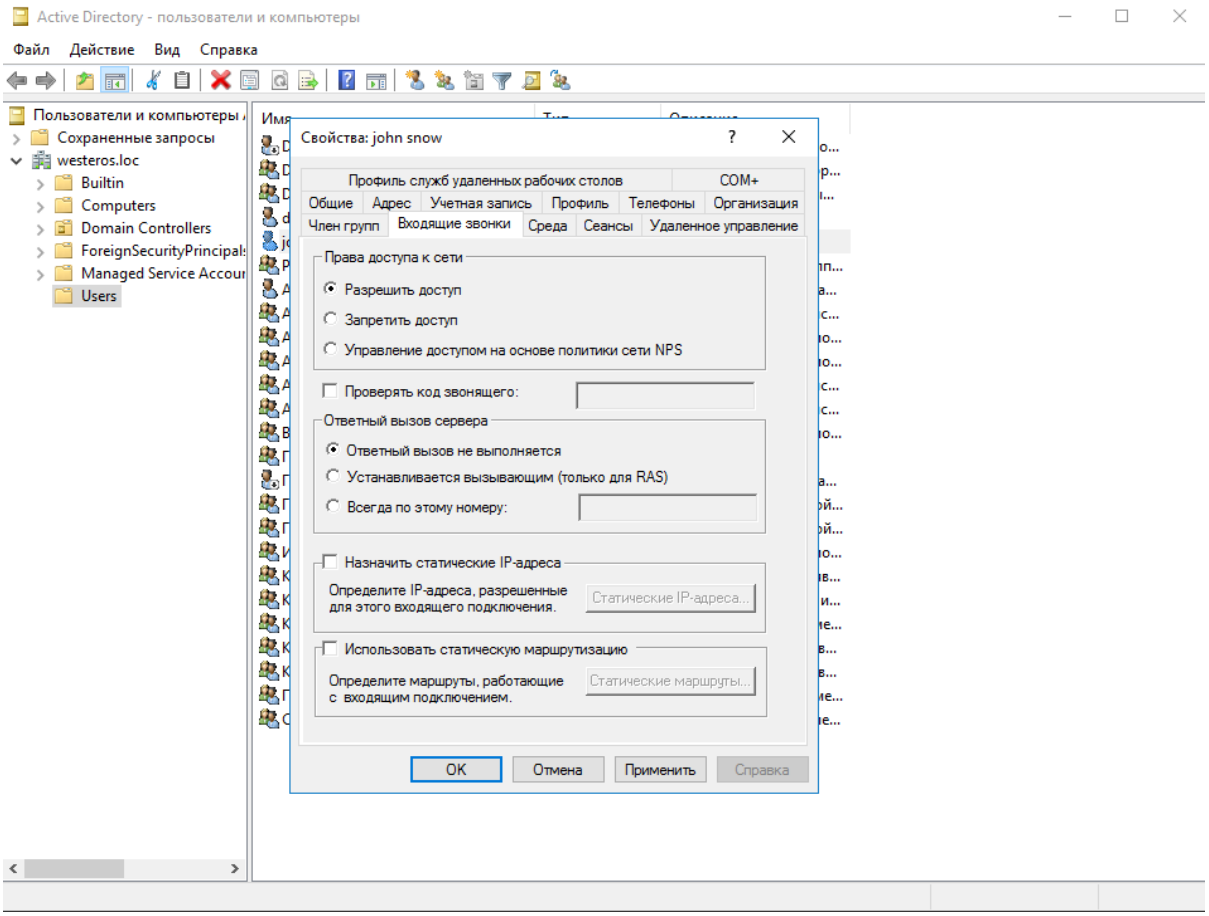
В отобразившемся окне перейдите во вкладку **Службы и порты**, отметьте **Безопасный веб-сервер(HTTPS),** нажмите **Применить,** затем **ОК.**




# Назначение пользователю прав на использование VPN-подключения

Подключаться к сети через VPN-соединения могут только те пользователи, учётные записи которых настроены для таких подключений. Для назначения пользователю таких прав выполните следующие действия.

Откройте оснастку Active Directory — Пользователи и компьютеры. Откройте свойства пользователя которому необходимо назначить права на VPN-соединения. Во вкладке **Входящие звонки** выберите **Разрешить доступ,** нажмите **Применить,** затем **ОК.**


Active Directory - пользователи и компьютеры
Файл Действие Вид Справка
Пользователи и компьютеры
Сохраненные запросы
westeros.loc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Свойства: john snow
Профиль служб удаленных рабочих столов
COM+
Общие Адрес Учетная запись Профиль Телефоны Организация
Член групп Входящие звонки Среда Сеансы Удаленное управление
Права доступа к сети
Разрешить доступ
Запретить доступ
Управление доступом на основе политики сети NPS
Проверять код звонящего:
Ответный вызов сервера
Ответный вызов не выполняется
Устанавливается вызывающим (только для RAS)
Всегда по этому номеру:
Назначить статические IP-адреса
Определите IP-адреса, разрешенные для этого входящего подключения.
Статические IP-адреса...
Использовать статическую маршрутизацию
Определите маршруты, работающие с входящим подключением.
Статические маршруты...
OK
Отмена
Применить
Справка

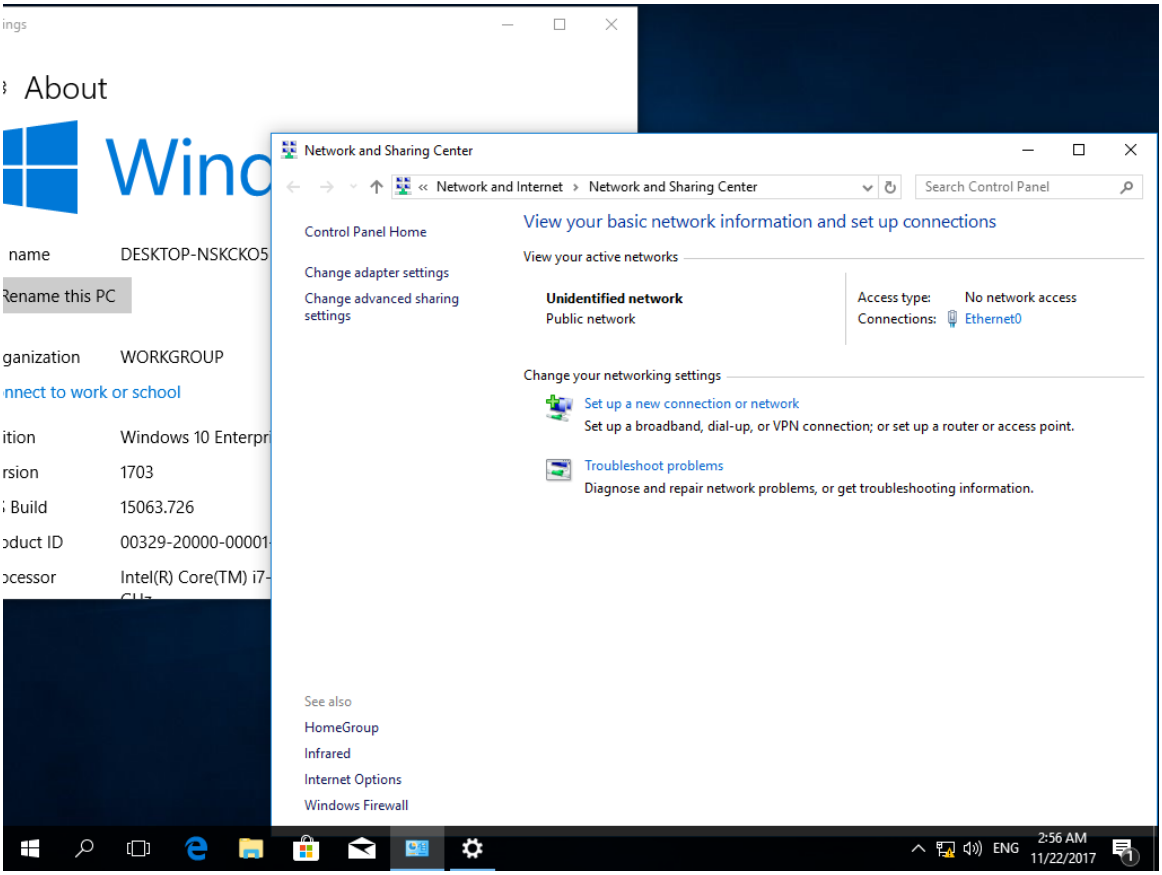
# Проверка работоспособности

Для того чтобы подключаться к сети через VPN-соединение, необходимо настроить соответствующее подключение на рабочей станции и осуществить это подключение с использованием электронного ключа JaCarta.

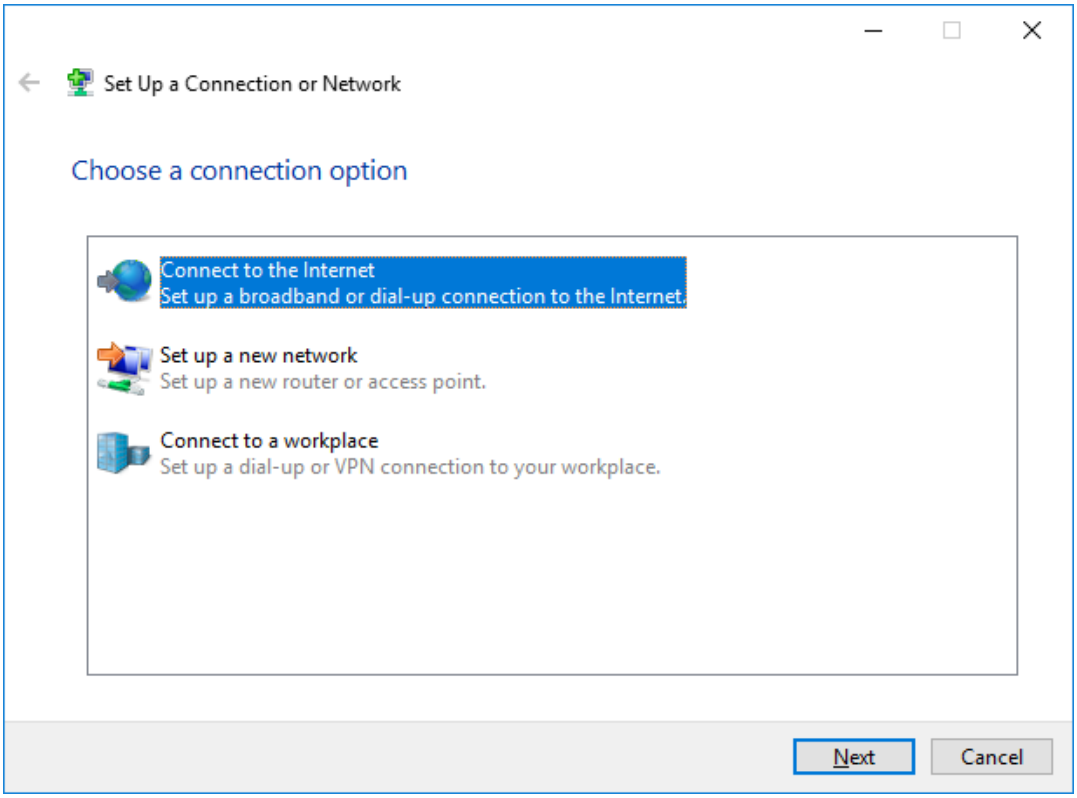
## Создание подключения

Перейдите на клиентскую рабочую станцию.

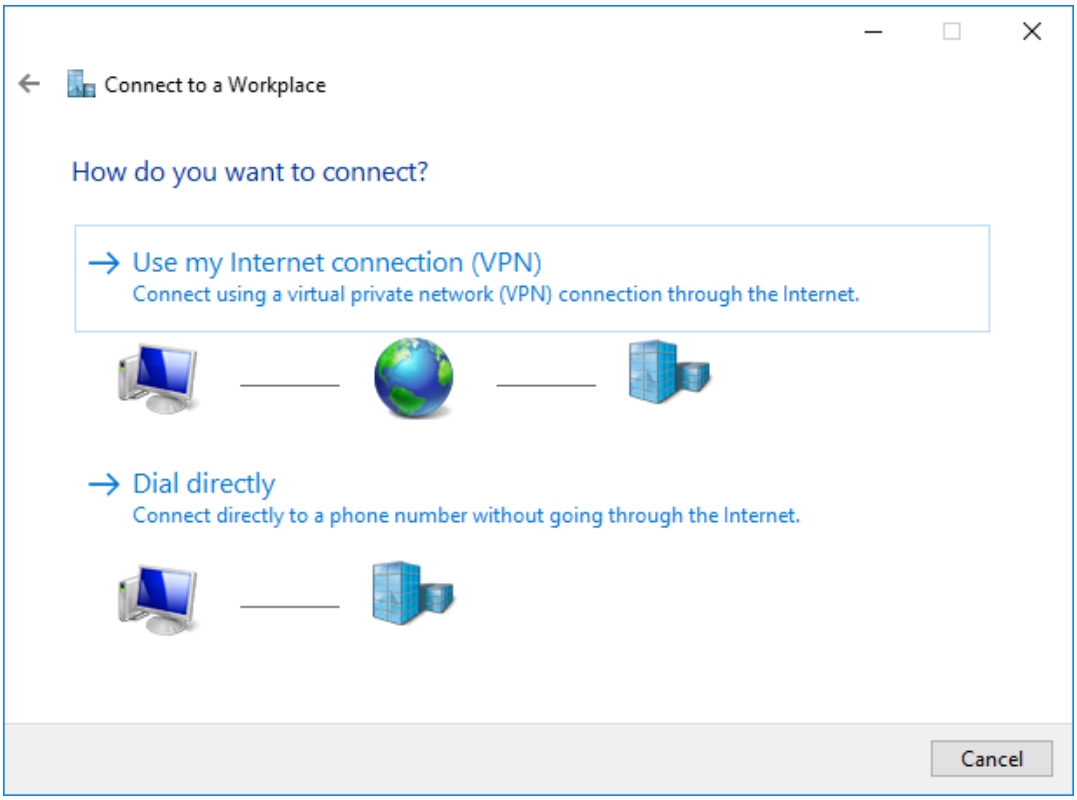
Откройте **Центр управления сетями и общим доступом,** выберите **Создание и настройка нового подключения к сети.**



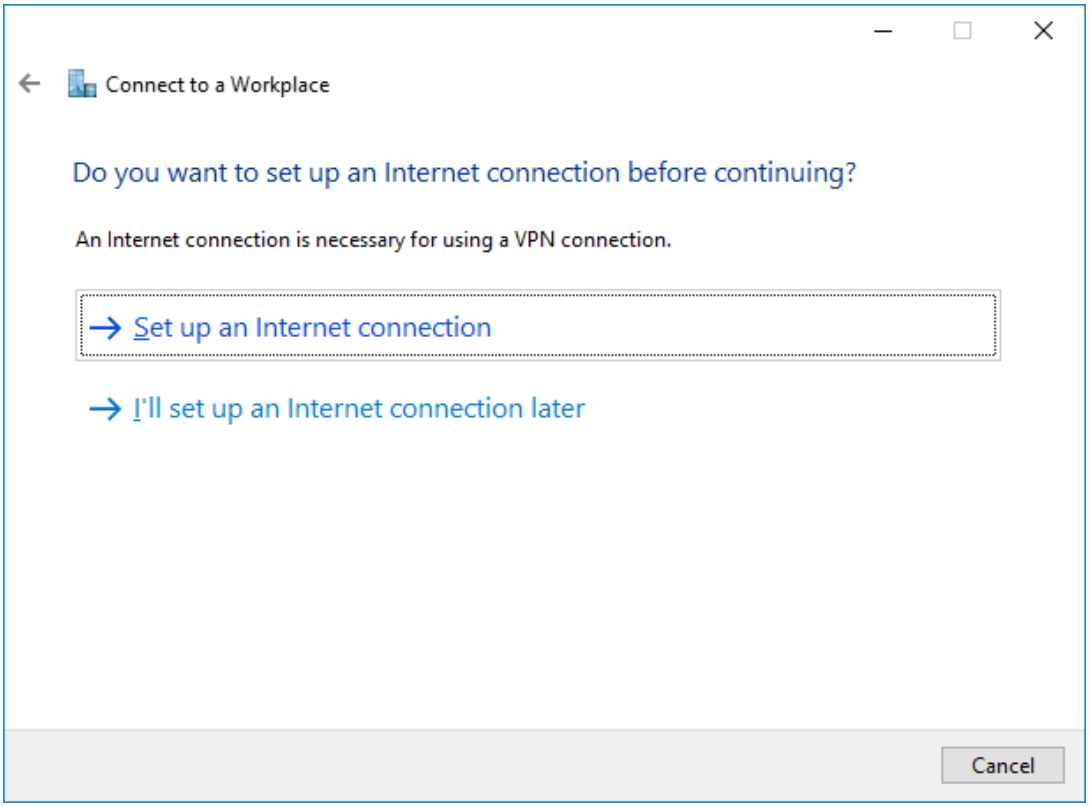

В отобразившемся окне выберите **Подключение к рабочему месту.**




Выберите **Использовать моё подключение к Интернету (VPN).**

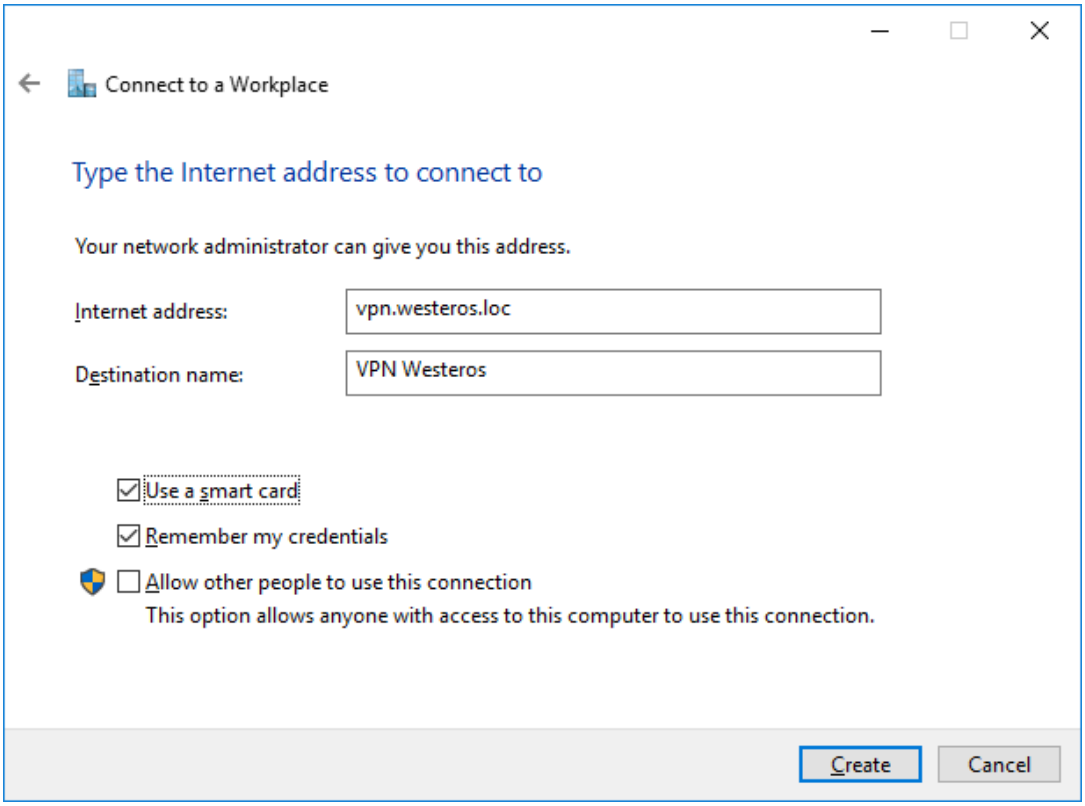



Отобразится следующее окно, выберите **Настроить.**



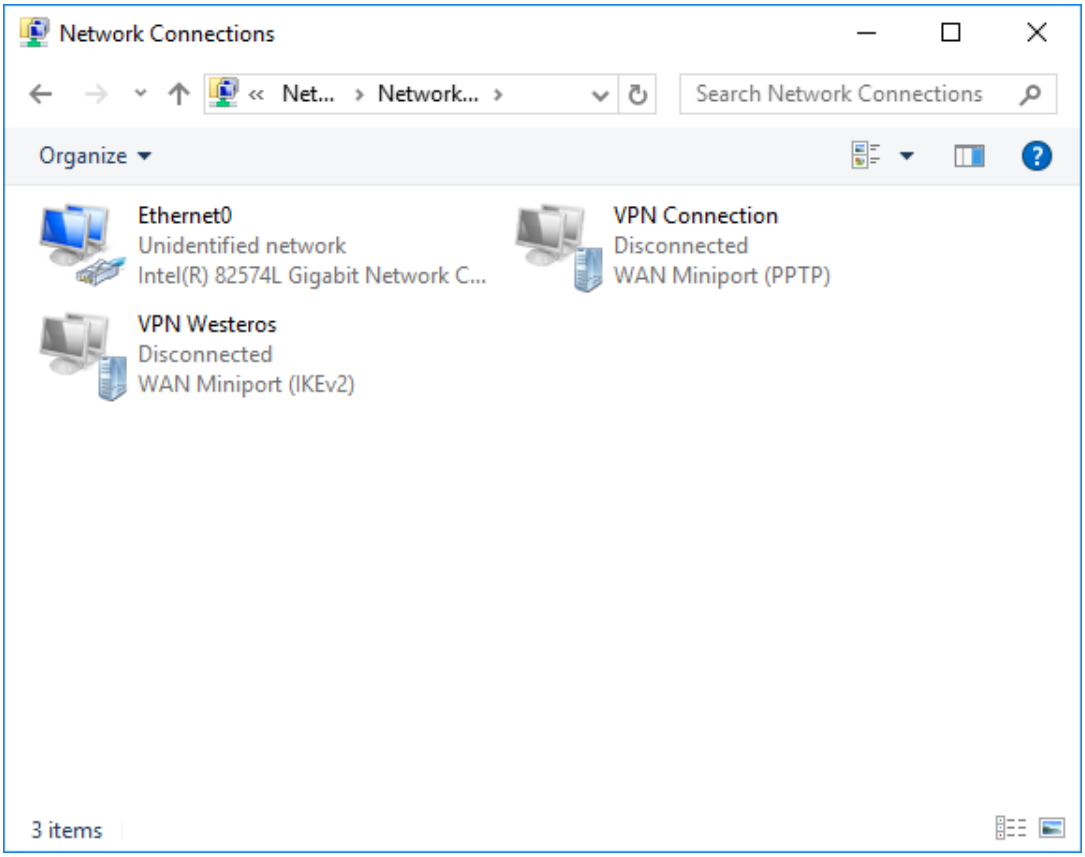

В следующем окне укажите **адрес, имя подключения.** Отметьте пункт **использовать смарт-карту.**

Нажмите **Создать.**

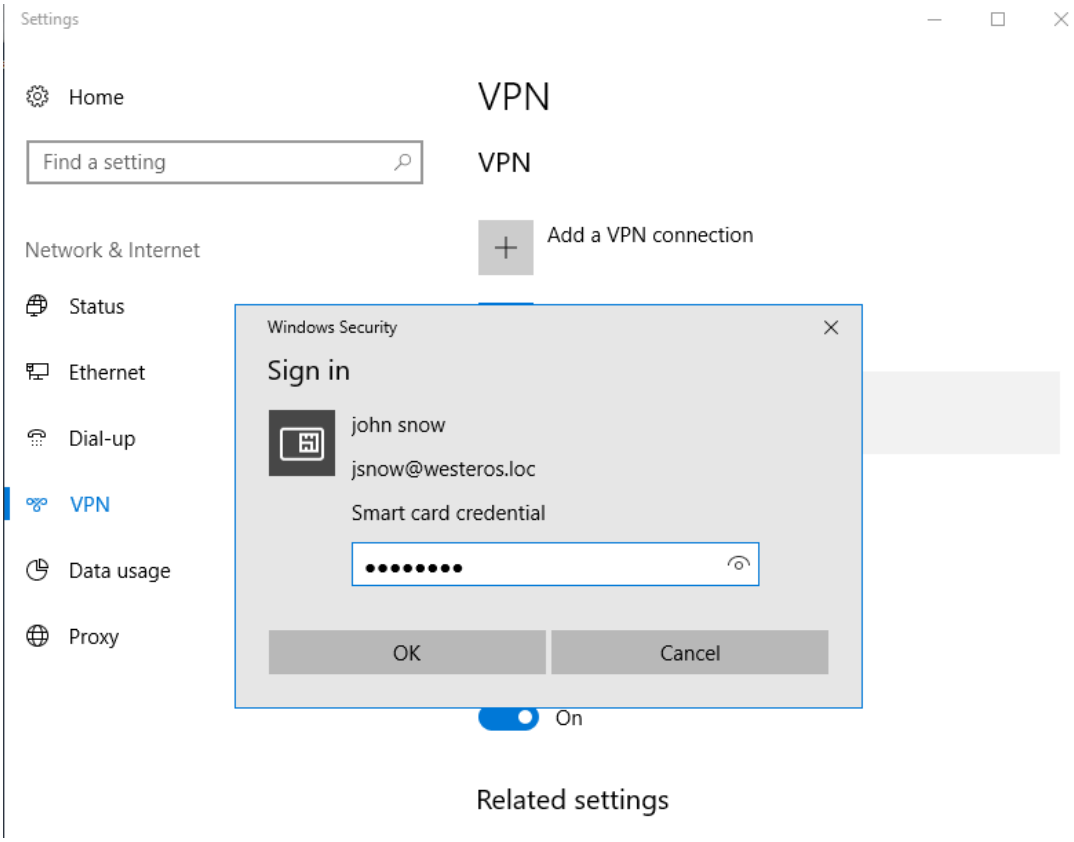



# Подключение к шлюзу

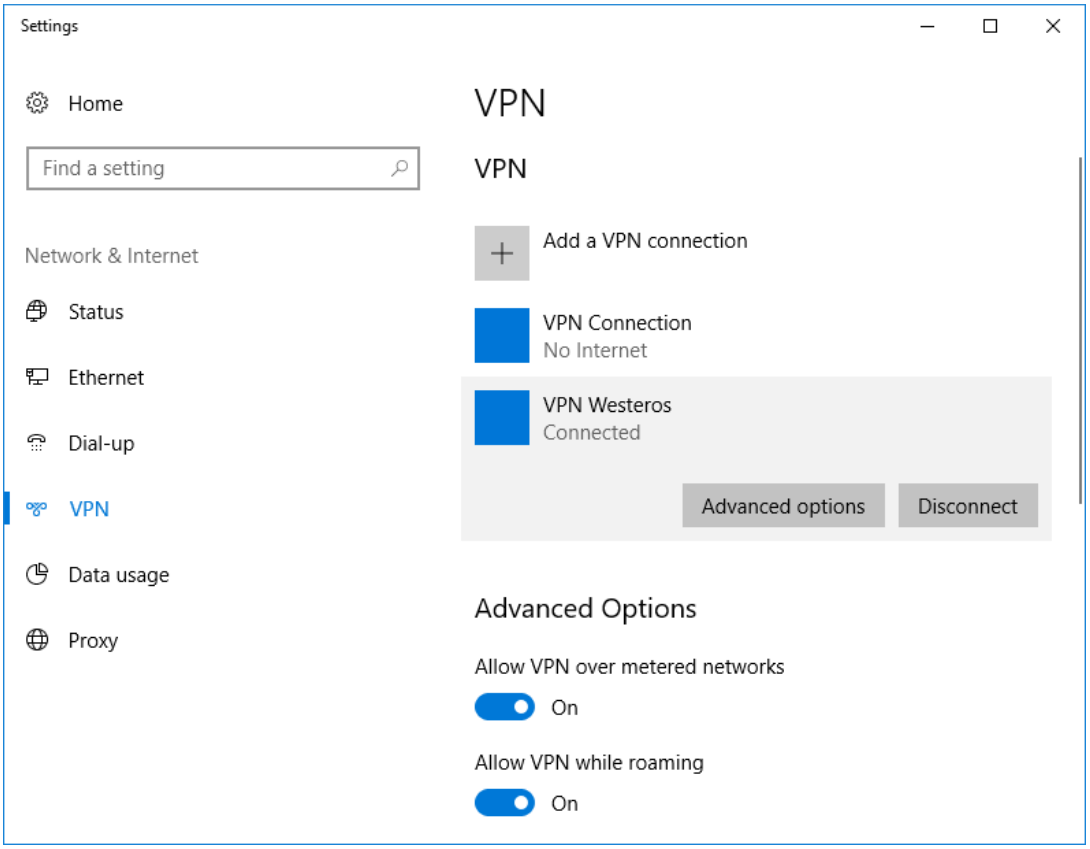
Щёлкните вновь созданное соединение.



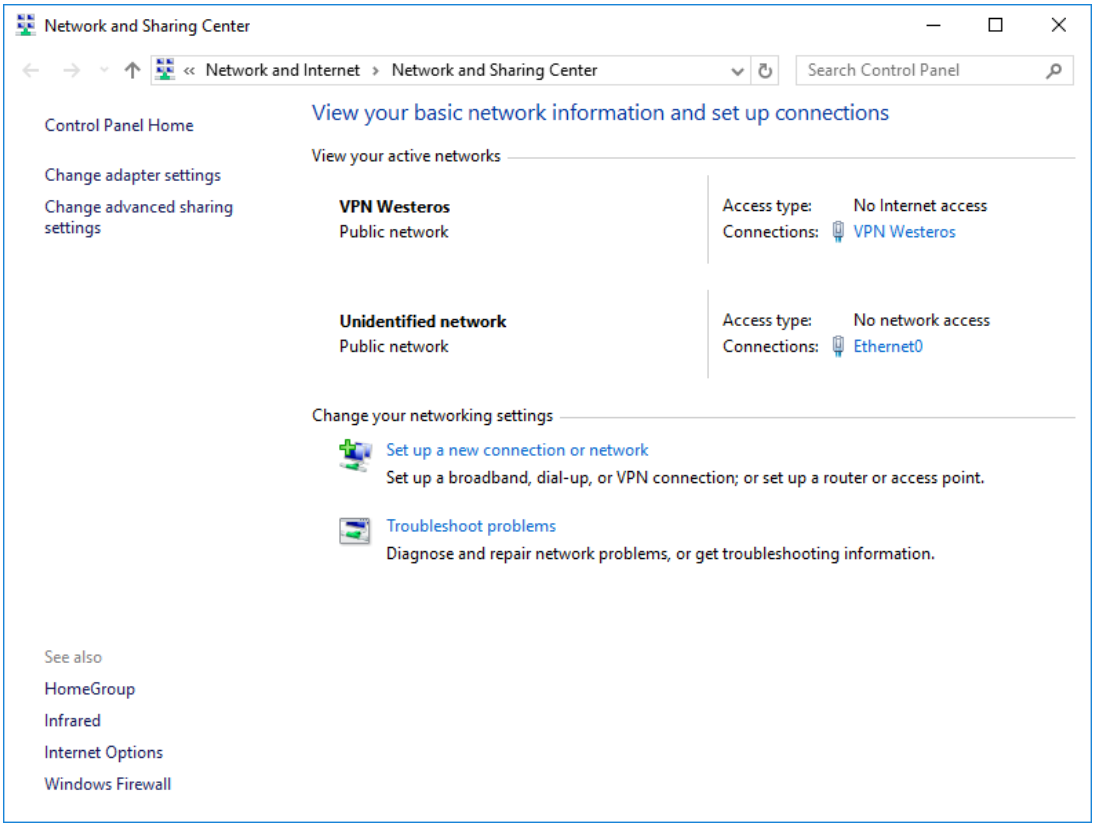

Введите **PIN-код.**




Если всё настроено верно, соединение произойдёт успешно. Статус **Connected.**




Также и в свойствах подключения отображено успешное подключение.




На этом настройка и проверка окончена.

# Контакты, техническая поддержка

## Офис (общие вопросы)

Адрес:129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней

## Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

**www.aladdin-rd.ru/support/index.php**

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

# Регистрация изменений

| Версия | Изменения |
|---|---|
| 1.0 | Исходная версия документа |
| | |
| | |

Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, №3442 от 10.11.17
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
Apple Developer



Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru