Run the following command to set up your Tor relay:  
*Only run this script if your hoster/ISP allows Tor!*

curl https://tor-relay.co/nf/0f1f2b437eea7a609a536a9f0be8739c.sh | bash

Or if you don't trust this page or your network connection and you want to inspect the file before running it:

wget https://tor-relay.co/nf/0f1f2b437eea7a609a536a9f0be8739c.sh

less 0f1f2b437eea7a609a536a9f0be8739c.sh

bash 0f1f2b437eea7a609a536a9f0be8739c.sh

Torrc Preview

SocksPort 0

RunAsDaemon 1

ORPort 9001

Nickname paradox

ContactInfo theindianbadger(at)gmail(dot)com [tor-relay.co]

DirPort 9030

ExitPolicy reject \*:\*

RelayBandwidthRate 10 MBits

RelayBandwidthBurst 50 MBits

AccountingStart month 1 00:00

AccountingMax 5000 GB

3) Optional Setup and Tips

Here are a few things you can do to ensure the security of your relay.

Updates

You should regularly install security updates for your operating system.

On Ubuntu and Debian you can update your system by running

apt-get update && apt-get upgrade

SSH

When you run a relay server you will see an increase in SSH login attempts.  
To increase sever security you should disable root login via password or only allow public-key access in general.  
  
First make sure that you added a user you can login with.  
[The Digitalocean Community provides some tips for initial server setup.](https://www.digitalocean.com/community/tutorials/initial-server-setup-with-ubuntu-14-04)   
  
To disable logins as root user edit this file as root:

nano /etc/ssh/sshd\_config

Search for the line that says

PermitRootLogin yes

And change it to

PermitRootLogin without-password

After that restart the SSH service

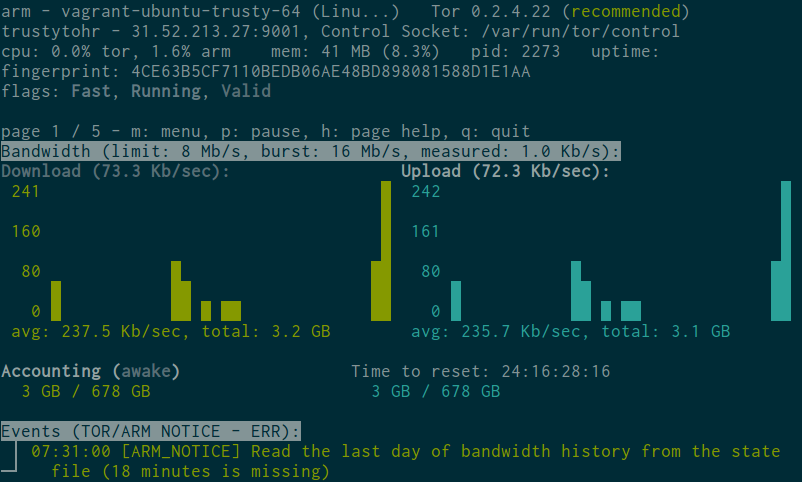
service ssh restart

Services

Don't run any unnecessary services. It is recommended to only run Tor itself on your relay server. This minimizes potential attack vectors.  
A static webpage should not be a problem but you probably don't want to run your Wordpress on a Tor server.

## MONITORING TOR

If we wanted to watch our relay’s activities from the command line, we could use arm. It’s like top for our relay:



To install it, just do:

$ sudo apt-get install tor-arm

One problem you may encounter is that arm needs to access resources owned by the debian-tor user, so I usually start it with:

$ sudo -u debian-tor arm

But be aware that this gives arm access to everything in /var/lib/tor/, including our keys, so we are expanding the attack surface. Hopefully this will be improved in future versions.