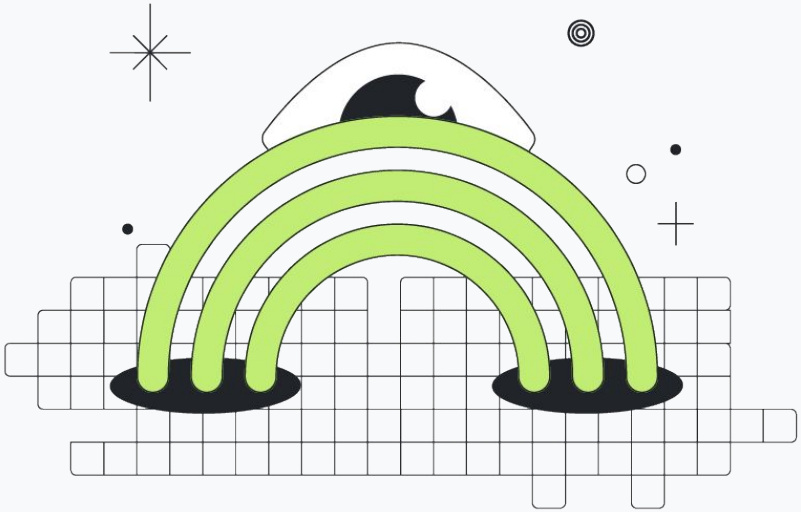
Understanding How Tor Works



Updated: 6 February 2025

1.
Origins of Tor

1995

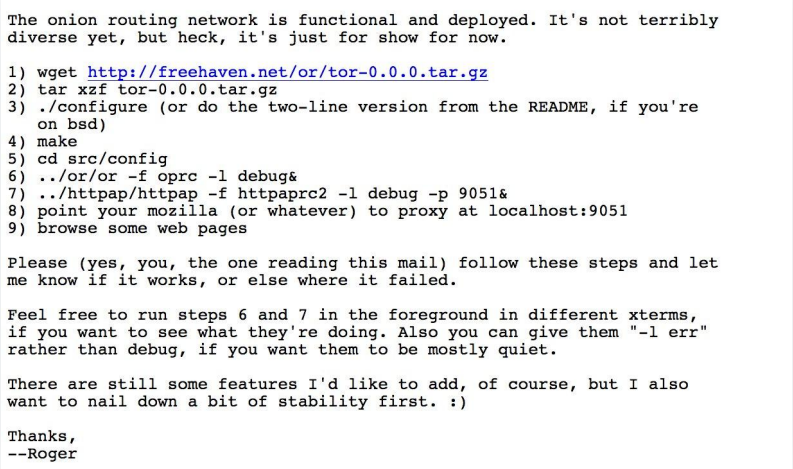
The concept of “onion routing” was invented in 1995 by Paul Syverson, David Goldschlag, and Michael Reed, then researchers at the **US Naval Research Laboratory (NRL)**.

Early 2000s

Roger Dingledine, a recent MIT graduate at the time, began working on an **onion routing project** with Paul Syverson at the NRL. Soon after, Roger's MIT classmate, Nick Mathewson, joined the research effort.

2002

To distinguish it from other onion routing projects, Roger called theirs **Tor**; in other words, ***The* Onion Routing** (not Router!). The first version of the software was deployed in **20 September 2002** as free and open source.



```
The onion routing network is functional and deployed. It's not terribly
diverse yet, but heck, it's just for show for now.

1) wget http://freehaven.net/or/tor-0.0.0.tar.gz
2) tar xzf tor-0.0.0.tar.gz
3) ./configure (or do the two-line version from the README, if you're
   on bsd)
4) make
5) cd src/config
6) ../or/or -f oprc -l debug&
7) ../httpap/httpap -f httpaprc2 -l debug -p 9051&
8) point your mozilla (or whatever) to proxy at localhost:9051
9) browse some web pages

Please (yes, you, the one reading this mail) follow these steps and let
me know if it works, or else where it failed.

Feel free to run steps 6 and 7 in the foreground in different xterms,
if you want to see what they're doing. Also you can give them "-l err"
rather than debug, if you want them to be mostly quiet.

There are still some features I'd like to add, of course, but I also
want to nail down a bit of stability first. :)

Thanks,
--Roger
```

2006

To maintain the development of Tor, Roger and Nick pursued funding and registered a **501(c)(3) nonprofit** organization **The Tor Project Inc.** in 2006.

A Growing Project

- The Tor Project, as a non-profit, maintains the development of the **Tor network** and **Tor Browser**.
- The organization also works to:
  - Combat censorship of Tor worldwide;
  - Maintain a community of Tor relay operators;
  - Run trainings on Tor for activists, journalists, and human rights defenders.

2.
Understanding Tor:
A Comparison with VPNs

When Browsing the Internet Regularly

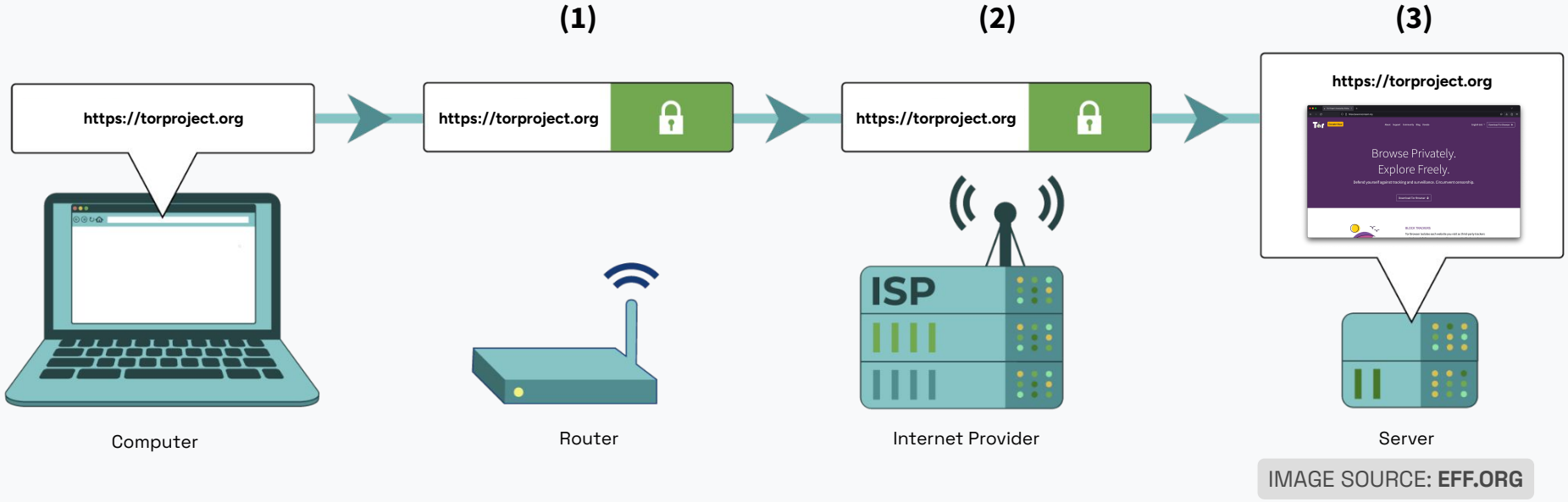


IMAGE SOURCE: **EFF.ORG**

When Browsing the Internet Regularly

Your request to connect to the Tor Project's website goes through a simple journey:

1. First it goes through your **WiFi router**.
2. Your WiFi router is connected to your **Internet Service Provider** (or ISP, the company from whom you purchase Internet like Vodafone, Zain, Orange, Telkom Kenya, etc.);
3. Your ISP then connects you to the **website** you wish to visit.

See next slide for reference.

When a Website is Censored

- Since your ISP is able to see which websites and applications you are requesting to visit, it is able to **block** your access to them.
- ISPs worldwide will often block access to the certain websites or applications (both or all!), perhaps at the order of a government.
- In order to bypass this censorship, you need to “pretend” that you’re visiting an unblocked location first, then from that location head to the website you initially intended to visit.
- **This is how VPNs work!** When you turn on VPN on your laptop, you tell your ISP that you wish to visit a VPN server located in a certain country which is usually not blocked by your ISP.

Connecting to a Website Through a VPN

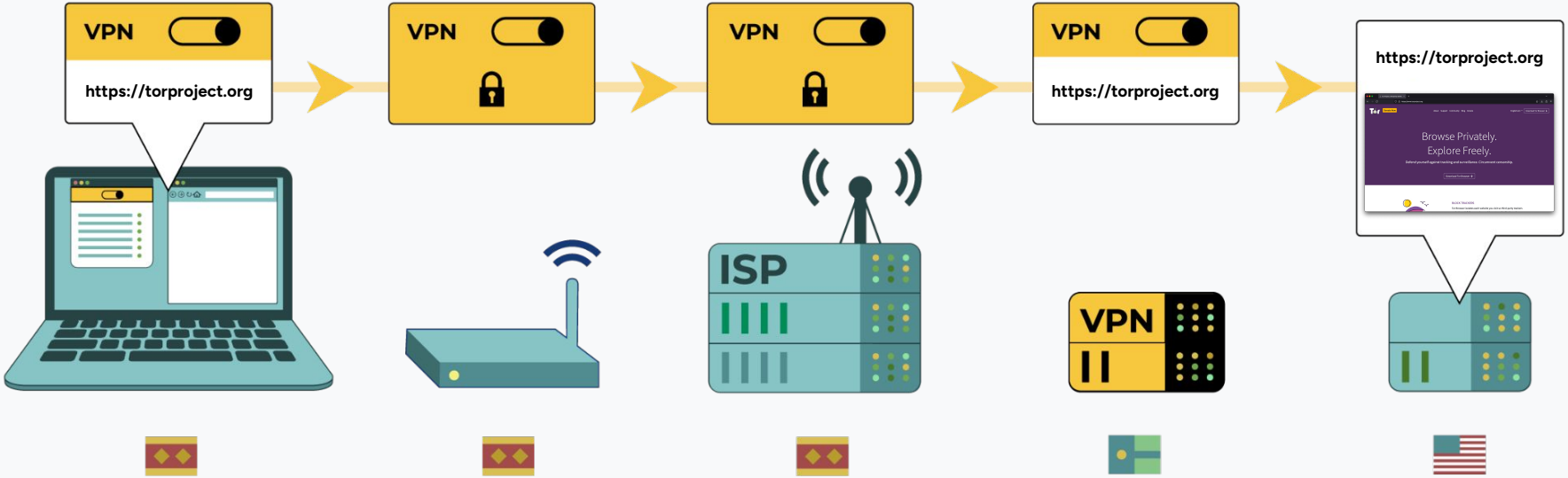


IMAGE SOURCE: **EFF.ORG**

Privacy by Trust

- When using a VPN to bypass internet censorship, you are **transferring your trust** from the ISP to the the VPN operator (often a private company).
- VPN operators tend to **collect personal data** about its users (credit card information, IP addresses, online activity, etc.) and **sell this data** to third parties. This data is also subject to **government search warrants**.

Connecting to a Website Through Tor

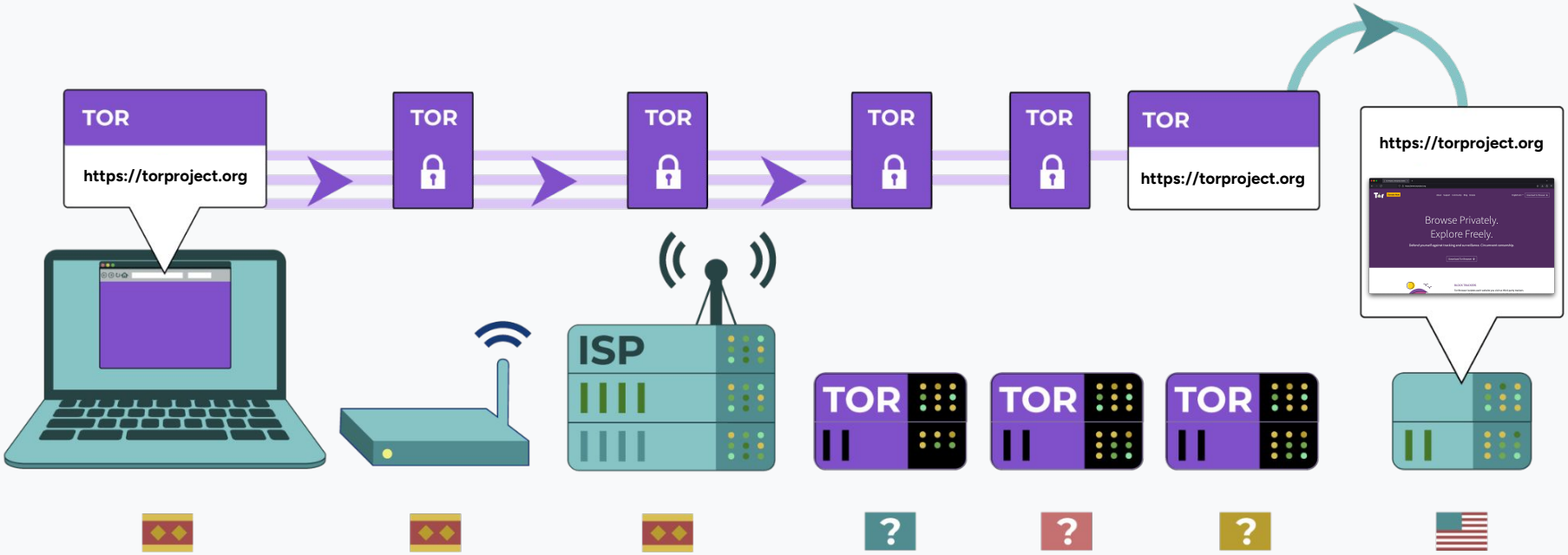


IMAGE SOURCE: **EFF.ORG**

VPN vs. Tor

- When using Tor, your traffic is routed through **3 servers instead of 1** such as through a VPN.
- Your traffic is **encrypted 3 times** and each server on the Tor network decrypts a layer.
- Tor servers are run entirely by volunteers instead of private corporations which tend to profit off of user data. Tor is therefore **decentralized** (VPNs aren't).

Privacy By Design

- Tor is completely **open source and free***, enabling privacy and security on the network through transparency of operation. Not all VPNs are open source or undergo independent security auditing.
- This makes a Tor connection **private by design**. Tor does not know who you are, where you are connecting from, and where you're going. No private data is stored.

** Free as in gratis, not freemium.*

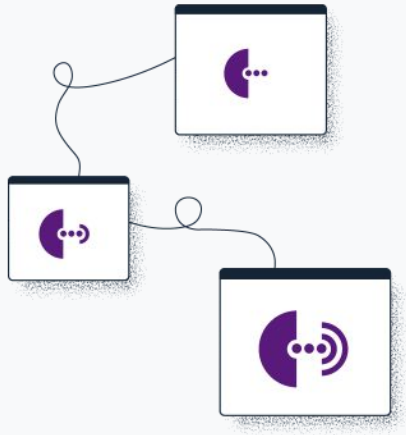
3.
A Deeper Look Into Tor

Anonymity Network

- When connecting to the Internet, our data can be **intercepted and surveilled** by hackers, sysadmins, state intelligence agencies.
- It's therefore susceptible to **identification** (i.e. it's possible to know *x* person visited *y* website or application).
- Tor modifies how we connect to the internet by routing our traffic through **3 volunteer-run servers**, and **encrypting the data 3 times**.
- Each server decrypts a layer ⇒ "onion peel" ⇒ "onion routing."

So What is Tor?

- Tor is a **free and open source software** that provides anonymous routing on the Internet.
- Tor runs on the network of **volunteer-run servers** (relays).
- To connect through Tor, people can **download Tor applications** that let you connect to the Tor network of servers (such as the Tor Browser).
- Often we say “Tor” just to talk about the non-profit “The Tor Project.”



Before We Start

- In this section, you'll encounter several technical terms referring to Tor servers, such as "server," "node," and "relay." Essentially, **they all mean the same thing**.
- There are different **types of relays**, mainly: “entry” or “guard” relay, “middle” relay, and “exit” relay. You will also see the term “bridges,” which are also a type of Tor relay. We will explain bridges separately.

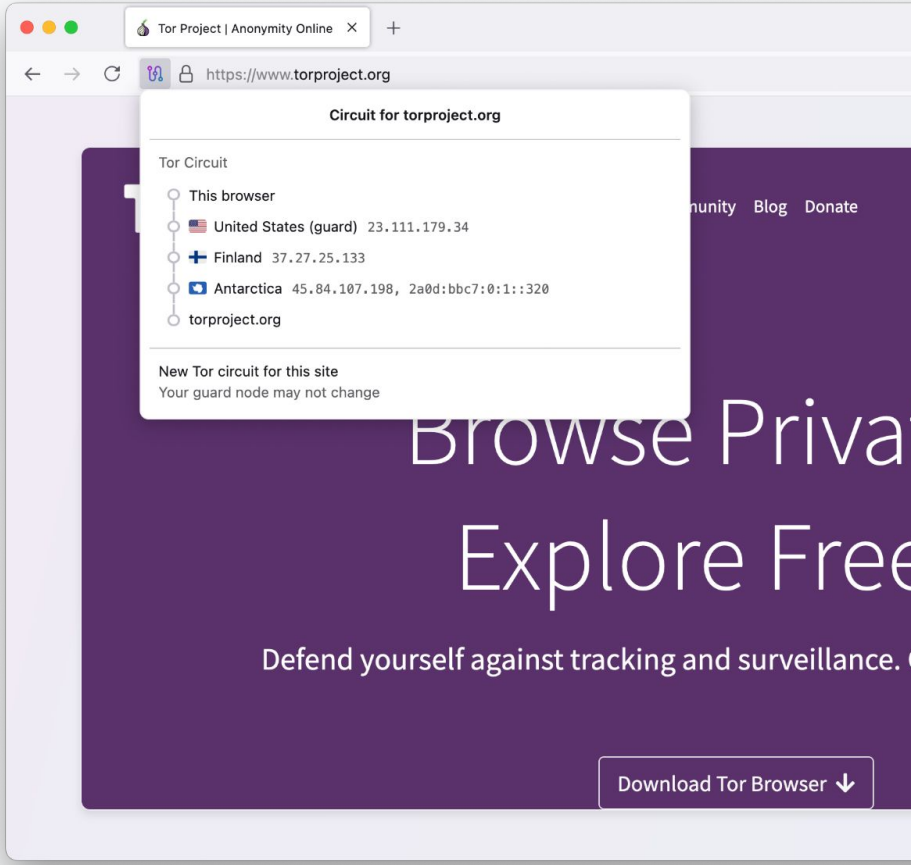
3.1.
Relays

Introduction to Tor Relays

- Tor relays are called as such since they pass a user's traffic from one server to another.
- Tor relays are distributed are around the world, and anyone can join by deploying their own Tor server:
  - You can choose to be part of the Tor network by deploying your own relay: https://community.torproject.org/relay/
- **Tor is not a peer-to-peer (P2P) program like BitTorrent!**

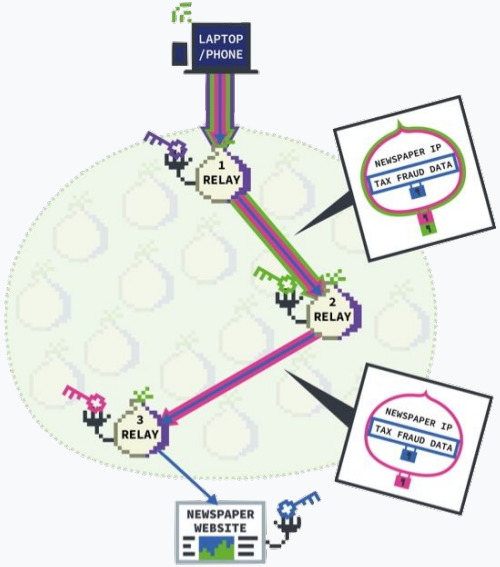
Types of Relays

- The first server in the three-hop route is called an entry or **guard relay**.
- The second is aptly called a **middle relay**.
- The third and final server is called an **exit relay** since it exits the user from the Tor network and connects them to their intended destination.
- The three-hop route is called a **Tor Circuit**.

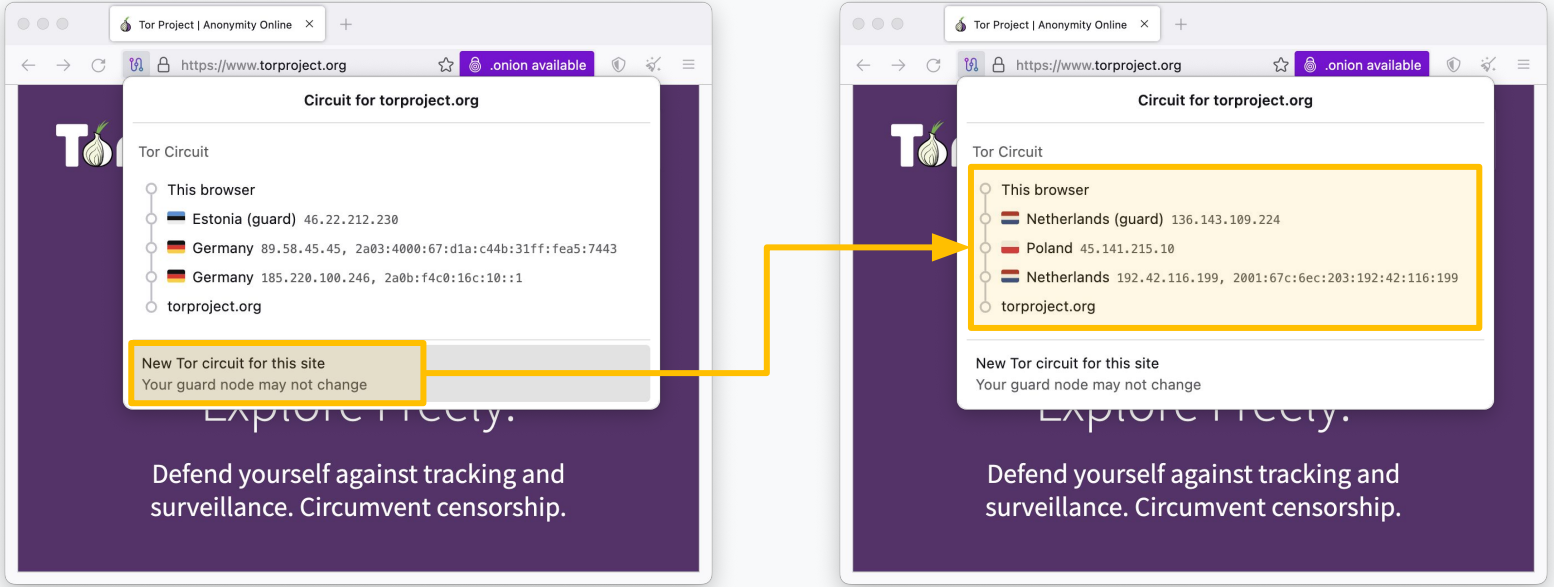


Why Three Relays?

- **Why not fewer?** A two-hop circuit might improve speed but would significantly reduce security. With only two relays, someone with enough resources could easily correlate a user's identity with their destination. The middle relay in a three-hop circuit acts as a critical buffer, making such attacks much harder.
- **Why not more?** Adding additional relays would increase network load and reduce connection speeds without, as far as we know, offering any meaningful improvement in security or anonymity. A slower network reduces usability, which could discourage adoption and weaken the system overall.

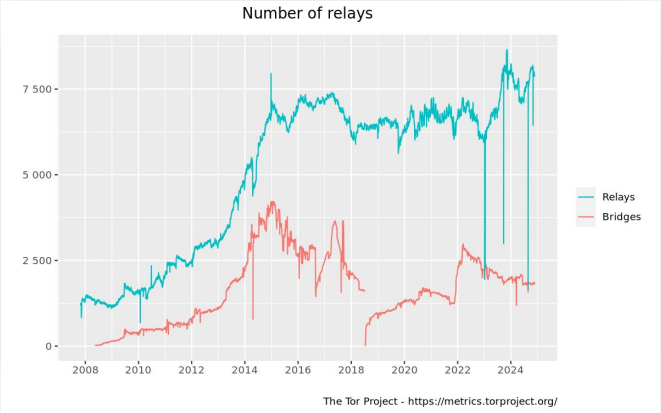


Displaying and Changing the Tor Circuit



A Growing Network of Volunteers

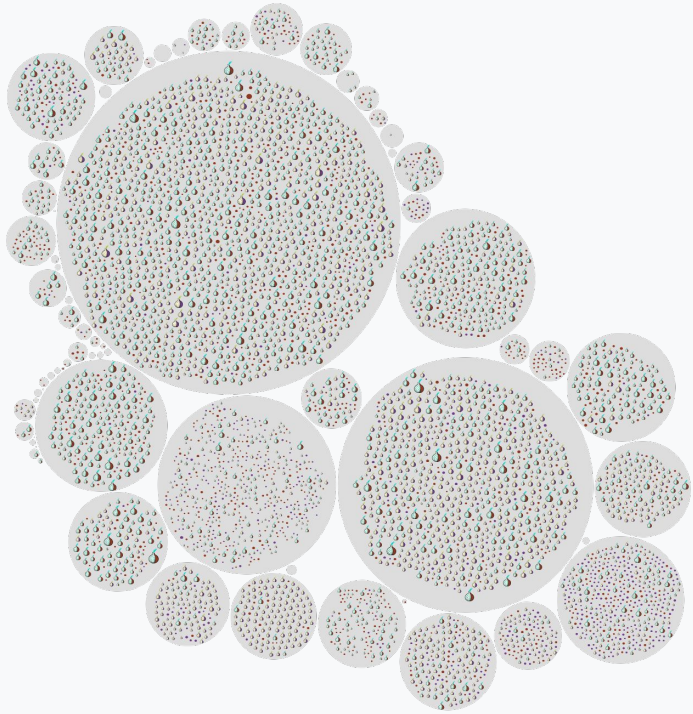
- Tor relays are run by volunteers from **around the world** which makes it a decentralized network.
- As of April 2024, we count: **7,880+ relays** and **1,820+ bridges**.
- Relay operators form a large, active community that meets regularly both online and in person.

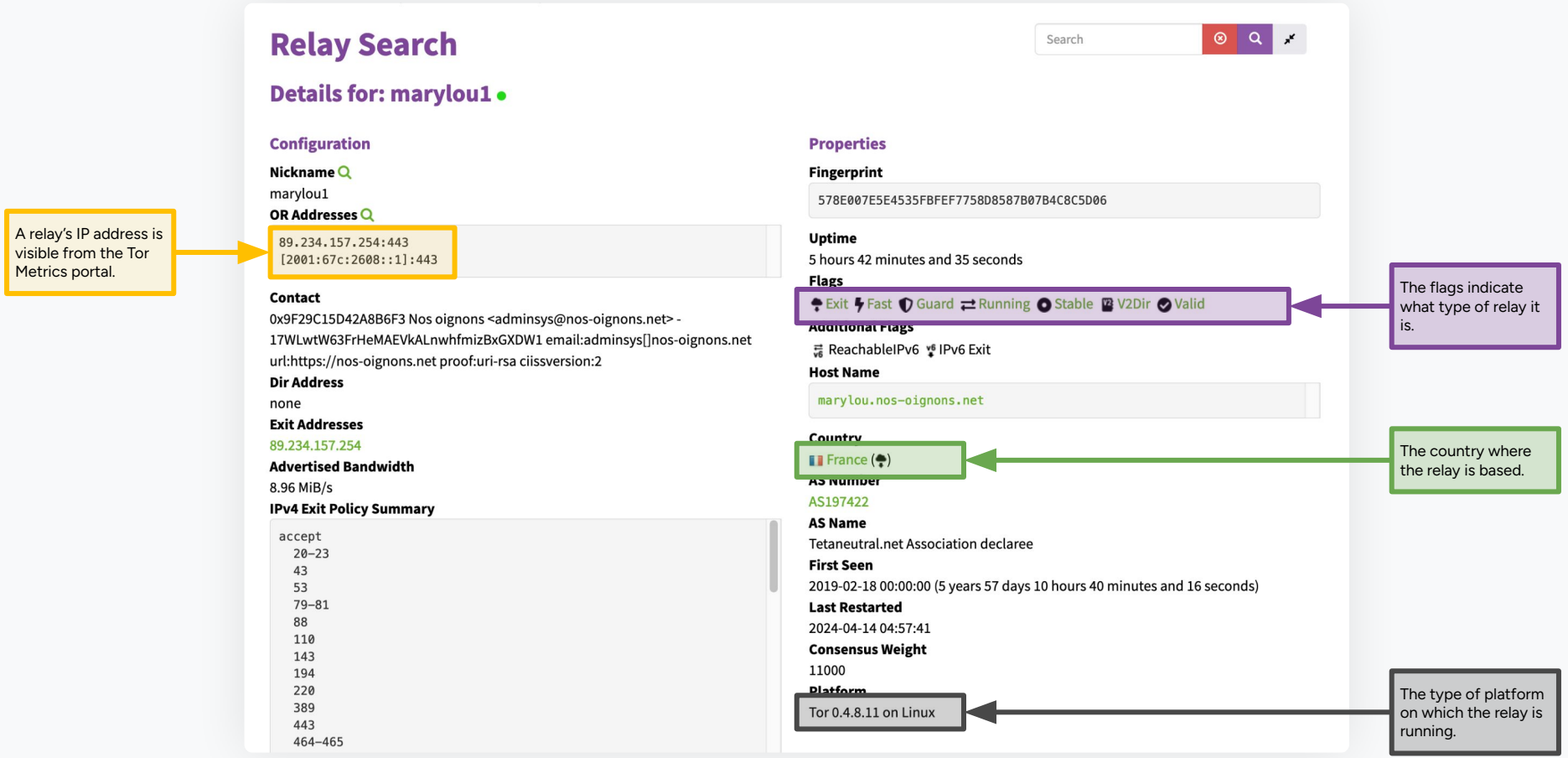


Relays form the backbone of the Tor network, without volunteers Tor would not be possible.

A Public Directory of Relays

- Fun fact: all Tor relays, i.e. the servers that make up the Tor network, are **publicly listed** on Tor's website.
- This is a conscious decision made by the Tor Project to increase transparency of the network and thus trust in it.
- Relays have their IP addresses publicly listed, while bridges keep their addresses **hidden** ⇒ Bridges are effectively private relays.
- To search through relays, simply visit the Tor Metrics portal: https://metrics.torproject.org/rs.html




Relay Search
Search
Details for: marylou1
Configuration
Nickname
marylou1
OR Addresses
89.234.157.254:443
[2001:67c:2608::1]:443
Contact
0x9F29C15D42A8B6F3 Nos oignons <adminsys@nos-oignons.net> - 17WLwtW63FrHeMAEVkALnwhfmizBxGXDW1 email:adminsys[]nos-oignons.net url:https://nos-oignons.net proof:uri-rsa ciissversion:2
Dir Address
none
Exit Addresses
89.234.157.254
Advertised Bandwidth
8.96 MiB/s
IPv4 Exit Policy Summary
accept
20–23
43
53
79–81
88
110
143
194
220
389
443
464–465
Properties
Fingerprint
578E007E5E4535FBFEF7758D8587B07B4C8C5D06
Uptime
5 hours 42 minutes and 35 seconds
Flags
Exit Fast Guard Running Stable V2Dir Valid
Additional Flags
ReachableIPv6 IPv6 Exit
Host Name
marylou.nos-oignons.net
Country
France
AS Number
AS197422
AS Name
Tetaneutral.net Association declaree
First Seen
2019-02-18 00:00:00 (5 years 57 days 10 hours 40 minutes and 16 seconds)
Last Restarted
2024-04-14 04:57:41
Consensus Weight
11000
Platform
Tor 0.4.8.11 on Linux
A relay's IP address is visible from the Tor Metrics portal.
The flags indicate what type of relay it is.
The country where the relay is based.
The type of platform on which the relay is running.

3.2.
Bridges

Bridges

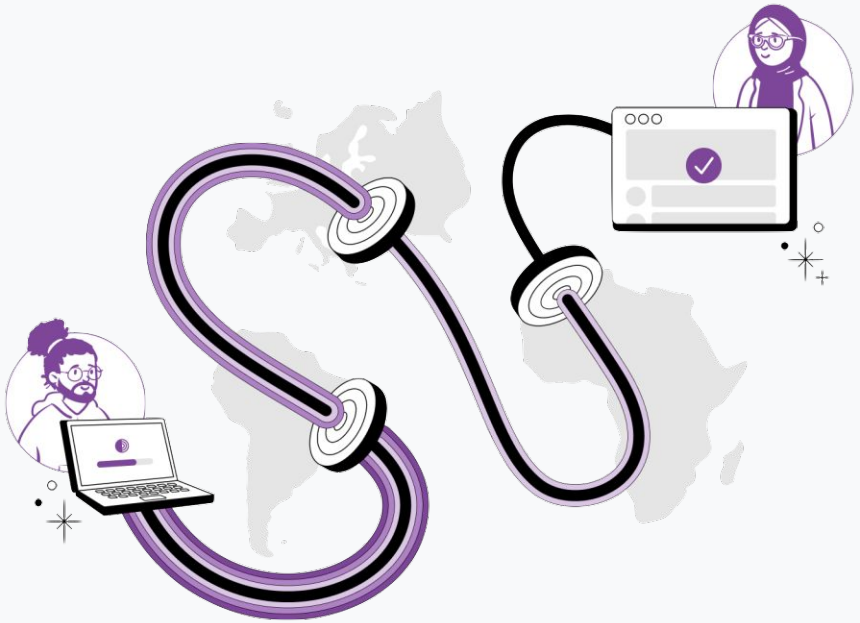
- A bridge provides an alternative way to connect to the Tor network. It's basically a Tor entry relay, but its IP address is **not listed** on the public directory (the Tor Metrics portal). This makes it harder for Internet Service Providers (ISPs) and governments to block access to the bridge.
- **What's the use of bridges?** Bridges are an anti-censorship feature and we recommend users to connect through a bridge rather than a regular entry relay **when Tor is blocked** in a user's country or region.
- Most bridges add an additional layer of masking called **Pluggable Transports**. Pluggable Transports disguise a bridges' Tor traffic by making it look like a regular connection rather than a Tor connection, adding another layer of obfuscation.

Pluggable Transports

Anyone surveilling your internet traffic might be able to recognize patterns that indicate that you're connecting to Tor, and block your access to it (don't worry, they won't know what you intended to visit over Tor). Pluggable Transports prevent this by transforming Tor's traffic to look like something else entirely. The main types of pluggable transports on Tor are:

1. **obfs4:** makes Tor traffic look like random encrypted traffic (like nothing specific).
2. **meek-azure:** makes it look like you're connecting to a Microsoft service.
3. **snowflake:** makes your traffic appear that you're connecting to a videoconference (channels your traffic through volunteer-run proxies using WebRTC). For more on Snowflake: https://snowflake.torproject.org.
4. **WebTunnel:** mimics encrypted web traffic (HTTPS).

Thank you!



The Tor Project
Support Channels

Signal: https://signal.me/#p/+17787431312

Email: frontdesk@torproject.org

WhatsApp: https://wa.me/447421000612

Telegram: https://t.me/torprojectsupportbot

Forum: https://forum.torproject.org