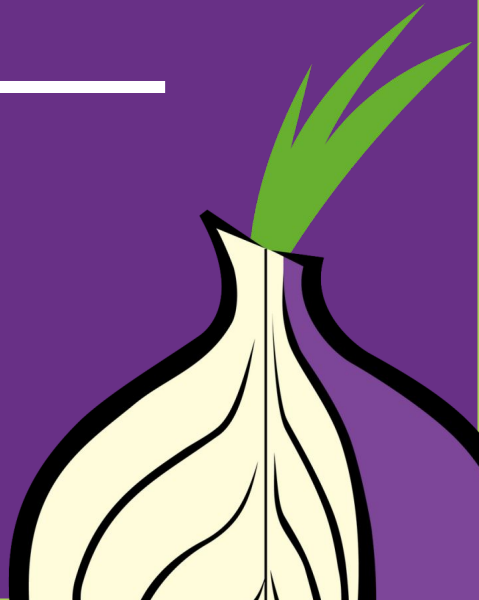
The Tor Network



Topics

- What's Tor?
- Types of relays
- Technical setup
- More about relays
- Relay diversity
- Getting help

What’s Tor?

- Tor is a free software and an open network
- Mitigates against tracking, surveillance and censorship
- Run by a US non-profit and volunteers from all over the world
- It’s Tor, not TOR

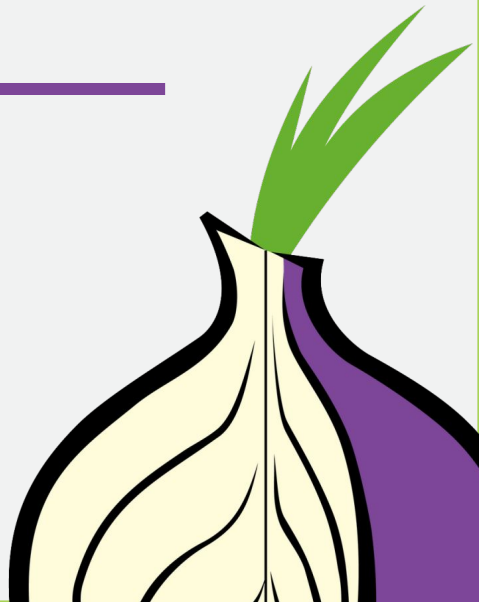
The Tor network

- An open network, everyone can be part of it. Basically, your server will relay the tor traffic to another server in the Internet.
- The network is composed by different types of servers run by volunteers around the world.
- To ingress in the network, the new server will pass automatically to a new relay lifecycle.

Why run a Tor relay?

- By running a Tor relay you can help make the Tor network:
  - faster (and therefore more usable)
  - more robust against attacks
  - more stable in case of outages
  - safer for its users (spying on more relays is harder than on a few)

Types of relays



Guard/middle (aka non-exit) relay

- A guard is the first relay in the chain of 3 relays building a Tor circuit.
- A middle relay is neither a guard nor an exit, but acts as the second hop between the two.
- To become a guard, a relay has to be stable and fast (at least 2MByte/s) otherwise it will remain a middle relay.

Exit relay

- The exit relay is the final relay in a Tor circuit, the one that sends traffic out its destination.
- That’s why exit relays have the greatest legal exposure and liability of all the relays.
- Before running an exit relay, check it with your local digital rights organization.
- **You should not run a Tor exit relay from your home**

Bridge

- Bridge is a node in the network that isn’t listed in the public Tor directory, which make it harder for ISPs and governments to block it.
- Bridges are relatively easy, low-risk and low bandwidth Tor nodes to operate.
- And there’s another special kind of bridge: Pluggable transports. It hides your tor traffic by adding an additional layer of obfuscation.

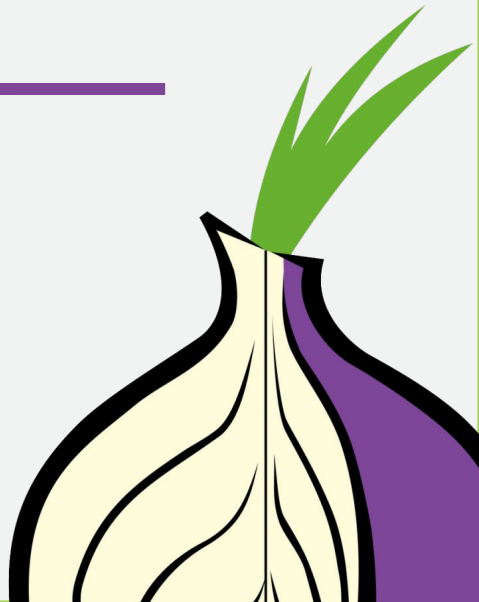
The lifecycle of a new relay

- Non-exit relays pass by a lifecycle of four phases (defined by days):
  - Days 0-3: the unmeasured phase
  - Days 3-8: network authorities start the remote measurement phase (the ramp-up guard phase)
  - Days 8-68: guard phase (where load counterintuitively drops and then rises higher)

The lifecycle of a new relay

- And after 68 days, if the relay is stable and fast enough, it receives a Guard flag (steady-state guard phase).
- Exit relays also have a lifecycle more or less similar.
- Read about all the phases in: https://blog.torproject.org/lifecycle-new-relay

Relay requirements



Before we start

- Never run a relay without the consent of network administrator or machine owner. Read the Terms of Service (ToS) first, so you don’t lose money.
- Choose which type of relay you will host. Non-exit relay is a easy way to start helping the network.
- Read the documentation:
- https://torproject.org/tor-relays

Bandwidth requirements

- At least 16 Mbit/s (Mbps) upload and download bandwidth available for Tor. More is better.
- The minimum requirements for a relay are 10 Mbit/s (Mbps).
- If you have less than 10 Mbit/s but at least 1 Mbit/s we recommend you run a bridge with obfs4 support.

Monthly outbound traffic

- It is required to use a minimum of 100 GByte of outbound/incoming traffic per month.
- If you have a metered plan you might want to configure tor to only use a given amount of bandwidth or monthly traffic.
- More (>2 TB/month) is better and recommended.

Public IPv4 address

- Every relay needs a public IPv4 address - either directly on the host (preferred) or via NAT and port forwarding.
- The IPv4 address is not required to be static but static IP addresses are preferred.
- Your IPv4 address should remain unchanged for at least 3 hours (network consensus).
- You can only run two Tor relays per public IPv4.

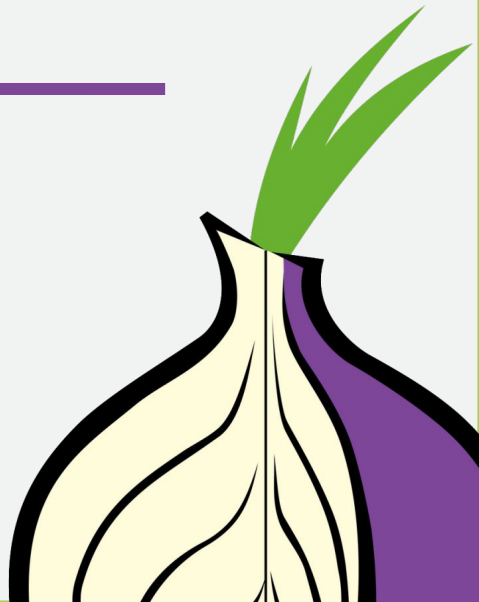
Other requirements

- Memory: A <40 Mbit/s non-exit relay should have at least 512 MB of RAM available.
- Disk storage: Tor does not need much disk storage. A typical Tor relay needs less than 200 MB.
- Any modern CPU should be fine.
- Uptime: Ideally the relay runs on a server which runs 24/7.

Choosing your relay hosting

- Tor community maintain the list GoodBadISPs, about the experience of running relays: https://trac.torproject.org/projects/tor/wiki/doc/GoodBadISPs
- Some providers only allow non-exit relays, so before buying a service, check the GoodBadISPs.
- This can cost anywhere between $3.00/mo and thousands per month.

Technical setup



Non-exit relay – Debian/Ubuntu

1. Enable the Torproject package repository

2. Install the tor package
   - `apt update && apt install tor`

3. Put the configuration file /etc/tor/torrc in place:
   - `Nickname myNiceRelay`
   - `ExitRelay 0`
   - `SocksPort 0`
   - `ControORPort 443`
   - `lSocket 0`
   - `ContactInfo tor-operator@your-emailaddress-domain`
   - `Log notice syslog`

4. Restart the tor daemon:
   - `systemctl restart tor@default`

Non-exit relay – FreeBSD

1. Install the tor package
    - `pkg install tor ca_root_nss`

2. Edit the configuration file/usr/local/etc/tor/torrc
    - `Nickname myNiceRelay`
    - `ORPort 9001`
    - `ExitRelay 0`
    - `SocksPort 0`
    - `ControlSocket 0`
    - `ContactInfo tor-operator@your-emailaddress-domain`
    - `Log notice syslog`

3. Ensure that the random_id sysctl setting is enabled:
    - `echo "net.inet.ip.random_id=1" >> /etc/sysctl.conf`
    - `sysctl net.inet.ip.random_id=1`

Non-exit relay – FreeBSD

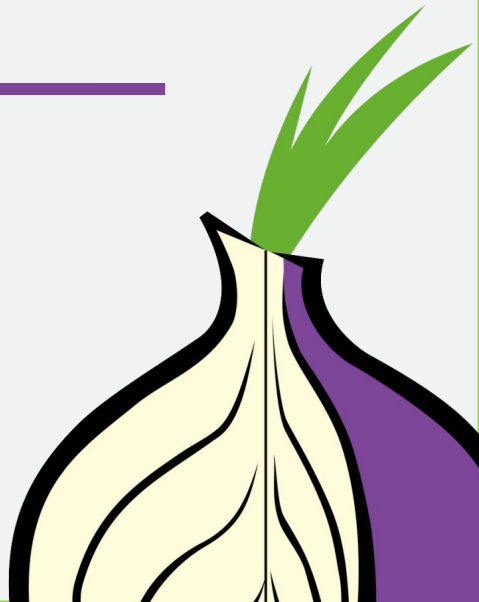
4. Start the tor daemon and make sure it starts at boot:
    - `sysrc tor_enable=YES`
    - `service tor start`

Optional, but recommended to get package updates faster: https://trac.torproject.org/projects/tor/wiki/TorRelayGuide/FreeBSD

Verify that your relay works

- After restarting the service, verify in the log file if it contains the following entry:
  - Self-testing indicates your ORPort is reachable from the outside. Excellent. Publishing server descriptor.
- About 3 hours after you started your relay it should appear on Metrics portal in Relay Search.

More about relays



Technical tips

- Enable automatic software updates.
- Backup your Tor Identity Keys.
- It’s possible to limit bandwidth usage (and traffic). Check the parameters, for example: AccountingMax, AccountingRule, AccountingStart.
- If run more than one Tor relay, you need to set MyFamily parameter.

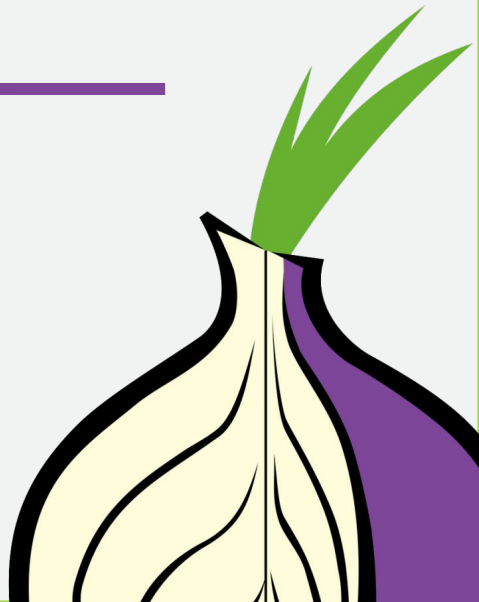
Orchestrating

- Running multiple relays by hand can be challenging.
- Configuration management tools can make the relay operator life easier:
  - Ansible-relayor: http://github.com/nusenu/ansible-relayor
  - Bash script: https://github.com/coldhakca/tor-relay-bootstrap

Metrics

- Metrics portal - https://metrics.torproject.org
- It’s possible to search: how many relays are in the network, how many are exit, etc
- In 2019 there are ~6,600 relays and ~1,500 bridges.
- Check: how many relays are in your country? Who run these relays? How diverse it is?

Network diversity



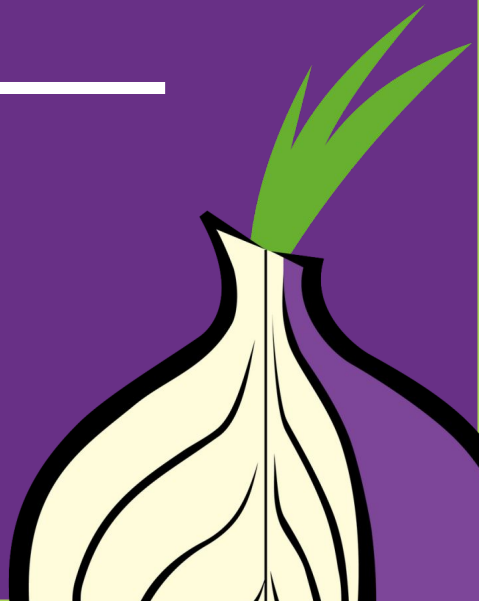
Monoculture

- A single kernel vulnerability in GNU/Linux impacting Tor relays could be devastating.
- Diversity of Operating System (OS): ~90% of relays are Linux.
- Diversity of Autonomous System (AS). Try to avoid the following hosters: OVH SAS (AS16276), Online S.a.s. (AS12876), Hetzner Online GmbH (AS24940), DigitalOcean, LLC (AS14061).

The TorBSD Diversity Project

- The Tor BSD Diversity Project (TDP) is an initiative seeking to extend the use of the BSD Unix operating systems in the network.
- Goals: increase the number of Tor relays running BSDs; Engage the BSD community about Tor anonymity; Port tor related programs to BSD operating systems.
- TorBSD website: https://torbsd.org/

More about exit relays



Legal information

- In many countries there are regulations that exclude communication service providers from liability.
- It's a good idea to consult with a lawyer or your local digital rights organization.
- Under most circumstances you will be able to handle legal matters by having an abuse response letter.

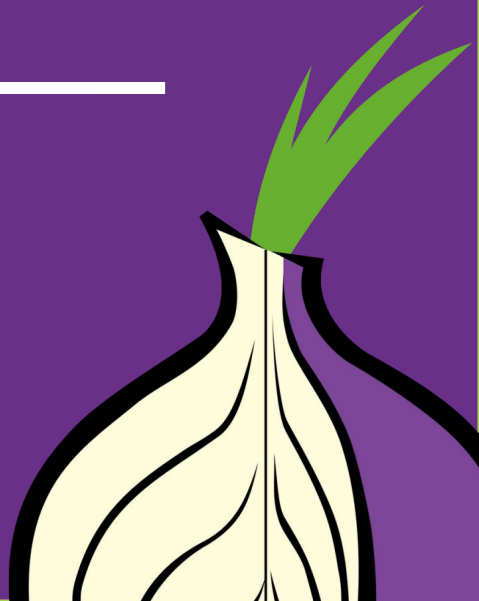
Legal resources

- The EFF Tor Legal FAQ answers many common questions: https://www.torproject.org/eff/tor-legal-faq.html.en
- It's important to respond to abuse complaints in a timely manner (usually within 24 hours).
- Abuse templates letters: https://trac.torproject.org/projects/tor/wiki/doc/TorAbuseTemplates

Tips for running an exit relay

- Get a separate IP for the relay and don’t use it for other services.
- Set up a Tor Exit Notice, so if someone checks your exit IP, they will easily know that it’s a Tor Exit.
- If you receive excessive complaints, consider running a Reduced Exit Policy.
- For more tips: https://blog.torproject.org/tips-running-exit-node

Running relays with others



Running a relay with others

- You can work with your university department, employer or institution, or an organization like Torservers.org
- Torservers.org is an independent, global network of organizations that helps the Tor network by running high bandwidth Tor relays.
- In many countries operating as a corporation instead of as an individual can also get you certain legal protections.

Relays associations

- It’s often advised to create some type of non-profit corporation. This is useful for having a bank account and shared ownership.
- To start a relay association, the most important thing is to have a group of people (3-5 suggested to start) interested in helping.
- For example: Torservers.org, Cold Hak, enn.lu, nos-oignons.

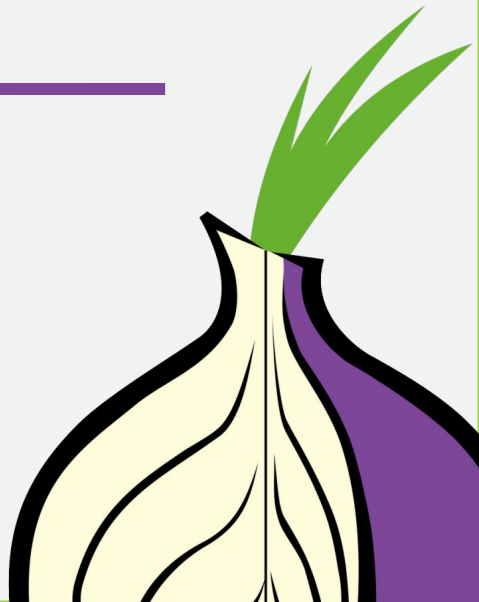
Running a relay with universities

- Universities are typically home to a reliable, robust, and well-equipped network.
- Many computer science departments and university libraries run relays, i.e., Massachussetts Institute of Technology (MIT CSAIL), Universitaet Stuttgart, the University of Waterloo.
- Start running a relay campaign in your university: https://www.eff.org/torchallenge/tor-on-campus.html

At your company or organization

- If you work at a Tor-friendly company or organization, that's another ideal place to run a relay.
- Companies like Brass Horn Communications, Quintex Alliance Consulting, and OmuraVPN
- And organizations like Digital Courage, Access Now, Derechos Digitales, and Lebanon Libraries in New Hampshire.

Bad relays



What is a bad relay?

- A bad relay is one that either doesn't work properly or tampers with our users' connections. This can be either through maliciousness or misconfiguration.
- For example: tampering with exit traffic in any way (including dropping accepted connections). Or, running HSDirs that harvest and probe .onion addresses

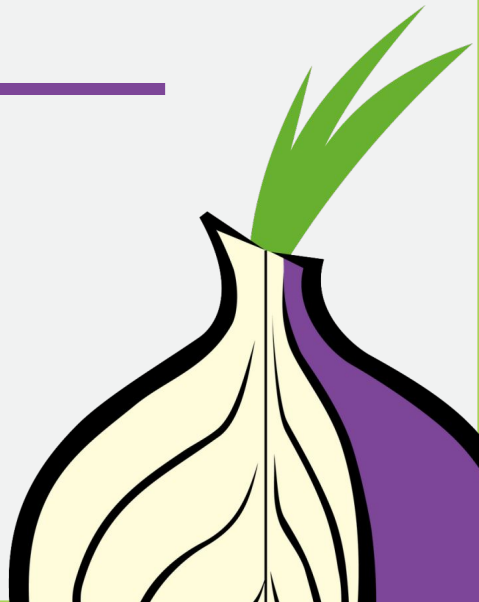
Reporting a bad relay

- Bad relays is also a private working group in Tor Project to detect misconfigured, malicious, or suspicious relay.
- Users can report bad relays sending an email to bad-relays@lists.torproject.org with the relay's IP address or fingerprint, what kind of behavior did you see, and any additional information it’s needed to reproduce the issue.

What happens to bad relays?

- After a relay is reported and we've verified the behavior we'll attempt to contact the relay operator.
- We'll flag it to prevent it from continuing to be used (BadExit, Invalid, Reject).
- The working group actively look for bad relays using open source tools like: exitmap, sysbilhunter.

How do I get help running a Tor relay?



Getting help

- Read the Tor Relay Guide documentation before:
- https://torproject.org/relay-guide
- Search the mailing list archive: tor-relays in https://lists.torproject.org
- Join the IRC channel: #tor-relays in irc.oftc.net
- Talk with our relay advocate: colin@torproject.org

Thank You!

Name: e-mail

Your PGP key fingerprint