Wireguard

Our Wireguard OS template is based on Ubuntu 20, and includes scripts that automate the installation of Wireguard and WGdashbaord for easy user management, monitoring and configuration.

The template is available for new VPS services, as well as when reinstalling the server from Veesp dashboard.

Please note that the scripts run after the VPS has been deployed/reinstalled and may take up to 15 minutes to complete.

⚠ Do not reboot/shut down the VPS right after it is deployed/reinstalled, and let the scripts finish installing/configuring the software.
Once the software is ready, VPS will reboot automatically and you will be able to access the WGdashboard.

How-to use it

1) In order to sign in, follow the link in "Your VPS is deployed" e-mail, or navigate to https://127.0.0.1:10086 (replace 127.0.0.1 with the IP of your server, port: **10086**).

2) Use the default user and login information - **admin/admin**

3) Upon logging in, navigate to the "Setting" section and change your username and then password (you want to do this the moment the server is deployed).

4) You can now start adding users (peers) by navigating to "wg0" under the "Configurations" section and pressing the "+" on the bottom-right of the page (⚠make sure you are not pressing "+" on the homepage, and is used to add new virtual interfaces. Do not press it unless you know what you are doing!).
Enter the name for the peer (public/private keys, as well as the assigned IP address will be selected automatically (although you can change them, if you find it necessary)) and press "Add".

5) Once user is created, you can access the QR code and/or download the configuration file for Wireguard client software on the bottom-right edge of the peer card.

6) Additionally, you can monitor the overall network use, or monitor network load created by specific peers at the bottom of the peer card on the same "wg0" page.

ⓘ We also strongly suggest securing the SSH access to your server (switching from root password to SSH public key authentication, or at the very least switching out the default ssh port and using a strong password).

⚠ Please note that we do not provide support for Wireguard beyond ensuring that the pre-installed software works "out of the box". For any questions regarding more advanced configuration of Wireguard, please refer to their documentation: Official, Un official (but more detailed).
Do note that manually editing Wireguard configuration files might break some WGdashboard functionality. If you are looking to deploy complex routing rules, which require manual configuration, it might be better to choose one of our regular OS template and install/configure everything by hand.

⚠ Important! Wireguard by default routes ALL traffic from the peer. Thus make sure that the connected peers do not emit malicious traffic, which violates our Terms of Service (spam, cyberattacks (bruteforce, network scanning), etc).
You, as the owner of the server, are solely responsible for the traffic emitting from your server, and we will suspend your server if you violate our Terms. Ensure that none of the client (peer) devices that will be connected to your server are infected with malware prior to routing their traffic via your Wireguard server.