Хотите организовать безопасный и защищенный доступ к интернету на смартфоне или ноутбуке при подключении к ненадежной сети, например к сети WiFi в гостинице или кафе? Виртуальная частная сеть (VPN) позволит вам конфиденциально и безопасно работать в незащищенных сетях, как если бы вы находились в частной сети. Трафик поступает с сервера VPN и продолжает движение в пункт назначения.

В сочетании с соединениями HTTPS данная схема позволяет защитить учетные данные и транзакции в беспроводной сети. Вы можете обойти географические ограничения и цензуру и скрыть свое местоположение и любой нешифруемый трафик HTTP от незащищенной сети.

Преимущества и недостатки L2TP протокола

Преимущества:

- Использует надежный и безопасный алгоритм шифрования AES-256
- Поддерживает большое количество операционных систем
- Простой в настройке

Недостатки:

- Использует UDP порт 500, который может быть заблокирован некоторыми брандмауэрами
- Немного медленнее, чем IPSec IKEv2, из-за двойной инкапсуляции

Для подключения VPN необходимо сгенерировать конфигурацию, как это сделать мы расскажем ниже.

Шаг 1. Приобретение сервера

На странице заказа NetRay оплатите тариф **VPN - PLUS (L2TP_IPSec)**

После успешной оплаты вы получите сообщение на почту. В сообщении будут указаны информация о сервере и данные удаленного управления.

***Данные авторизации не являются уникальными. При первом входе система принудительно инициирует смену пароля.*

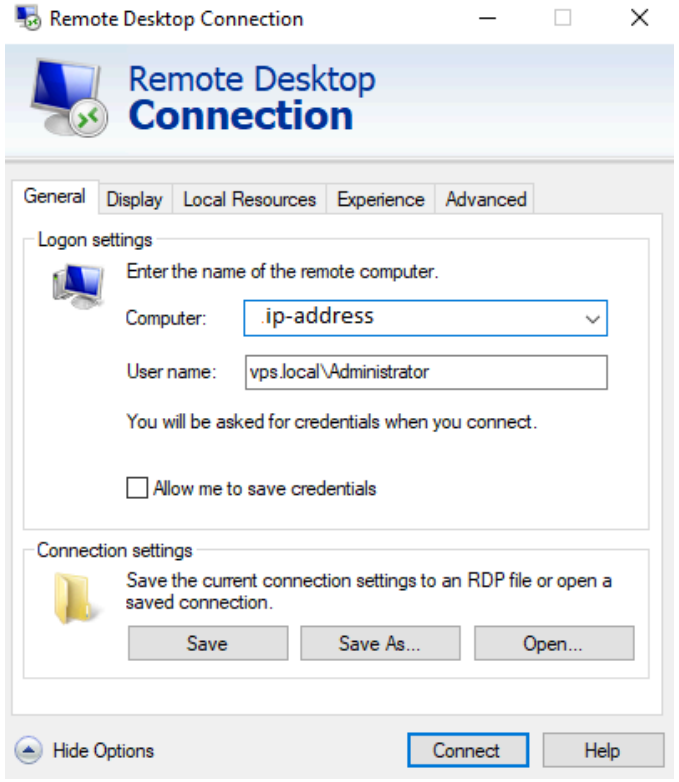
После подключения к серверу вам потребуется подтвердить вашу личность с помощью пароля. Обязательно создайте надежный и уникальный пароль не менее 8 символов.

Шаг 2. Подключение к серверу

Для удаленного управления выделенным сервером необходимо подключиться к нему через RDP:

Если у вас ОС **Windows**:

1. Откройте меню **Пуск** → **Подключение к удаленному рабочему столу**. Или **Win+R** и введите в поле “**mstsc**”
2. В поле **Компьютер** введите полученный из письма публичный IP-адрес сервера.
3. Нажмите **Подключить**.



4. Введите **Имя пользователя** и **Пароль.** *После подключения к серверу вам потребуется подтвердить вашу личность с помощью пароля. Обязательно создайте надежный и уникальный пароль не менее 8 символов.*.
5. Нажмите **OK**.

Если у вас ОС **Linux:**

1. Установите RDP-клиент (rdesktop, Remmina и пр.).
2. Откройте Терминал.
3. Подключитесь к серверу (пример для rdesktop) :

```
rdesktop <server IP> -u <user> -p <password>
```

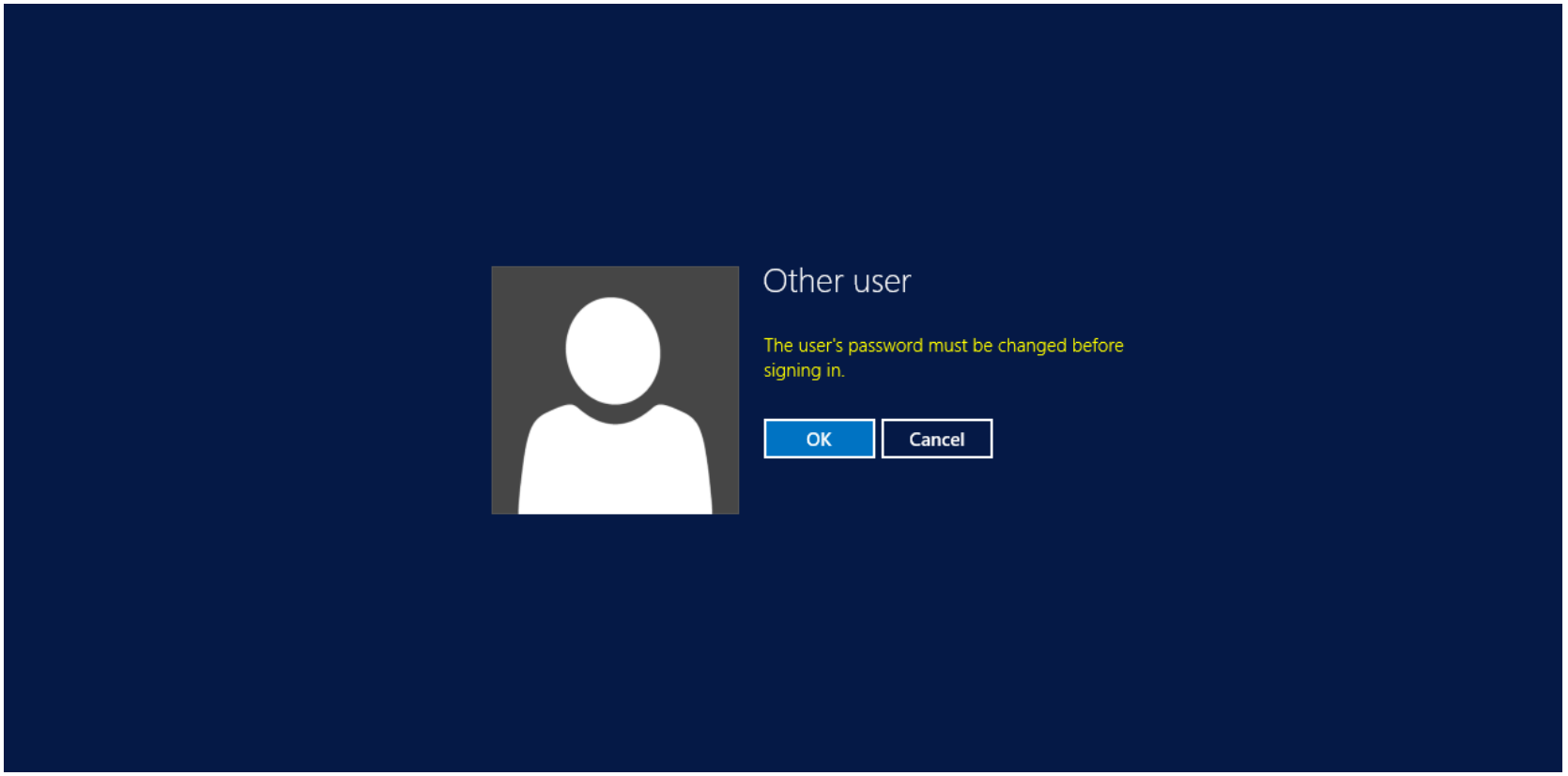
Укажите:

- <server IP> — публичный IP-адрес сервера;
- <username> — имя пользователя;
- <password> — пароль.

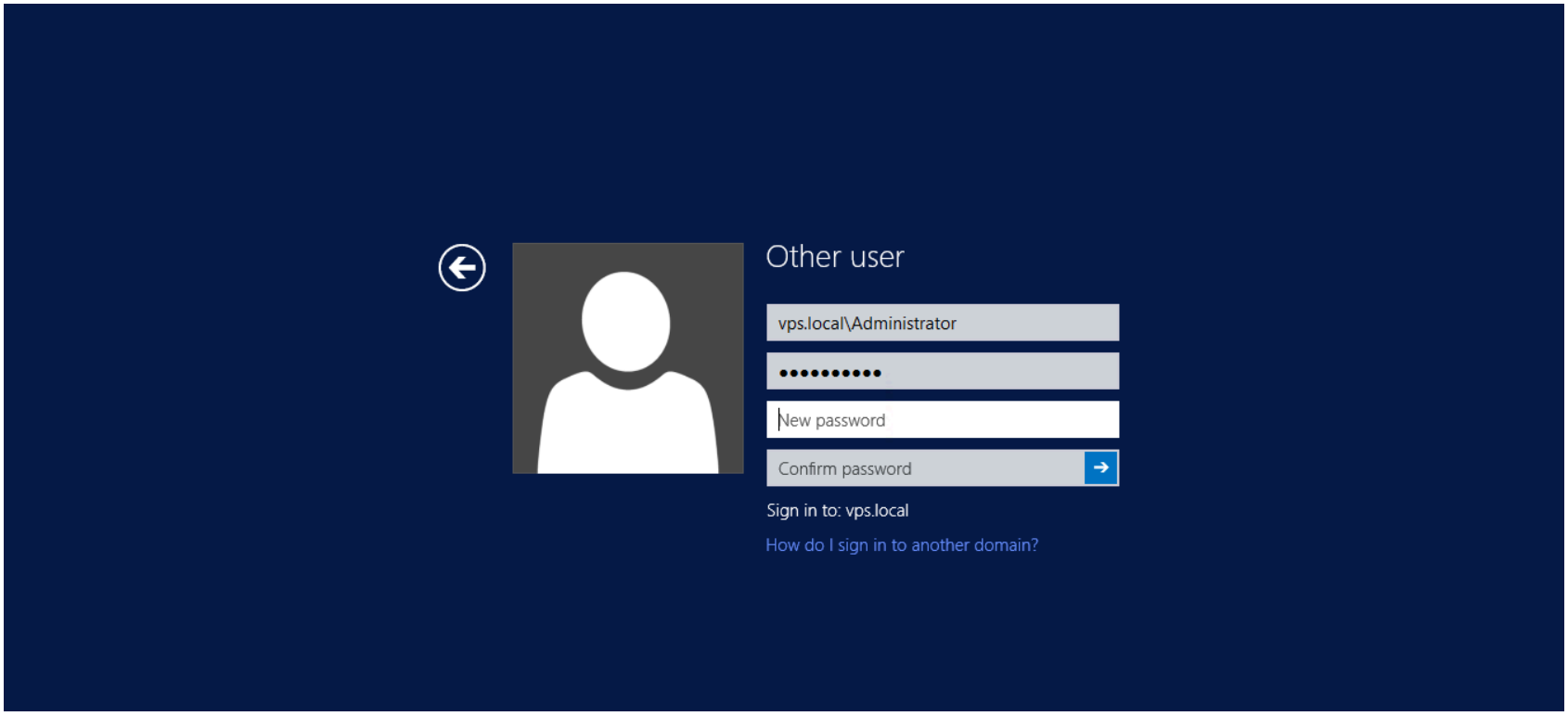
Если у вас ОС **MacOS:**

1. Установите Microsoft Remote Desktop и запустите его.
2. Нажмите +.
3. В поле PC name введите публичный IP-адрес сервера.
4. Введите Username и Password.
5. Нажмите Save.
6. Дважды щелкните по созданному подключению в списке.

После подключения к серверу вам потребуется подтвердить вашу личность с помощью пароля.
При первом входе система принудительно инициирует смену пароля.



Обязательно создайте надежный и уникальный пароль не менее 8 символов.

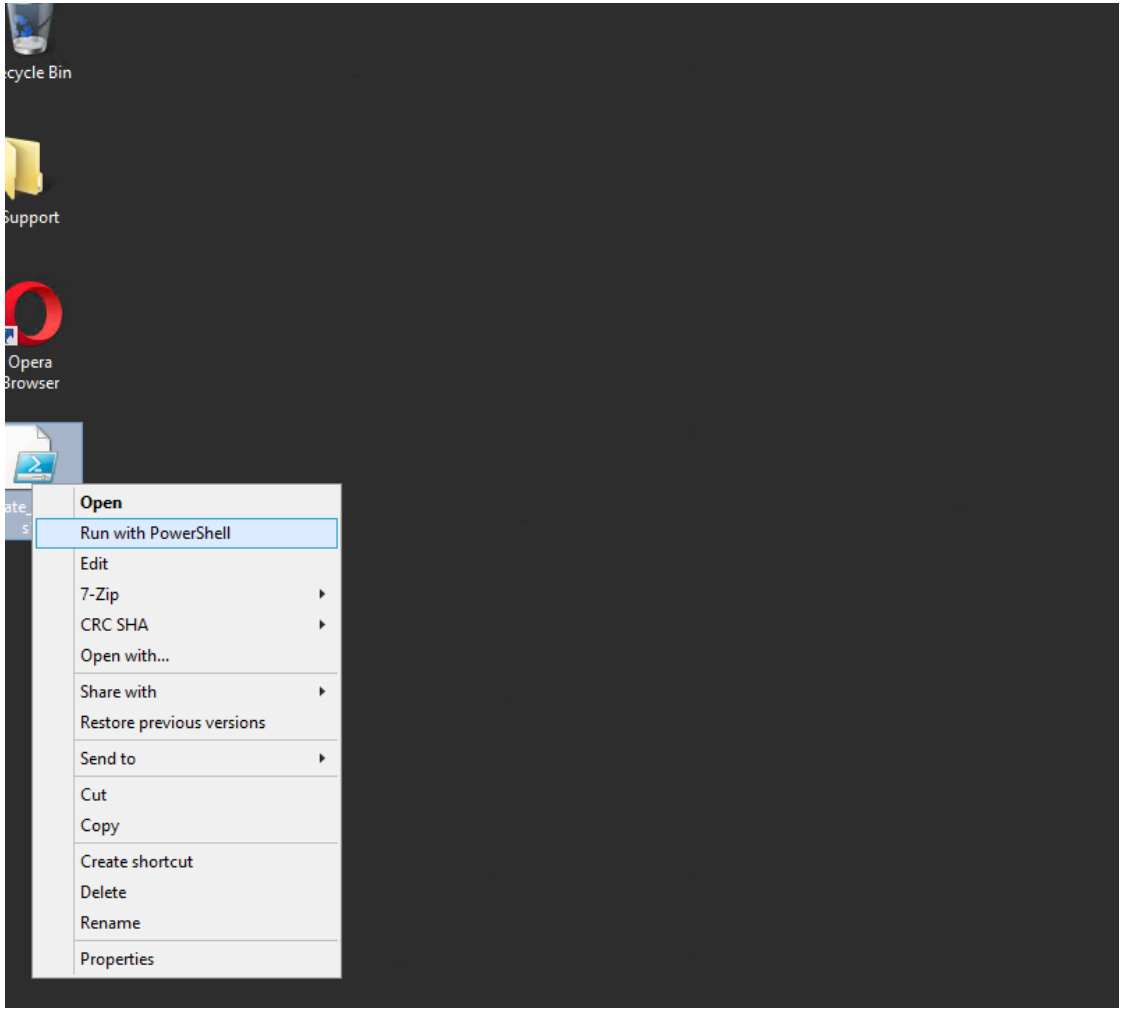


Шаг 3. Получение конфигурации

На вашем сервере уже предустановлен сценарий для генерации конфигураций.
Вы можете сгенерировать конфигурацию и загрузить ее на любое из своих устройств.

Для получения VPN конфигурации, вам необходимо:

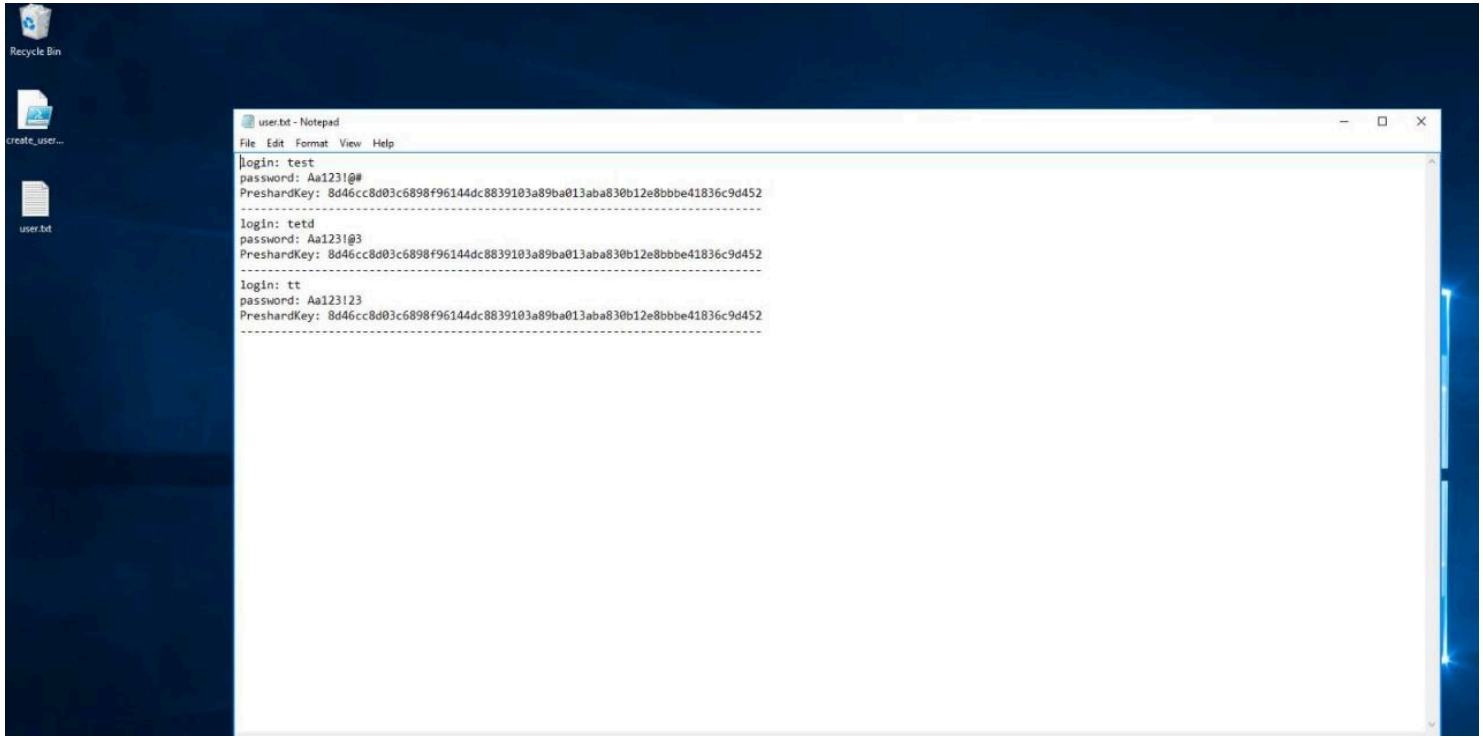
1. Запустить на вашем рабочем столе сервера через контекстное меню Run with PowerShell **“Create_user.ps1”**



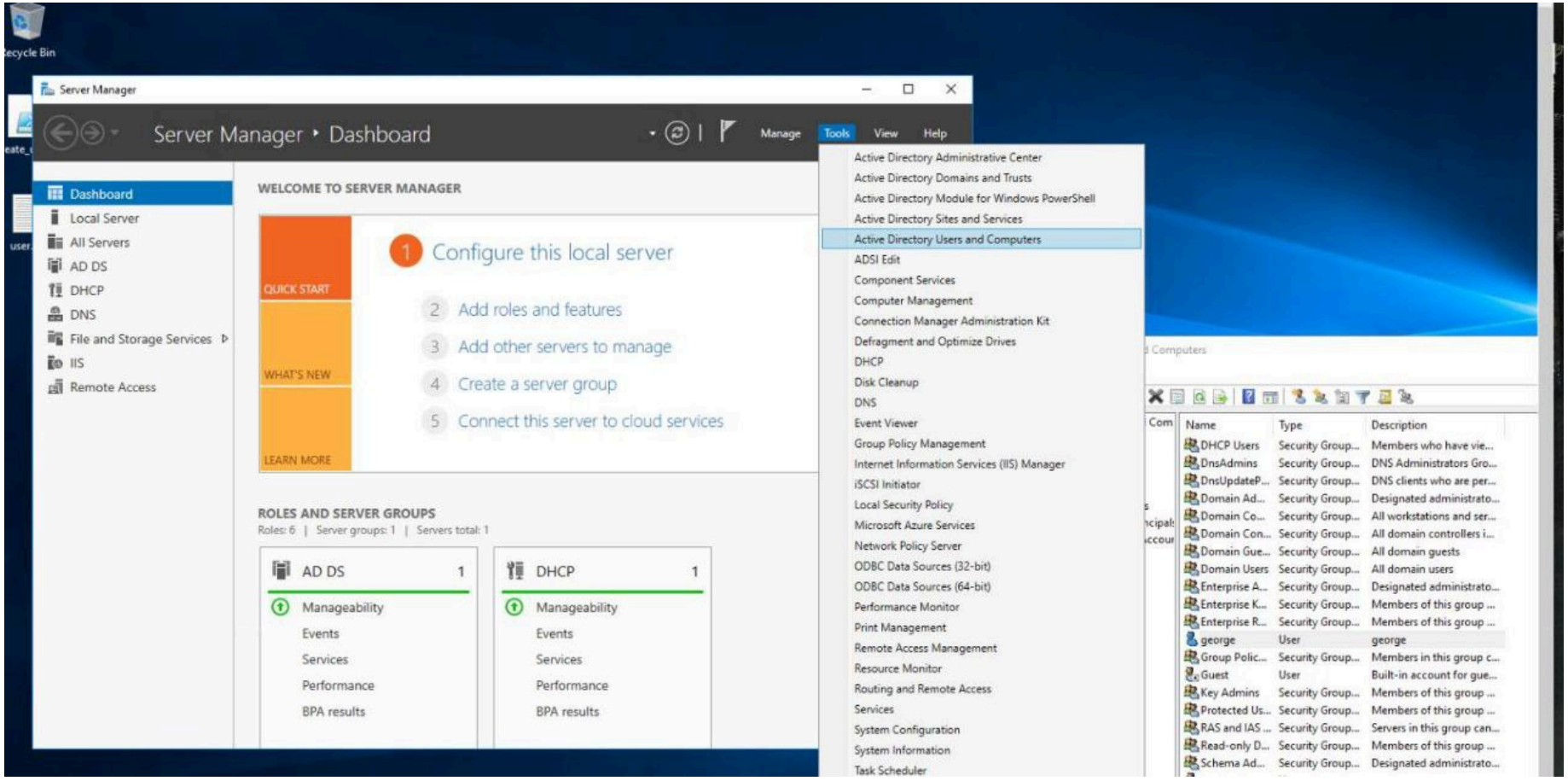
2. В запущенной программе вам будет предложено ввести логин и пароль для пользователя, которого вы хотите создать. В конце работы программы будет создан файл “user.txt” с введенными вами данными, а также секретный ключ PreshardKey.

*** Обратите внимание что пароль должен быть не менее 8 символов, должен содержать большие и маленькие буквы, цифры и спецсимволы. Например: Aa123!@#*

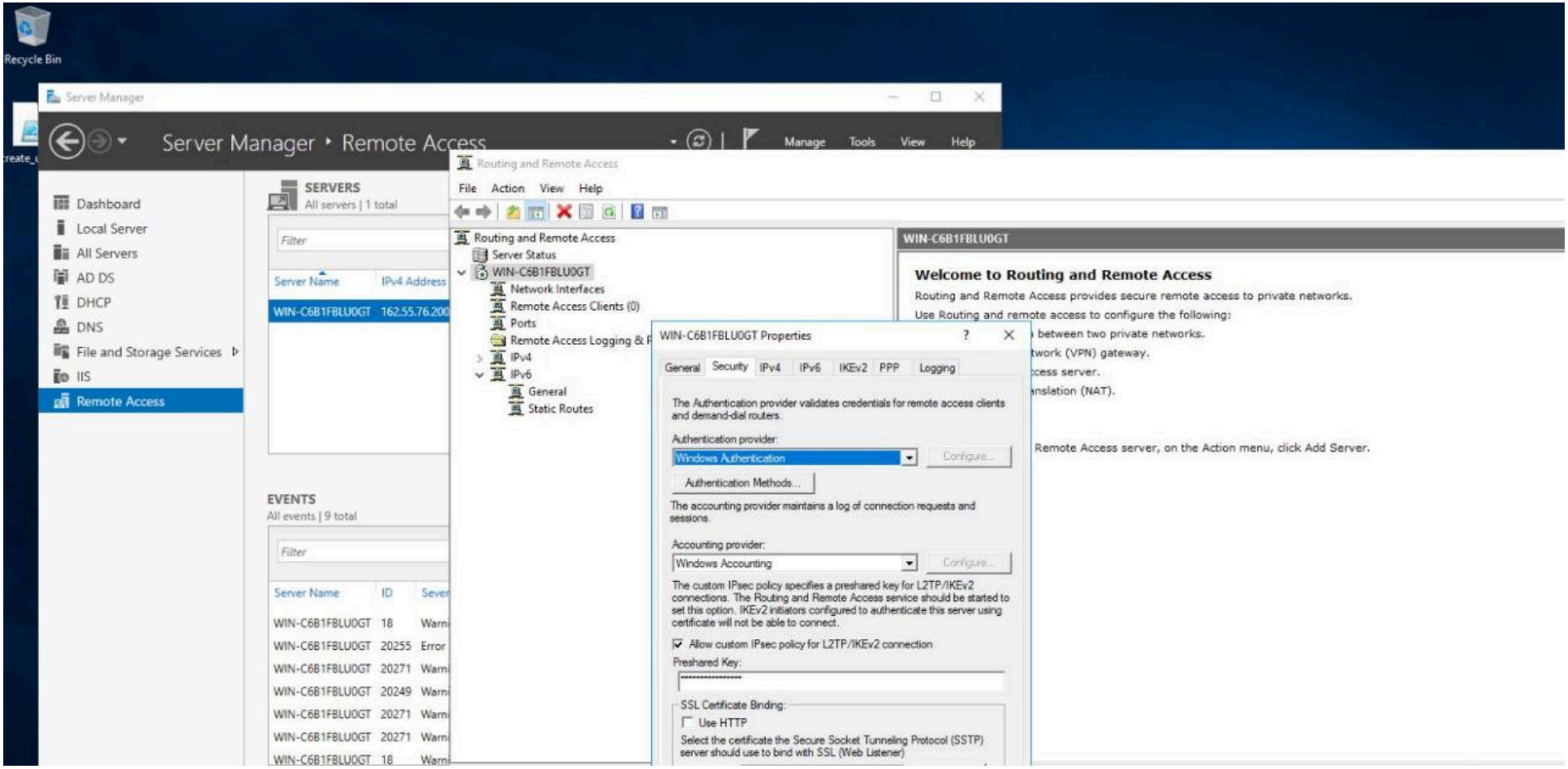
После создания пользователя вы теперь можете спокойно подключаться к VPN



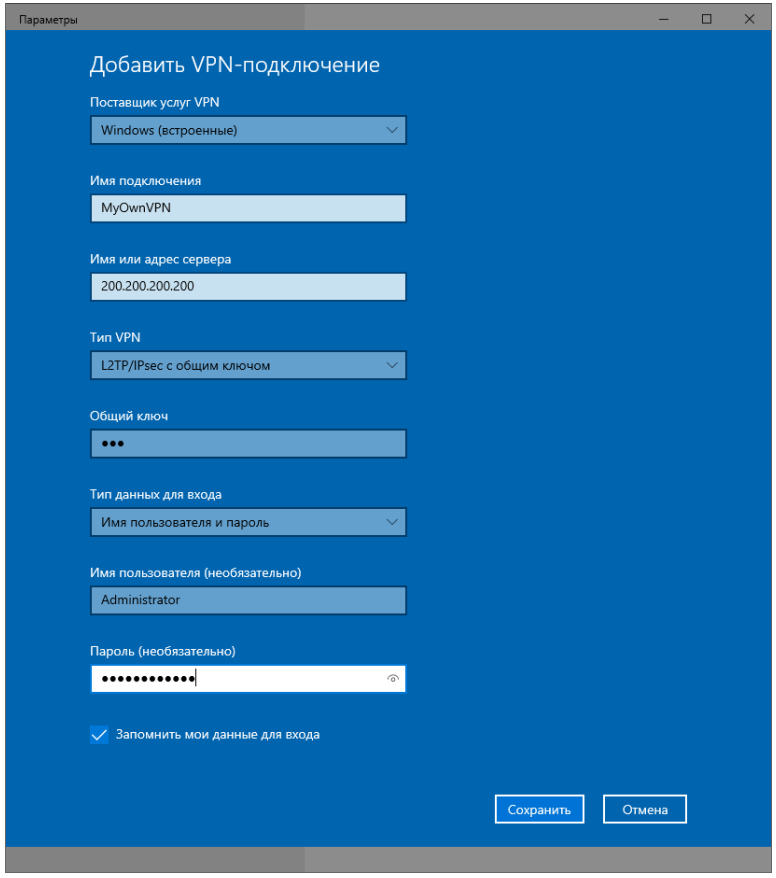
3. Если вы хотите проверить уже существующих пользователей, заблокировать или удалить их, то вам необходимо перейти во вкладку “**Active Directory Users and Computers**”



4. Если вы хотите сменить ключ PreshardKey, то вы можете это сделать через вкладку “**Routing and Remote Access**”. В открывшимся окне выберите ваш сервер и нажмите ПКМ “**Свойства**”, затем вкладку “**Security**”



Шаг 4. Подключение VPN



- Windows (Вам нужен пункт №5 “**Подключаемся по VPN**”)
  - *Имя подключения* задавайте какое вам хочется.
  - *IP адрес* – это адрес вашего VPN сервера.
  - *Тип VPN* – l2TP с общим ключом.
  - *Общий ключ* – это PreshardKey в файле “user.txt”
  - *Логин и пароль* — также находится в файле “user.txt”.
- Linux
- MacOS (раздел “**Настройка VPN (L2TP/IPsec) для MacOS**”)
- Android
- iOS

Шаг 5. Проверка IP-адреса

Далее обязательно проверьте свой IP-адрес. Это можно сделать с помощью бесплатных whois-сервисов, посетив нужный сайт. Например:

- 2ip
- whoer.net
- hidemy