How to Secure Your DigitalOcean Droplet/VPS Server using Ubuntu Firewall (UFW)

https://orbisius.com/blog/secure-digitalocean-droplet-vps-server-ubuntu-firewall-ufw-p6810

There are login/authentication attacks done every single second.

Not sure how those hackers manage to detect that a new server is up and running but they start checking for weak points as soon as possible.

Once they get access to it they can install a trojan horse and do all kinds of things.

You don’t want to be paying for somebody else’s mining stuff.

Ubuntu server logs the login attempts in the following file. The system also adds data when a user is deleted or created.

/var/log/auth.log

One of the best ways to protect your server is to block 99% of the access to it and allow access only to the services that are critical. Then whoever needs to have access, the admin whitelists their IP address one by one.

If you’re using a mobile hotspot or a dynamic IP address that might be an issue but you can get a VPN that gives you a static IP address or set up another VPS server that runs a VPN server.

If the connections to the server will be from random IP addresses e.g. you’re running an (S)FTP server then another option to protect the server is to install fail2ban software.

It will improve the security of your server as it will automatically block IPs addresses when they attempt to login incorrectly multiple times.

Very Secure Ubuntu Server

This tutorial teaches you how to make your Ubuntu server very secure. In our products we tend to keep things separate whenever possible so a single server is responsible for one thing. If it's going to host a marketing site it has only the software it needs to run the marketing site. That's usually WordPress, Database server & web server. No email hosting or anything like that. This makes each server efficient and less vulnerable.

We strongly suggest that you use an external service such as Google Workspace/gmail or Zoho to handle the emails if that's the case because it's way easier to switch hosting providers when you know that your emails will keep working.

Additionally, security has to be done in many levels. This is the server level. Security best practices should be applied to the software layer too.

The worlds most secure server is the one that's turned off but that's very practical :)

What is the firewall?

The Firewall acts like a barrier between the internet traffic that comes to your server and the services that are running on it.

It can be configured to block or allow Internet traffic to reach some of the services/programs that are running on your server such as web server(s), databases, email etc.

The firewalls use rules configured by the admin. You need admin/root access to the server in order to complete the suggested steps.

In this post we'll use the program that comes with Ubuntu server. It's called ufw.

UFW stands for uncomplicated firewall. It is a nice & easy to use tool that allows you to add/delete/list rules easily.

How to Protect Your Server

Do you have a DigitalOcean VPS server yet?

The very first thing to do is to select Ubuntu server and make sure the version ends in LTS.
The LTS version stands for Long Term Support version. You want to receive software updates for as long as possible.

Then, the next important thing is to do is update the Ubuntu server software.

This is necessary because some services have been updated right after the official Ubuntu server version was released.

Apply any updates

```
apt-get update
apt-get upgrade -y
```

Many tutorials keep prefixing the commands with sudo.
This can be avoided. You just need to switch to root and you won't have to type that much.
You will need to type the following command and then enter your password. You will be root/admin now.
Of course you need to be super extra careful especially with the rm command.

To switch to root execute the following command.

```
sudo su
```

Next you need to run these commands

```
ufw default deny incoming
ufw default allow outgoing
ufw allow 80/tcp
ufw allow 443/tcp
```

Whitelist your own IP address

To get your IP address you can just type what’s my IP in Google and it will give it to you. We’ll need it because we want to whitelist it.
It's good to put a comment because when you list the firewall rules you'd know why an IP address was whitelisted right away. This is very useful, too, if you hire somebody else to work on your server. They won't just delete that IP address when they know what who belongs to.

ufw allow from 111.222.333.444 comment 'CEO home office IP'

Explanations

ufw default deny incoming - blocks all access to the server by default. This is good. This way we can only allow access to certain ports only.

ufw default allow outgoing - This allows the server to make outgoing connections. It needs to be able to pull software updates from the official channels.

ufw allow 80 - allows access to the default HTTP on port 80 to be accessible

ufw allow 443 - allows access to the secure HTTP port 443 to be accessible.

Activate/Enable Ubuntu UFW/Firewall

We intentionally left this step as last just to make sure you have done the previous ones.
If you haven't done them do so now because if you have skipped any of the steps you will get locked out!

ufw enable

This should enable the firewall.

If you have whitelisted your IP address then you should still have a connection to the server.

Locked yourself out?

yes, this normal and expected because this is a very secure Ubuntu server set up.

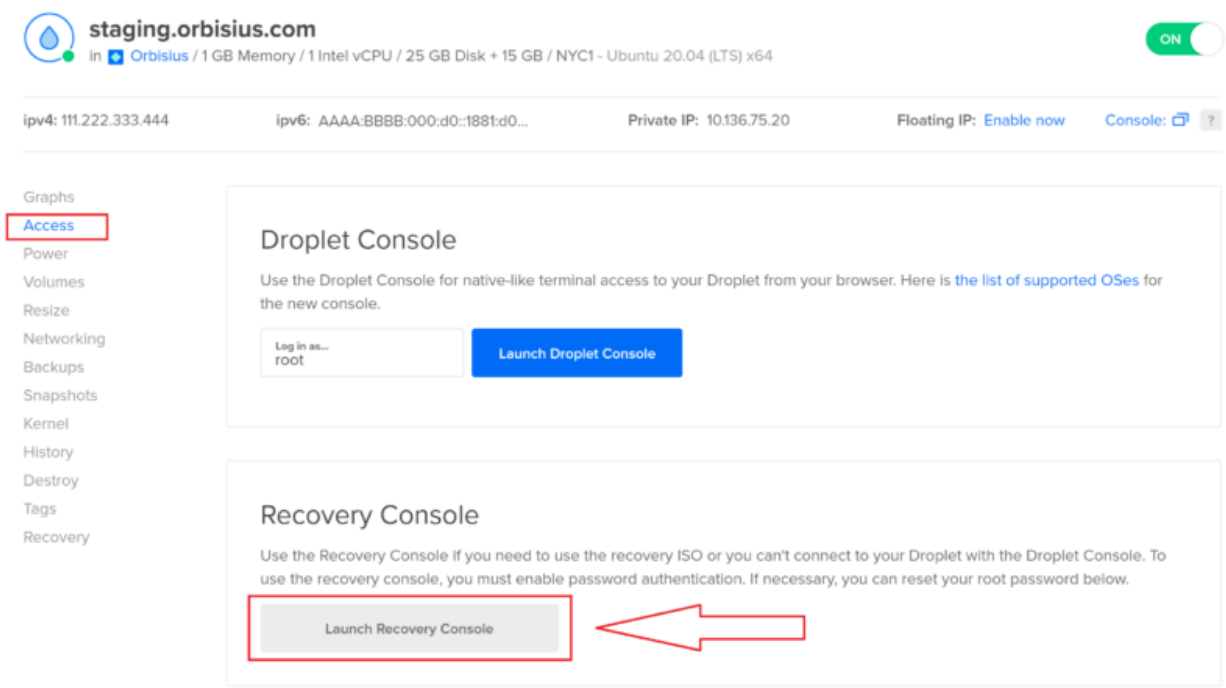
The great thing about VPS servers is that the providers such as DigitalOcean give you a console that you can access from within your browser.

With dedicated servers you have to pay to get that kind of access called KVM. Some providers attach one on your server for free but only for 2-3 hours.

You need to go access the VPS/Droplet from DigitalOcean Cloud and then > Access > **Recovery Console** .

Then you need to enter your root username and password.

After you login you need to execute the same commands for whitelisting an new IP address shown in this post.



How to get to DigitalOcean VPS Droplet Recovery Console

If you do not have a **DigitalOcean** account, you can sign up here

If you need help implementing some of the steps in this howto/tutorial **contact us** (free estimate)

Disclaimer: The content in this post is for educational purposes only. Always remember to take a backup before doing any of the suggested steps just to be on the safe side. Referral Note: When you purchase through an referral link (if any) on this page, we may earn a commission.