

# Instructions for using a firewall on an Ubuntu VPS

Here are the instructions for using a firewall on a VPS:

1. Install a firewall software on your VPS. One of the most popular firewall software for Linux servers is ufw. You can install it by running the command `sudo apt-get install ufw`
2. By default, the firewall is inactive, to enable it you can run the command `sudo ufw enable`
3. To allow incoming traffic on port 80 (HTTP) and port 443 (HTTPS), you can add the following rules to the ufw configuration:

```
sudo ufw allow 80/tcp  
sudo ufw allow 443/tcp
```

4. To block all incoming traffic on other ports, you can run the command `sudo ufw default deny incoming`
5. Verify that the firewall is working correctly by checking the ufw status by running the command `sudo ufw status`
6. To make the firewall rules persistent across reboots, ufw save the rules automatically.
7. If you need to open other ports for specific services such as ftp, ssh or mysql you can use the same command structure `sudo ufw allow [port_number]/[protocol]`

Please note that these instructions provide a basic setup for a firewall on a VPS, and you may need to customize the rules based on your specific use case. It's always a good idea to test your firewall configuration before putting it in production to avoid locking yourself

---

Revision #1

Created 25 January 2023 15:05:27 by Daniel Azimi

Updated 3 June 2023 06:27:52 by Daniel Azimi