

WireGuard

WireGuard - это коммуникационный протокол и бесплатное программное обеспечение с открытым исходным кодом, который реализует зашифрованные виртуальные частные сети.

- [Документация пользователя](#)
 - [Настройка WireGuard на Windows](#)

Документация пользователя

Настройка WireGuard на Windows

Установка

Скачиваем WireGuard с официального сайта по ссылке:

<https://download.wireguard.com/windows-client/wireguard-installer.exe>

Запускаем скаченный файл и ждем окончания установки программы.

Запустить Powershell под администратором. Через Powershell добавляем параметр в реестр:

```
reg add HKLM\Software\WireGuard /v DangerousScriptExecution /t REG_DWORD /d 1 /f
```

Настройка

Открыть программу со значка в трее. Добавить туннель. Добавить пустой туннель. Внести конфигурацию в окно программы.

Настройки можно уточнить у администратора сервера WireGuard.

[Interface]

PrivateKey = abcd

Address = 172.16.0.2/32

PostUp = powershell -command "\$wgInterface = Get-NetAdapter -Name %WIREGUARD_TUNNEL_NAME%;

ROUTE ADD 192.168.0.0 MASK 255.255.255.0 172.16.0.1 IF \$wgInterface.ifIndex METRIC 95"

PreDown = powershell -command "\$wgInterface = Get-NetAdapter -Name %WIREGUARD_TUNNEL_NAME%;

ROUTE DELETE 192.168.0.0 MASK 255.255.255.0 172.16.0.1 IF \$wgInterface.ifIndex METRIC 95"

Table = off

[Peer]

PublicKey = efgh

AllowedIPs = 0.0.0.0/0

Endpoint = 1.2.3.4:13231

PersistentKeepalive = 15

PrivateKey - Закрытый ключ шифрования (Устанавливается при создании нового подключения)

Address - Локальный адрес

PostUp - Исполняемый скрипт после поднятия туннеля.

PreDown - Исполняемый скрипт после закрытия туннеля.

Table - Включение основного шлюза

PublicKey - Открытый ключ шифрования сервера

AllowedIPs - Разрешенные адреса с удаленной сети

Endpoint - Адрес и порт подключения к серверу

PersistentKeepalive - Время для обмена пакетами поддержки.

После внесения настроек, нажимаем "Подключится".