Censorship Circumvention with Tor

Alexander Færøy

November 1, 2019

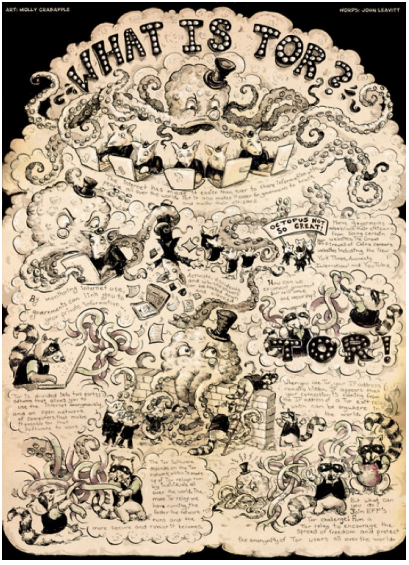
Driving IT

About Me

- Core Developer at The Tor Project since early 2017.
- Free Software developer since 2006.
- Worked with distributed systems in the Erlang programming language, WebKit-based mobile browsers, embedded development, and software development consulting.
- Co-organizing the annual Danish hacker festival BornHack.

What is Tor?

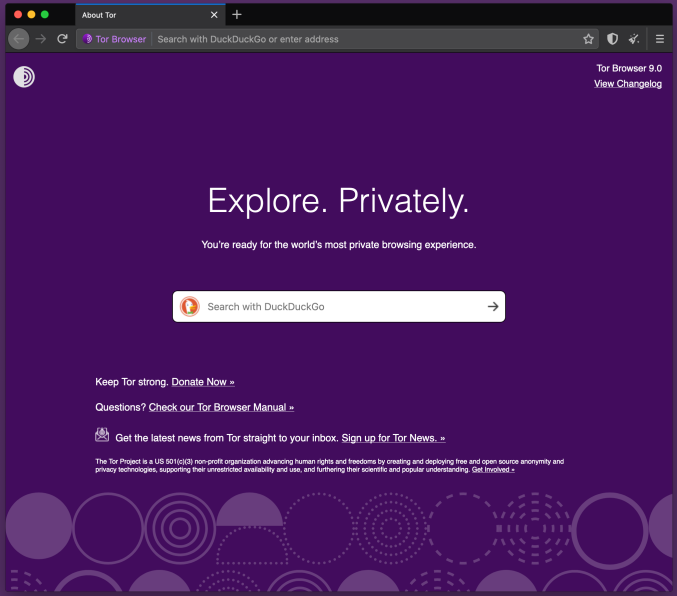
- Online anonymity, and censorship circumvention.
  - Free software.
  - Open network.
- Community of researchers, developers, users, and relay operators.
- U.S. 501(c)(3) non-profit organization.

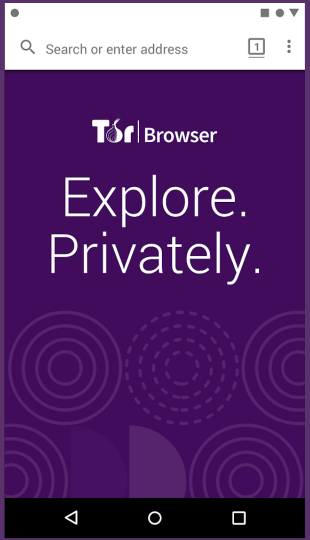


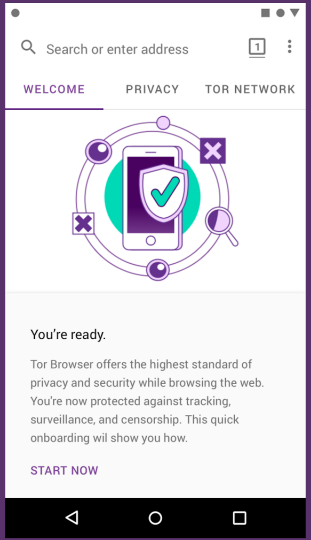
History

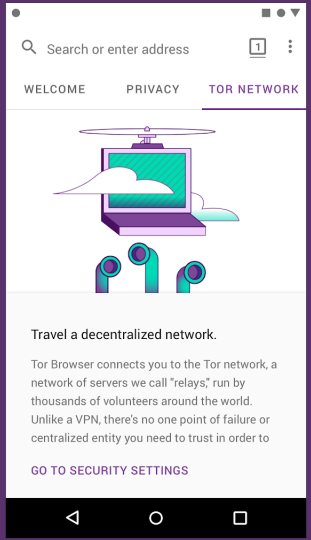
1990s	Onion routing for privacy online.
Early 2000s	Working with the U.S. Naval Research Laboratory.
2004	Sponsorship by the Electronic Frontier Foundation.
2006	The Tor Project, Inc. became a non-profit.
2007	**Expansion to anti-censorship.**
2008	Tor Browser development.
2010	The Arab spring.
2013	The summer of Snowden.
2018	**Dedicated anti-censorship team created.**

Somewhere between 2,000,000 and 8,000,000 daily users.

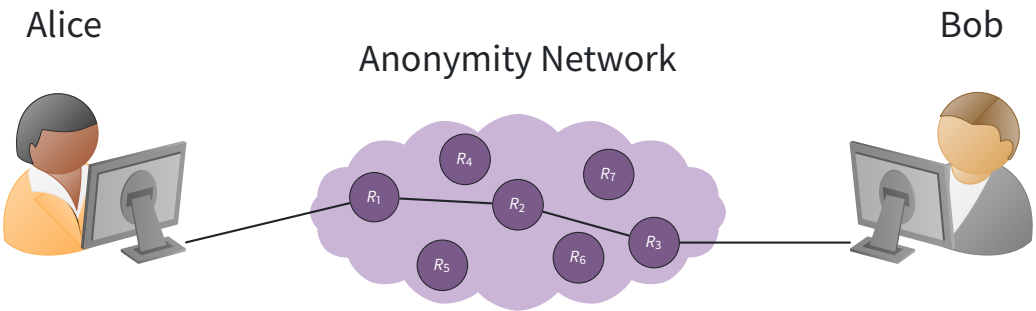

About Tor
Tor Browser
Search with DuckDuckGo or enter address
Tor Browser 9.0
View Changelog
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Keep Tor strong. Donate Now »
Questions? Check our Tor Browser Manual »
Get the latest news from Tor straight to your inbox. Sign up for Tor News. »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »


Search or enter address
Tor Browser
Explore.
Privately.


Search or enter address
WELCOME
PRIVACY
TOR NETWORK
You're ready.
Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding wil show you how.
START NOW

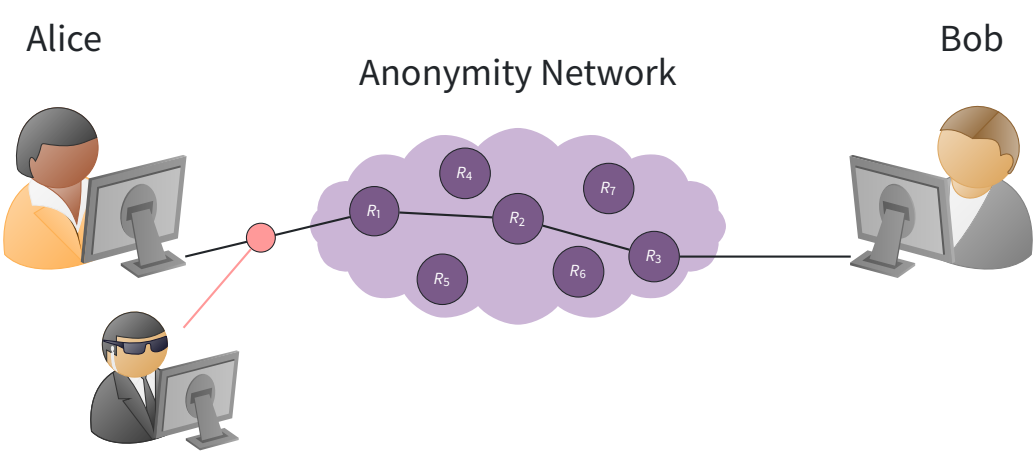

Search or enter address
WELCOME
PRIVACY
TOR NETWORK
Travel a decentralized network.
Tor Browser connects you to the Tor network, a network of servers we call "relays," run by thousands of volunteers around the world. Unlike a VPN, there's no one point of failure or centralized entity you need to trust in order to
GO TO SECURITY SETTINGS

Threat Model

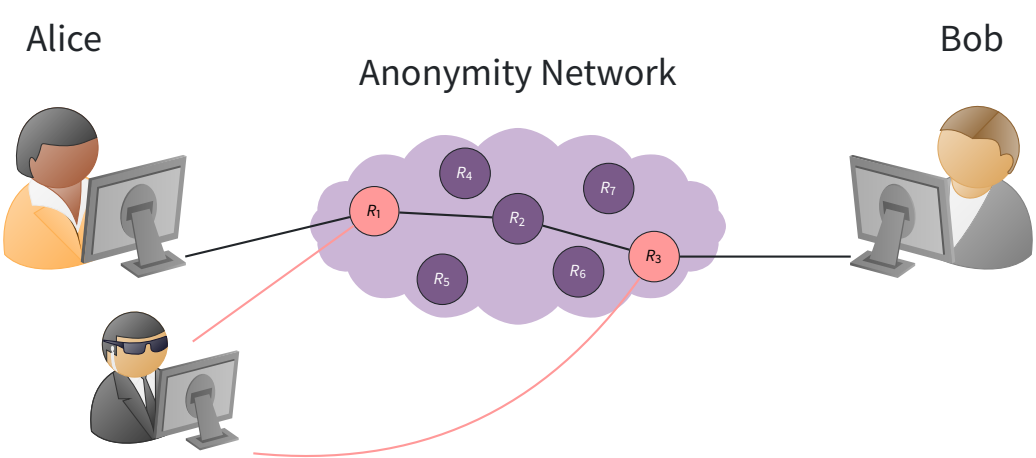


What can the attacker do?

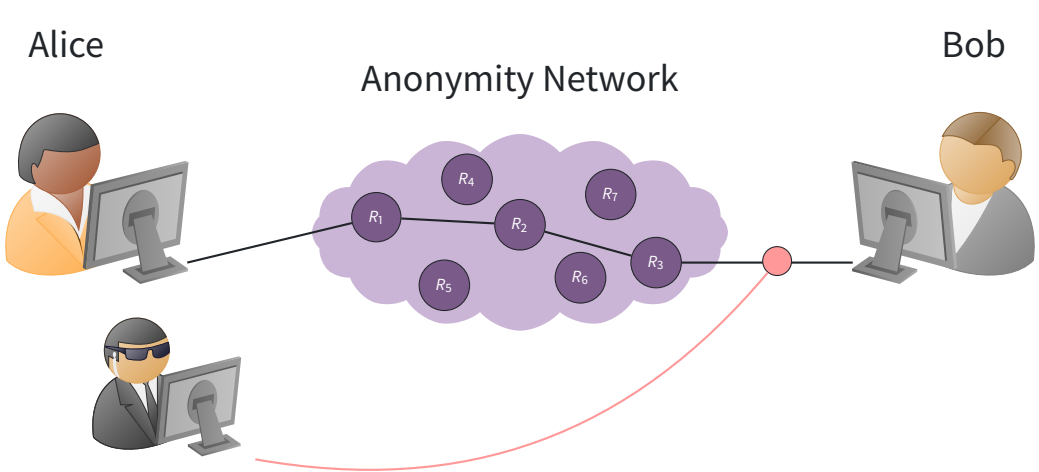
Threat Model



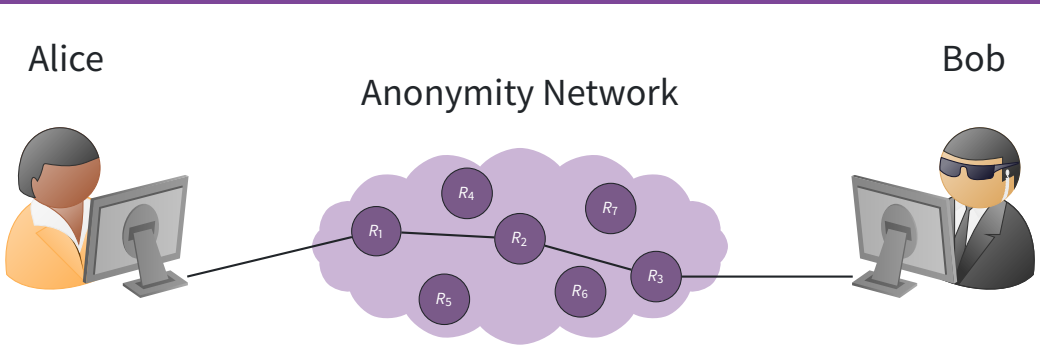
Threat Model



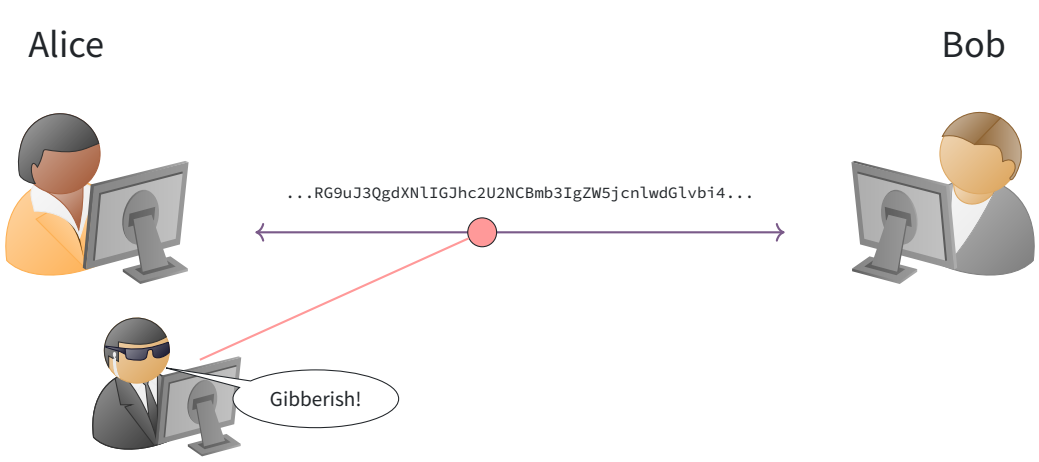
Threat Model



Threat Model



Anonymity isn't Encryption



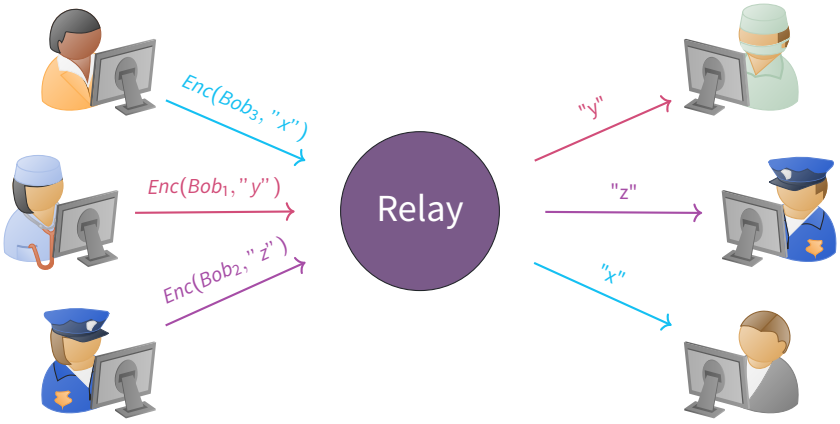
Encryption just protects contents.

Metadata

"We Kill People Based on Metadata."

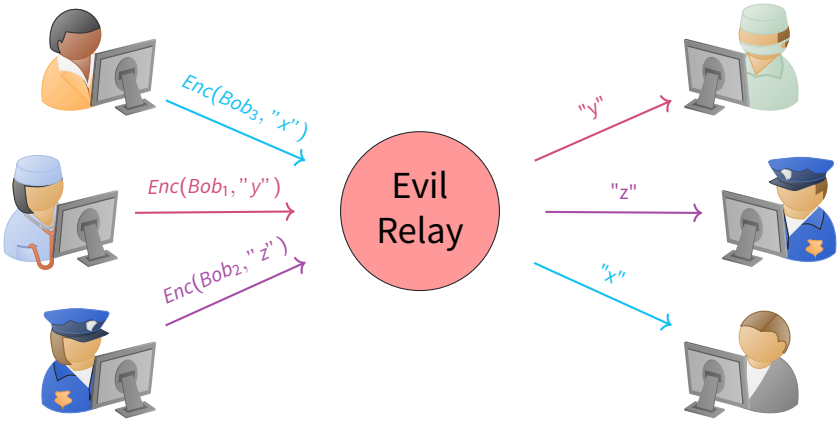
—Michael Hayden, former director of the NSA.

A Simple Design

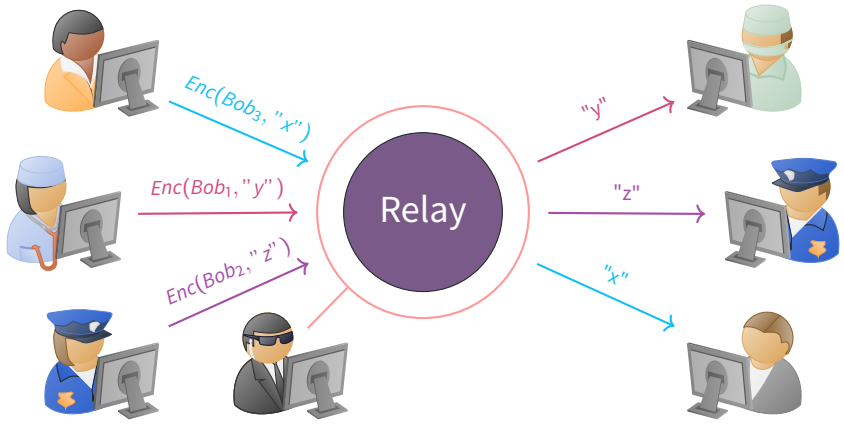


Equivalent to some commercial proxy providers.

A Simple Design

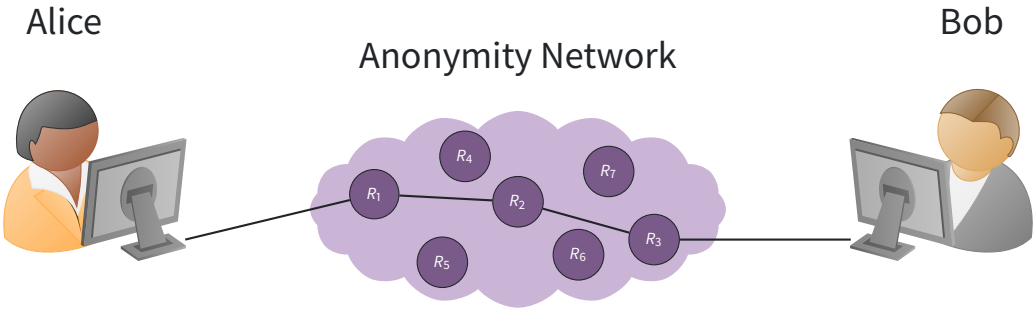


A Simple Design



Timing analysis bridges all connections going through the relay.

The Tor Design



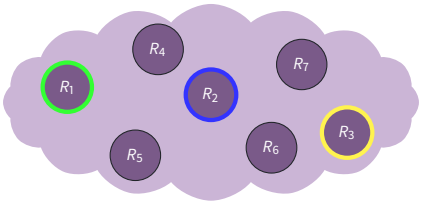
Add multiple relays so that no single relay can betray Alice.

The Tor Design

Alice

Anonymity Network

Bob



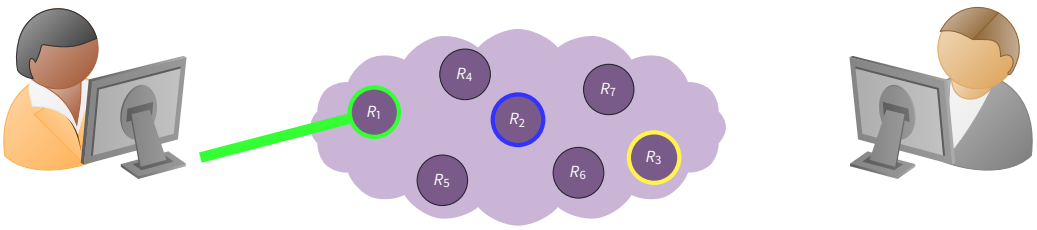
Alice picks a path through the network: R_1, R_2, and R_3 before finally reaching Bob.

The Tor Design

Alice

Anonymity Network

Bob



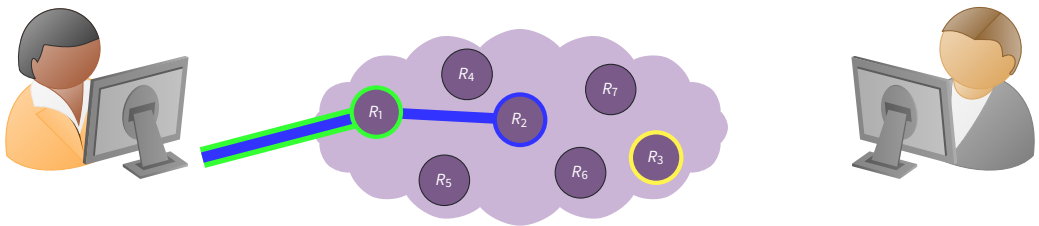
Alice makes a session key with R_1.

The Tor Design

Alice

Anonymity Network

Bob



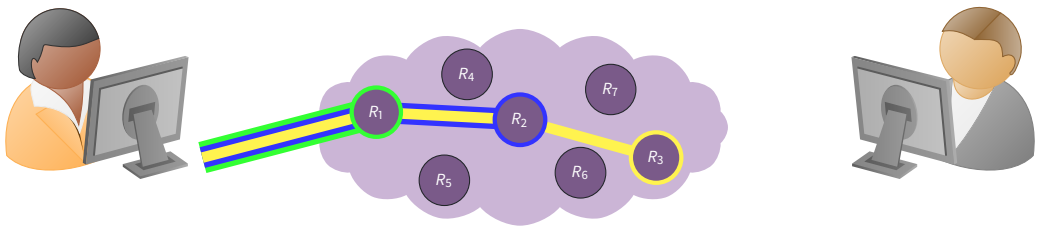
Alice asks R_1 to extend to R_2.

The Tor Design

Alice

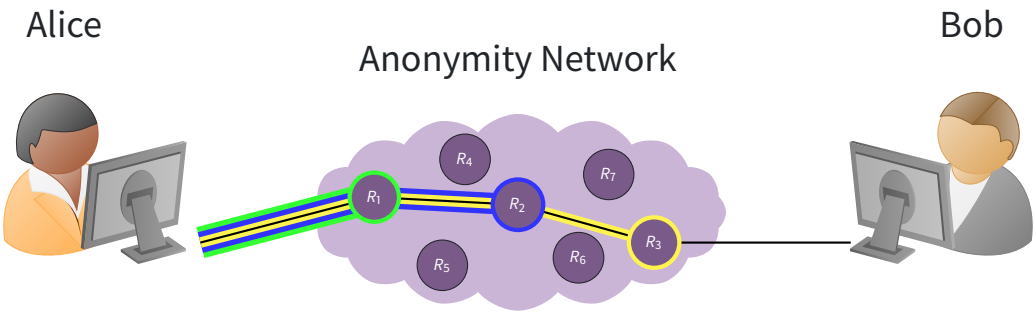
Anonymity Network

Bob



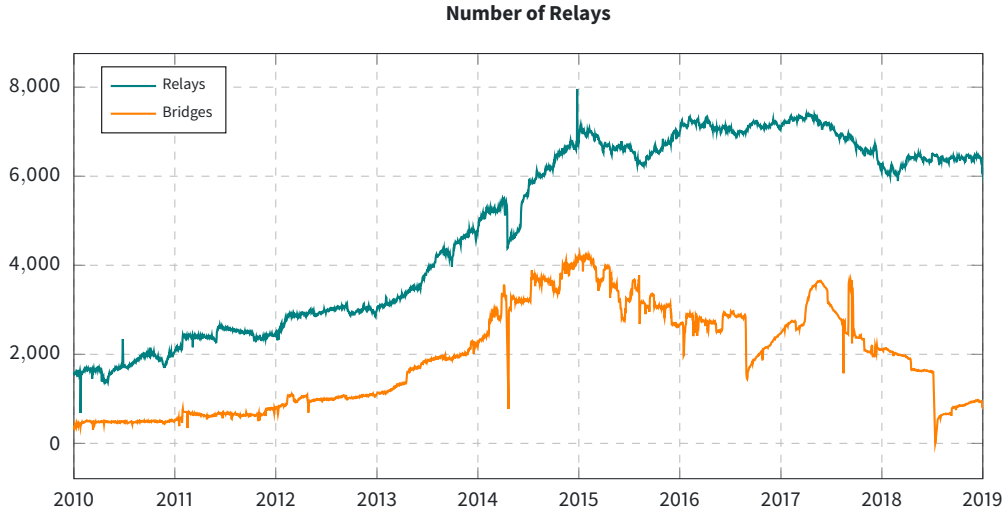
Alice asks R_2 to extend to R_3.

The Tor Design



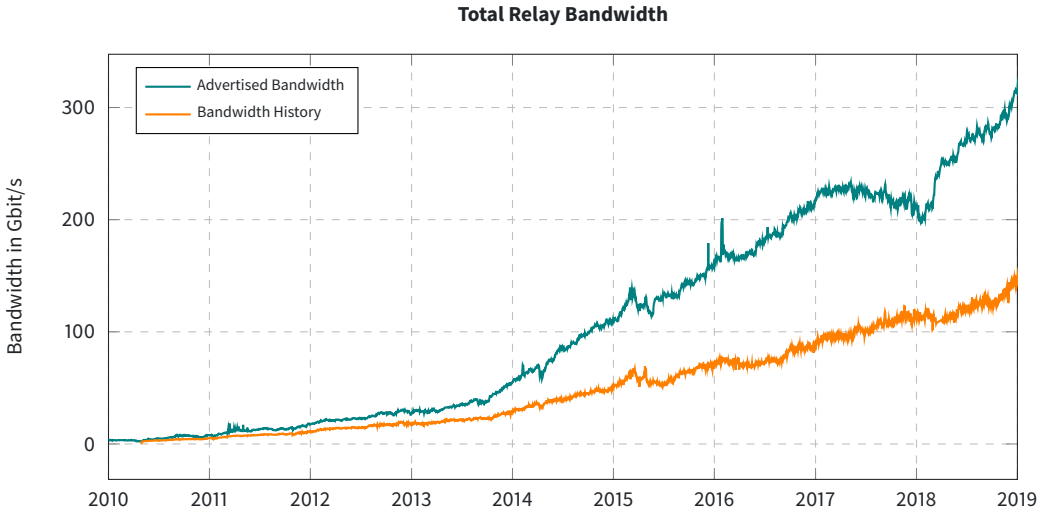
Alice finally asks R_3 to connect to Bob.

The Tor Network



Source: metrics.torproject.org

The Tor Network



Source: metrics.torproject.org

The Tor Network

Tor's **safety** comes from **diversity**:

1. Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation.
2. Diversity of users and reasons to use it. 50,000 users in Iran means almost all of them are normal citizens.

Research problem: How do we measure diversity over time?

I live in Iran and I have been using Tor for censorship circumvention. During political unrest while the government tightens grip on other censorship circumvention alternatives, **Tor with obfuscation plugins remains the only solution.**

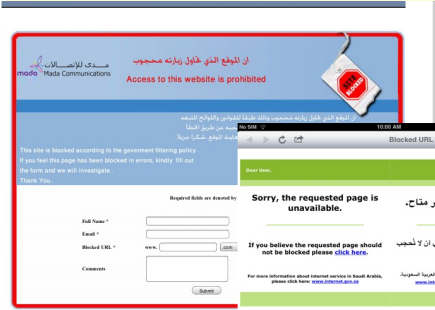
Tor changed my personal life in many ways. **It made it possible to access information on Youtube, Twitter, Blogger and countless other sites.** I am grateful of Tor project, people working on it as well as people running Tor nodes.

—Anonymous Tor User.

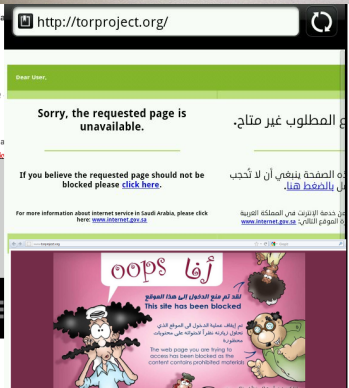

يالله بالستر ...!
تصفح بأمان!
عذراً، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الانترنت وسيلة لتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي تريد بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.
إذا كانت لديك وجهة نظر مختلفة، الرجاء النقر هنا.
Surf Safely!
This website is not accessible in the UAE.
The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the 'Internet Access Management Regulatory Policy' of the Telecommunications Regulatory Authority of the United Arab Emirates.
If you believe the website you are trying to access does not contain any such content, please click here.
© 2009 zammitcre FZ LLC.


خطر!
تصفح بأمان!
تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي تريد بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.
إذا كانت لديك وجهة نظر مختلفة، الرجاء النقر هنا.
Surf Safely!
This website is not accessible in the UAE.
BOMB
Site is now TRUSTED


هذا الموقع محظور
This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.
إذا كنت ترغب في إضافة النظر في تصنيف هذا الموقع، يرجى التفضل بتعبئة استمارة الملاحظات
If you would like the classification on this site to be reviewed, please fill in and submit the Feedback Fo


Access Denied
our request was denied because of its content categorization: "Computers/Internet;Proxy Avoida


عزيزي العميل : تم حجب هذا الموقع بناء على القوانين والقوانين
بأن هناك خطأ يرجى إرسال رسالة على البريد الالكتروني unblock.kw@kw.zain.com مع ذكر عنوان الموقع الذي تم حجبه.
Dear Customer: This site has
categorizing this site, please


http://torproject.org/
Dear User,
Sorry, the requested page is unavailable.
If you believe the requested page should not be blocked please click here.
For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
عزيزي المستخدم،
عفواً، الموقع المطلوب غير متاح.
إذا كنت ترى أن هذه الصفحة ينبغي أن لا تُحجب تفضل بالضغط هنا.
مزيد من المعلومات عن خدمة الإنترنت في المملكة العربية السعودية: www.internet.gov.sa

مدى للاتصالات
mada Mada Communications
ان الموقع الذي حاول زيارته محجوب
Access to this website is prohibited
This site is blocked according to the government filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate.
Thank You
Required fields are denoted by
Full Name *
Email *
Blocked URL *
Comments
Submit

9:28 AM
Site Blocke...
http://torproject.org/
Dear User,
Site Blocked
This web site has been blocked for violating regulations and laws of Kingdom of Bahrain.
If you believe the requested page should Not be blocked please click here.
الموقع محظور
هذا الموقع مغلق لمخالفته الأنظمة والقوانين في مملكة البحرين.
إذ كنت ترى أن هذه الصفحة ينبغي أن لا تحجب تفضل بالضغط هنا.

oops! أوقا
This site has been blocked
The web page you are trying to access has been blocked as the content contains prohibited materials

Du var på vej ind på en ulovlig hjemmeside

Vi vil meget gerne hjælpe dig med at finde den film eller serie, du søger.

Søg med FilmFinder →

Hvis du er på udkig efter musik, bøger eller møbler

Gå til SHARE WITH CARE →

SHARE WITH CARE

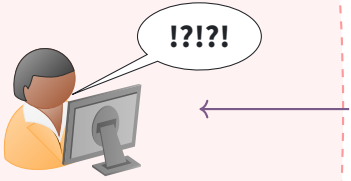
Hjemmesiden er blevet blokeret, fordi den er dømt ulovlig ved en dansk domstol. Brug Share With Care til at finde det, du leder efter, lovligt. På den måde passer du både på dig selv og på kulturen. **Læs mere om Share With Care**

Introduction to Censorship

Censored Region

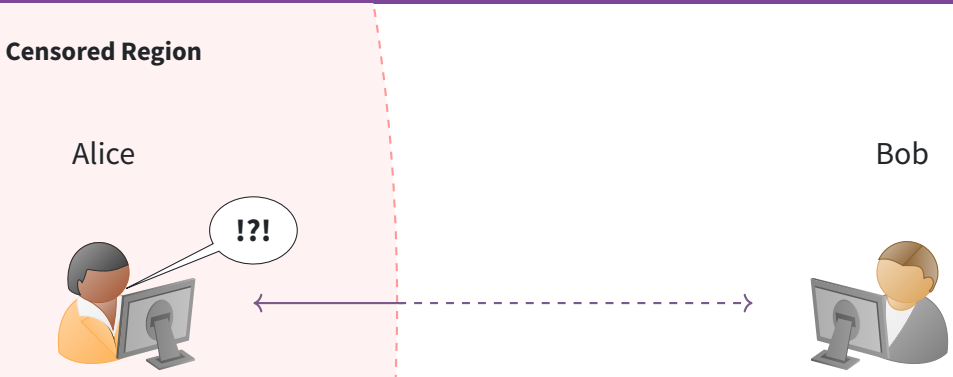
Alice

Bob



Alice is unable to reach Bob.

Introduction to Censorship



Alice can reach Bob, but their connection is throttled.

Introduction to Censorship

Censored Region

Alice

Bob

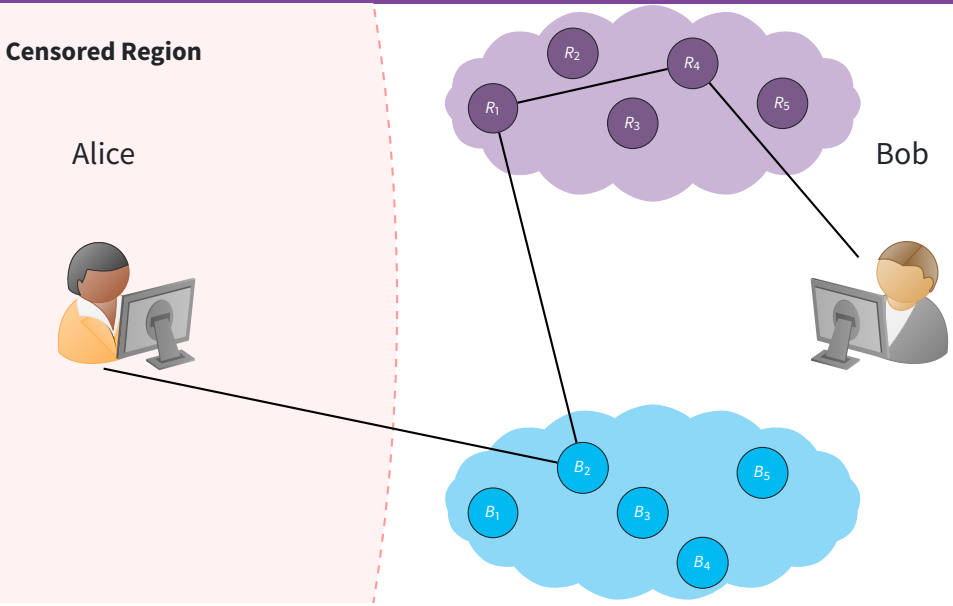
Alice can reach Bob because the censor thinks Bob is fine.

Anti-censorship Strategies

1. Censors will apply censorship to **all** relays in the network and effectively block access to the Tor network.
2. Censors will apply censorship to **known** bridges.

Solution: We make it difficult to find and block bridges and we make it difficult to learn if a given connection is between a Tor user and an entry-point into the Tor network.

Bridges



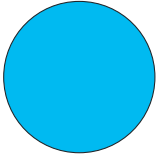
Bridges

Censored Region

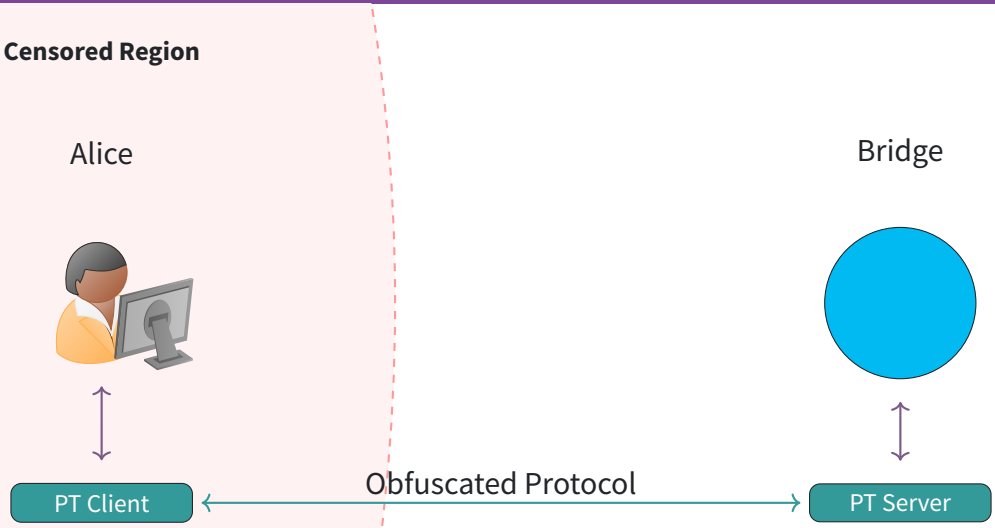
Alice

Tor Protocol

Bridge



Bridges and Pluggable Transports



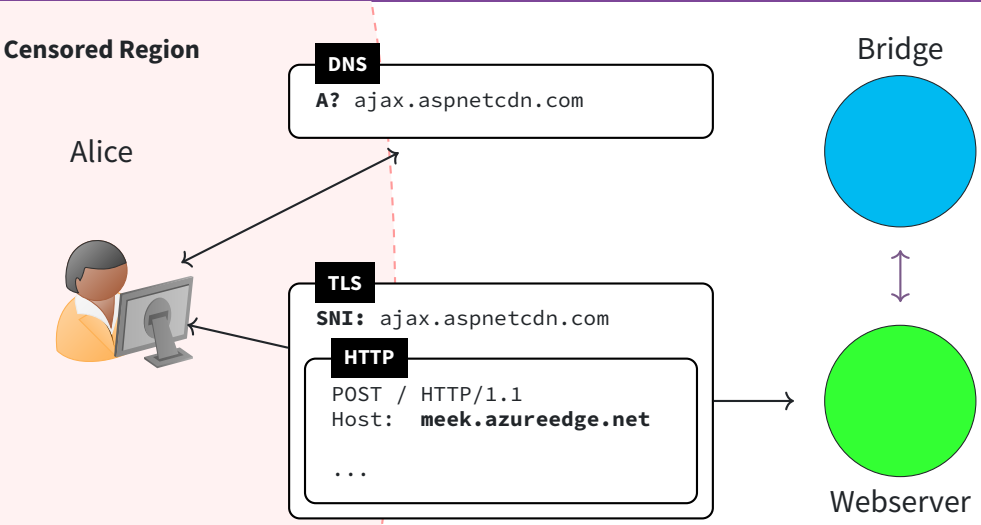
Pluggable Transports

- Allows people to easily build, experiment, and deploy their own obfuscation technology without having to modify the Tor source code itself.
- The specification for Pluggable Transports is open and allows other vendors to implement support for PTs in their own products.
- Allows people to experiment with different transports for Tor that might not be doing any anti-censorship related obfuscation.

Obfourscator (obfs4)

- Makes it hard for passive DPI to verify the presence of the obfs4 protocol unless the adversary knows the bridge parameters.
- Makes active probing hard unless the adversary knows the bridge parameters.
- Uses Tor's ntor handshake (x25519), but uses Elligator2 to encode the elliptic-curve points to be indistinguishable from uniform random strings. The link layer encryption uses NaCl secret boxes (XSalsa20 and Poly1305).

SNI Domain Fronting using Meek



SNI Domain Fronting using Meek

Very **efficient**, but **expensive** :-(

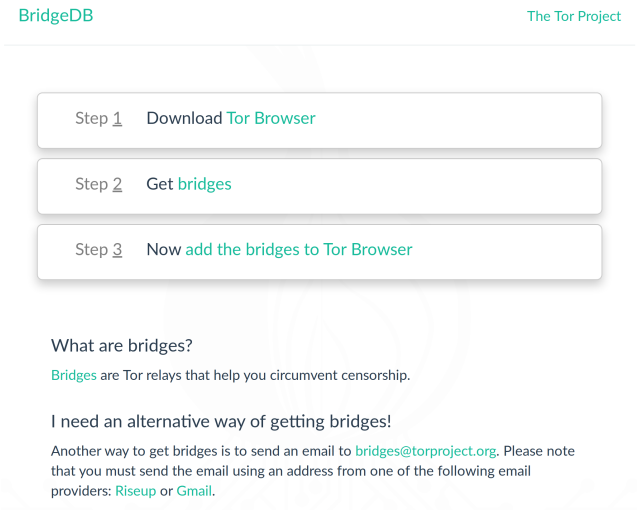
Unpopular with the cloud providers:

Google	Never been a supported feature of Google.
Amazon	Already handled as a breach of AWS ToS.

Domain Fronting in the Future?

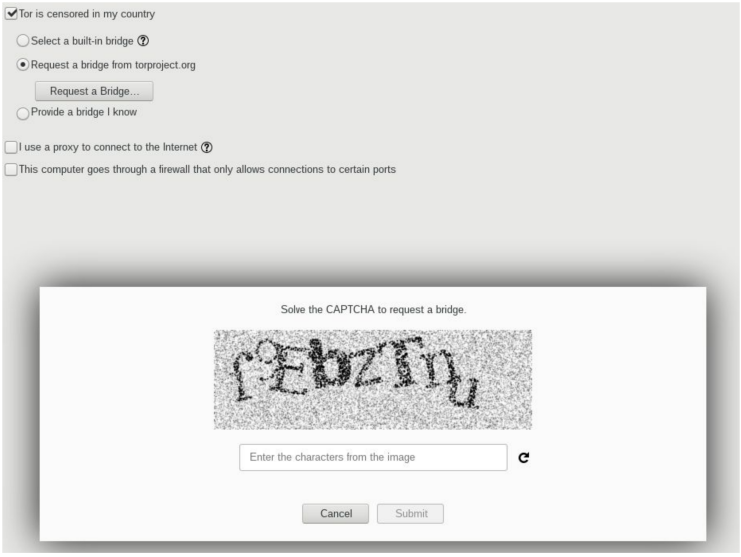
- Use Encrypted SNI?
- Use message queue services hosted by the different cloud providers?
- Generally continue to use centralized services to give people in censored areas access.

Bridge Distribution



Source: bridges.torproject.org

Bridge Distribution using Moat



Snowflake

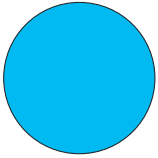
Censored Region

Alice

Snowflake PT Client

Snowflake Broker

Bridge



Snowflake PT Server

Snowflake

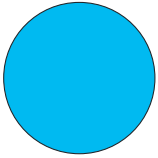
Censored Region

Alice

Snowflake PT Client

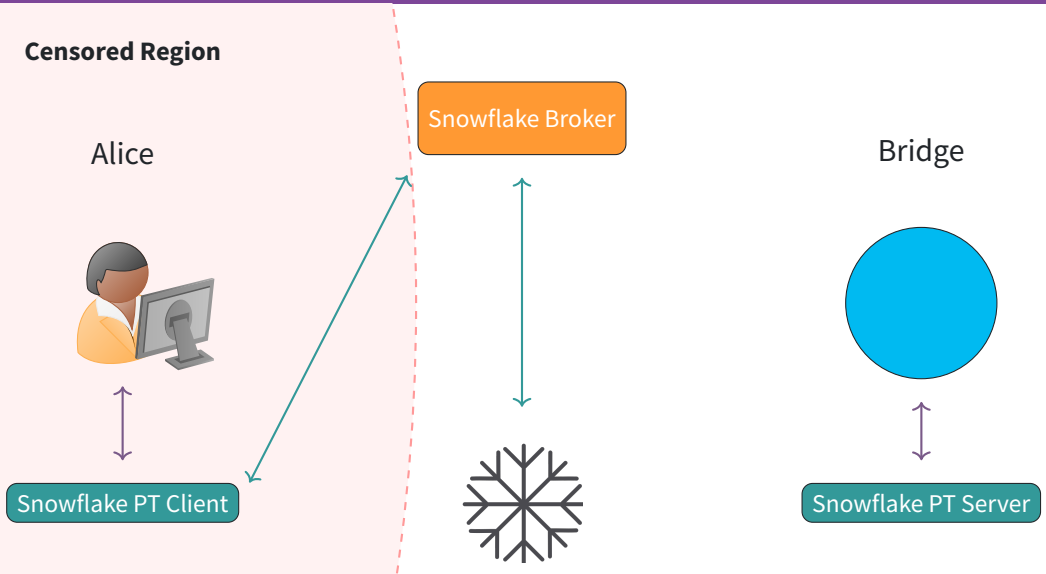
Snowflake Broker

Bridge



Snowflake PT Server

Snowflake


Censored Region
Alice
Snowflake Broker
Bridge
Snowflake PT Client
Snowflake PT Server

Snowflake

Censored Region

Alice

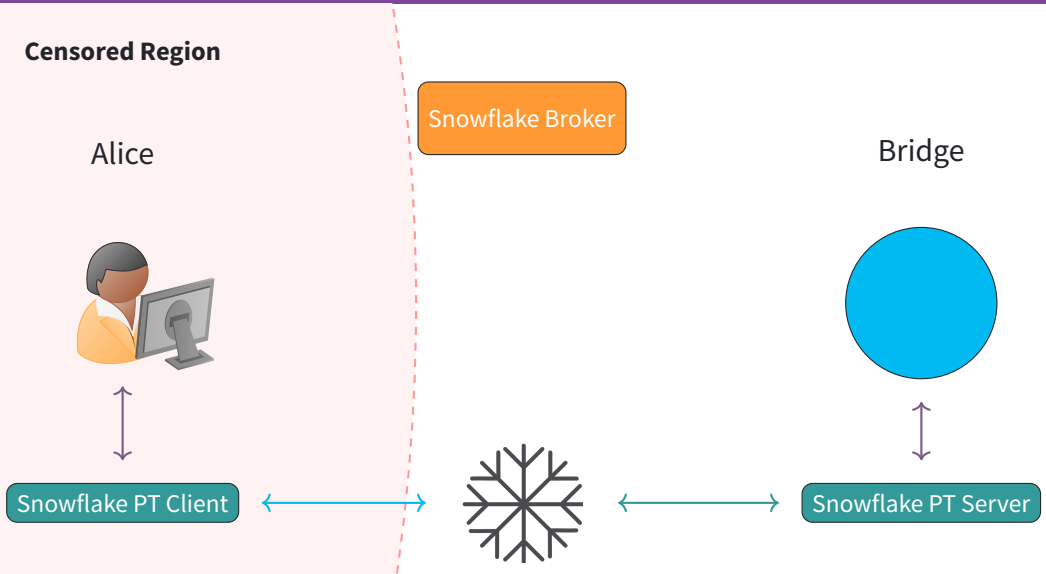
Snowflake PT Client

Snowflake Broker

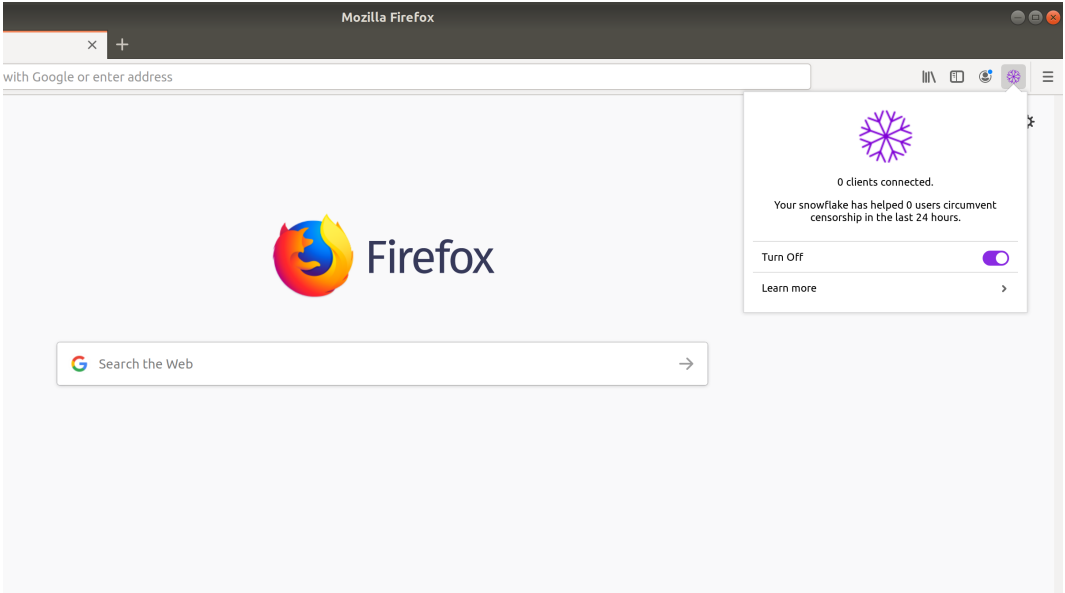
Bridge

Snowflake PT Server

Snowflake


Censored Region
Snowflake Broker
Alice
Bridge
Snowflake PT Client
Snowflake PT Server

Snowflake


Mozilla Firefox
with Google or enter address
0 clients connected.
Your snowflake has helped 0 users circumvent censorship in the last 24 hours.
Turn Off
Learn more
Firefox
Search the Web

Tor is not foolproof

- Operational security mistakes.
- Browser metadata fingerprinting.
- Browser exploits.
- Traffic analysis.

How can you help?

- Run a Tor relay or a bridge!
- Teach others about Tor and privacy in general.
- Find, and maybe fix, bugs in Tor.
- Test Tor on your platform of choice.
- Work on some of the many open research projects.
- Donate at donate.torproject.org

Questions?