**[Как установить Wireguard на Ubuntu 20.04 LTS](https://infoit.com.ua/linux/kak-ustanovit-wireguard-na-ubuntu-20-04-lts/)**

[FORGERO](https://infoit.com.ua/author/forgero/)  05.04.2021

**Как установить Wireguard на Ubuntu 20.04 LTS**

В этом руководстве мы покажем вам, как установить Wireguard на Ubuntu 20.04 LTS. Для тех из вас, кто не знал, Wireguard — это надежное, продвинутое программное обеспечение с открытым исходным кодом для VPN-туннелирования, которое вы можете установить и использовать прямо сейчас для создания безопасного соединения точка-точка с сервером. Он кроссплатформенный и может работать практически где угодно, включая Linux, Windows, Android и macOS. Wireguard — это одноранговая VPN. он не использует модель клиент-сервер. В зависимости от конфигурации одноранговый узел может действовать как традиционный сервер или клиент.

В этой статье предполагается, что у вас есть хотя бы базовые знания Linux, вы знаете, как использовать оболочку, и, что наиболее важно, вы размещаете свой сайт на собственном VPS. Установка довольно проста и предполагает, что вы работаете с учетной записью root, в противном случае вам может потребоваться добавить ‘ sudo‘ к командам для получения привилегий root. Я покажу вам пошаговую установку Wireguard на Ubuntu 20.04 (Focal Fossa). Вы можете следовать тем же инструкциям для Ubuntu 18.04, 16.04 и любого другого дистрибутива на основе Debian, например Linux Mint.

**Установите Wireguard на Ubuntu 20.04 LTS Focal Fossa**

**Шаг 1. Во-первых, убедитесь, что все ваши системные пакеты обновлены, выполнив следующие aptкоманды в терминале.**

sudo apt update

sudo apt upgrade

**Шаг 2. Установка Wireguard на Ubuntu 20.04.**

WireGuard доступен из репозиториев Ubuntu по умолчанию. Выполните следующие команды, чтобы установить его:

sudo apt install wireguard

**Шаг 3. Настройте WireGuard.**

Сначала выполните следующую команду, чтобы сгенерировать пару ключей:

wg genkey | sudo tee /etc/wireguard/privatekey | wg pubkey | sudo tee /etc/wireguard/publickey

Затем создайте новый файл с именем и добавьте следующее содержимое:wg0.conf

sudo nano /etc/wireguard/wg0.conf

[Interface]

Address = 10.0.0.1/24

SaveConfig = true

ListenPort = 51820

PrivateKey = SERVER\_PRIVATE\_KEY

PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE

PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -t nat -D POSTROUTING -o ens3 -j MASQUERADE

Приведенные выше термины из файла определены ниже:wg0.conf

* Address — разделенный запятыми список IP-адресов v4 или v6 для wg0интерфейса. Используйте IP-адреса из диапазона, зарезервированного для частных сетей (10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16).
* ListenPort — порт, на котором WireGuard будет принимать входящие соединения.
* PrivateKey — закрытый ключ, сгенерированный wg genkeyкомандой. (Чтобы увидеть содержимое файла запуска: )sudo cat /etc/wireguard/privatekey
* SaveConfig — при значении true текущее состояние интерфейса сохраняется в файле конфигурации при завершении работы.
* PostUp — команда или скрипт, который выполняется перед запуском интерфейса. В этом примере мы используем iptables для включения маскарадинга. Это позволит трафику покидать сервер, предоставляя клиентам VPN доступ в Интернет.
* PostDown — команда или скрипт, который выполняется перед отключением интерфейса. Правила iptables будут удалены, как только интерфейс выйдет из строя.

В и личных файлах ключ не должны быть доступны для чтения обычных пользователей. Используйте, чтобы установить разрешения на 600:wg0.confchmod

sudo chmod 600 /etc/wireguard/{privatekey,wg0.conf}

После этого запустите wg0интерфейс, используя атрибуты, указанные в файле конфигурации:

sudo wg-quick up wg0

[#] ip link add wg0 type wireguard

[#] wg setconf wg0 /dev/fd/63

[#] ip -4 address add 10.0.0.1/24 dev wg0

[#] ip link set mtu 1420 up dev wg0

[#] iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE

Чтобы запустить интерфейс WireGuard во время загрузки, выполните следующую команду:

sudo systemctl enable wg-quick@wg0

**Шаг 4. Настройте брандмауэр.**

Вам необходимо открыть UDP-трафик на порт 51820:

sudo ufw allow 51820/udp

Наконец, мы можем запустить службу Wireguard, используя следующую команду:

sudo wg-quick up wg0

Поздравляю! Вы успешно установили Wireguard . Благодарим за использование этого руководства по установке Wireguard VPN в системе Ubuntu 20.04 LTS Focal Fossa. Для получения дополнительной помощи или полезной информации мы рекомендуем вам [посетить официальный сайт Wireguard](https://www.wireguard.com/) .