Граждане России и Украины:

Подключайтесь к интернету анонимно.

Понять, как обойти блокаду сайтов и социальных сетей, введенную российским правительством во время войны.

Читать на английском языке - Страница 11
Read in English - Page 11

АНОНИМНЫЙ ПОДКЛЮЧЕНИЕ

VPN-соединение устанавливает безопасное соединение между вами и Интернетом.
При использовании VPN весь трафик данных направляется через зашифрованный виртуальный туннель.
Это маскирует IP-адрес, который вы используете при работе в Интернете, делая ваше местоположение невидимым для всех.

https://protonvpn.com/

ProtonVPN - это *VPN*-сервис, предоставляемый швейцарской компанией *Proton Technologies AG*, стоящей за почтовым сервисом *ProtonMail*.

https://www.expressvpn.com/

Обеспечивает конфиденциальность ваших данных в *Windows*, а также имеет строгую политику *"no-log* и автоматический переключатель для защиты от случайной утечки данных.

https://mullvad.net/

Не требует регистрации
Он генерирует номер учетной записи для использования в качестве доступа.
Основная конфигурация
Включите в настройках > расширенные > включите кнопку "Всегда требовать *VPN (*автоматическое подключение*)".*

РЕКОМЕНДУЕМЫЕ СЕТИ ДЛЯ ПОДКЛЮЧЕНИЕ

Норвегия - Все собственные серверы
Польша - Сторонние серверы
Румыния - Сторонние серверы
Швеция - Все собственные серверы
Нидерланды (The Netherlands) - собственные и сторонние серверы
Сингапур - Сторонние серверы
Финляндия - Все собственные серверы
Бельгия - Сторонние серверы
Германия - Собственные серверы и серверы сторонних производителей

ДЕЦЕНТРАЛИЗОВАННЫЙ СЕРВИСЫ.

Mailfence - это собственная служба обмена зашифрованными сообщениями, основанная на стандарте OpenPGP, которая предлагает как запуск, так и цифровую подпись.

https://mailfence.com/

ОБМЕН ФАЙЛАМИ И ОБЛАЧНЫЕ ДАННЫЕ ХРАНЕНИЕ

https://upload.disroot.org/
https://anonfiles.com/
https://github.com/xwiki-labs/cryptpad
https://cryptpad.fr/
https://pad.riseup.net/

БЕЗОПАСНЫЙ ВЕБ БРОУЗИНГ

uBlockOrigin

бесплатное, кроссплатформенное расширение браузера с открытым исходным кодом для блокировки контента, включая блокировку рекламы.

Decentraleyes

бесплатное расширение браузера с открытым исходным кодом, используемое для эмуляции локальной сети распространения контента.

ClearURL

Это расширение автоматически удаляет элементы отслеживания URL-адресов, чтобы помочь защитить вашу конфиденциальность при работе в Интернете.

Privacy Badger

Privacy Badger автоматически учится блокировать невидимые трекеры. Вместо того чтобы вести списки блокируемых объектов, Privacy Badger автоматически обнаруживает трекеры, основываясь на их поведении.

HTTPS Everywhere

HTTPS Everywhere - это дополнение, разработанное Electronic Frontier Foundation для браузеров Google Chrome, Mozilla Firefox и Opera, которое автоматически включает протокол HTTPS, делая браузер более безопасным.

ПРОЕКТ ONION TOR

Браузер Tor использует сеть Tor для защиты вашей конфиденциальности и анонимности. Использование сети Tor имеет два основных свойства:

Ваш интернет-провайдер и любой, кто наблюдает за вашим соединением локально, не смогут отследить вашу интернет-активность, включая названия и адреса посещаемых вами веб-сайтов.

Операторы веб-сайтов и услуг, которые вы используете, и все, кто следит за ними, будут видеть соединение, исходящее из сети Tor, вместо вашего реального интернет-адреса (IP), и не будут знать, кто вы такой, пока вы явно не назовете себя.

Для **Windows**

1- Перейдите на страницу загрузки Tor Browser.

2- Скачайте файл Windows .exe.

3- (Рекомендуется) Проверьте подпись файла.

4- Когда загрузка будет завершена, дважды щелкните файл .exe. Завершите процесс работы мастера установки.

Для **macOS**

1- Перейдите на страницу загрузки Tor Browser.

2- Скачайте файл macOS .dmg.

3- (Рекомендуется) Проверьте подпись файла.

4- Когда загрузка будет завершена, дважды щелкните файл .dmg. Завершите процесс работы мастера установки

Для **GNU/Linux**

1- Перейдите на страницу загрузки Tor Browser.

2-Скачайте файл GNU/Linux .tar.xz.

3- (Рекомендуется) Проверьте подпись файла.

4- Теперь следуйте методу командной строки:

4.1- После завершения загрузки распакуйте архив командой tar -xf [ТВ архив].

4.2- Находясь в директории Tor Browser, вы можете запустить Tor Browser, выполнив команду:
./start-tor-browser.desktop

Примечание: Если эта команда не выполняется, вероятно, вам нужно сделать файл исполняемым. Из этой директории выполните: chmod +x start-tor-browser.desktop

ПРОЕКТ **ONION TOR** -> МОСТ

Большинство подключаемых транспортов, таких как obfs4, полагаются на использование "мостовых" реле. Как и обычные реле Tor, мосты управляются добровольцами; однако, в отличие от обычных реле, их список не публикуется, поэтому противник не сможет легко их идентифицировать.

Использование мостов в сочетании с подключаемыми транспортами помогает скрыть факт использования Tor, но может замедлить соединение по сравнению с использованием обычных ретрансляторов Tor.

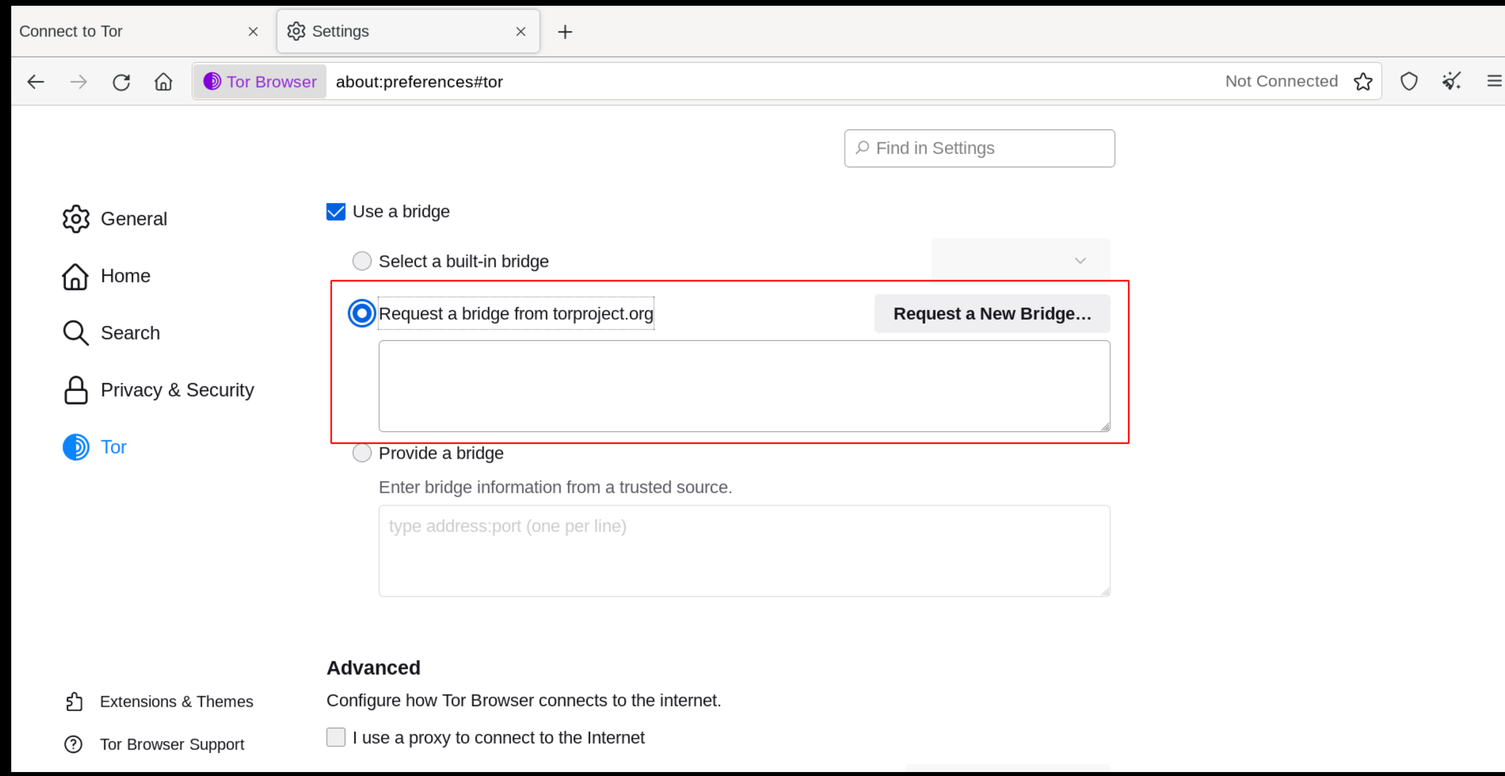
Другие подключаемые транспорты, например meek, используют различные методы борьбы с цензурой, которые не зависят от мостов. Для использования этих транспортов вам не нужно получать адреса мостов.

ПОЛУЧЕНИЕ АДРЕСОВ МОСТОВ

Поскольку адреса мостов не являются общедоступными, вам придется запрашивать их самостоятельно. У вас есть несколько вариантов:

- Посетите сайт *https://bridges.torproject.org/* и следуйте инструкциям,
- илиОтправить письмо на *bridges@torproject.org* с адреса электронной почты *Gmail* или *Riseup* или
- Использовать *Moat* для получения мостов из браузера *Tor.*

ПРОЕКТ ONION TOR -> МОСТ



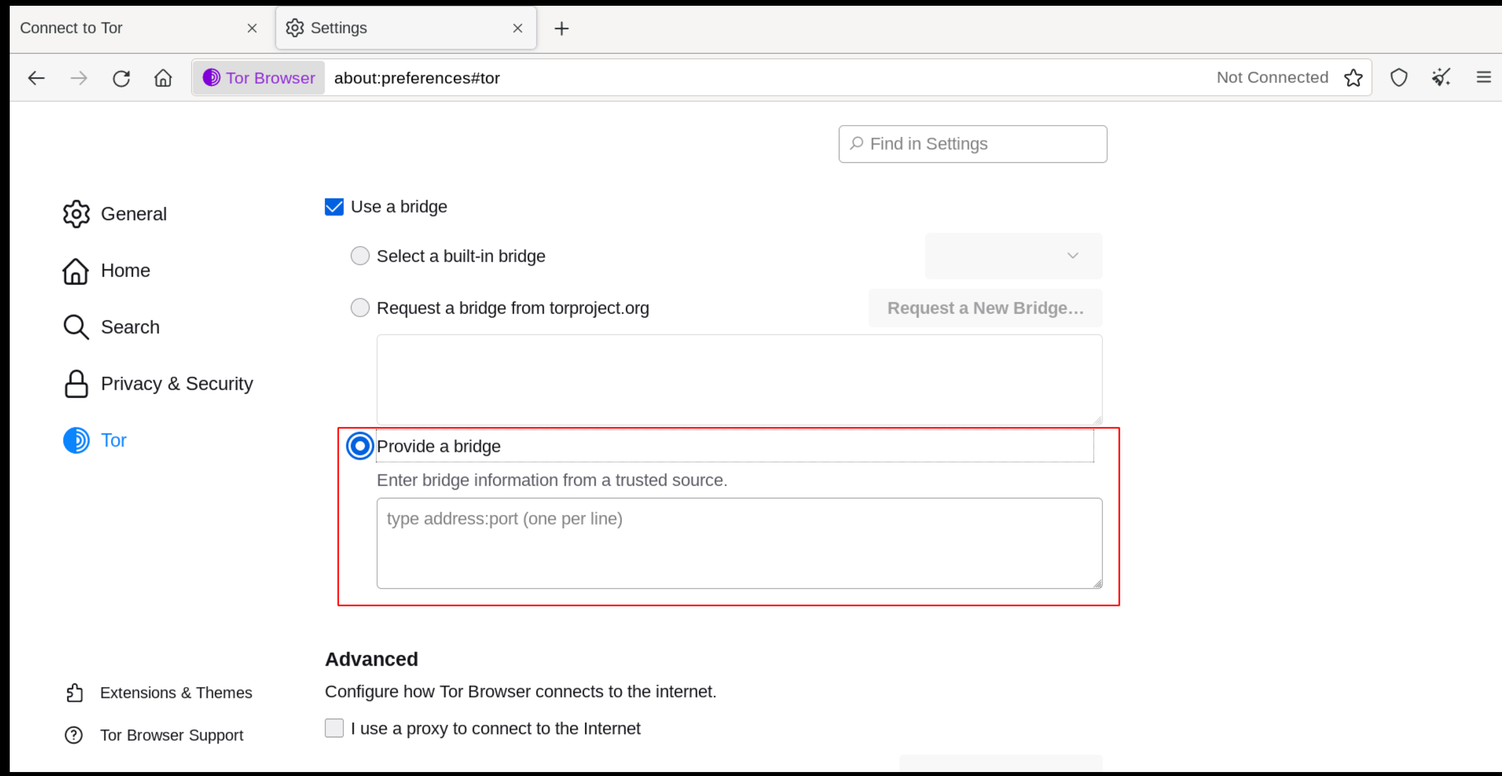
ИСПОЛЬЗОВАНИЕ МОСТА

Если вы запускаете Tor Browser впервые, нажмите "Настройки сети Tor", чтобы открыть окно настроек Tor. В разделе "Мосты" установите флажок "Использовать мост", затем выберите "Запросить мост с torproject.org" и нажмите "Запросить мост...", чтобы BridgeDB предоставил мост. Заполните капчу и нажмите "Отправить". Нажмите "Подключиться", чтобы сохранить настройки.

Или, если у вас запущен Tor Browser, нажмите на "Preferences" (или "Options" в Windows) в меню гамбургера ( ), а затем на "Tor" в боковой панели. В разделе "Мосты" установите флажок "Использовать мост", а в опции "Запросить мост у torproject.org" нажмите "Запросить новый мост...", чтобы BridgeDB предоставил мост. Введите капчу и нажмите "Отправить". Ваши настройки будут автоматически сохранены, как только вы закроете вкладку.

ПРОЕКТ ONION TOR -> МОСТ

ВВОД МОСТА АДРЕСА



Или, если у вас запущен Tor Browser, нажмите на "Preferences" (или "Options" в Windows) в меню гамбургера ( ), а затем на "Tor" в боковой панели. В разделе "Мосты" установите флажок "Использовать мост", а в опции "Предоставить известный мне мост" введите адрес каждого моста в отдельной строке. Ваши настройки будут автоматически сохранены после закрытия вкладки.

Если соединение не работает, возможно, полученные вами мосты не работают. Пожалуйста, воспользуйтесь одним из описанных выше способов получения дополнительных адресов мостов и повторите попытку.

Переведено с помощью www.DeepL.com/Translator (бесплатная версия)

ДОСТУП К СОЦИАЛЬНЫМ СЕТЯМ ВНУТРИ **ONION/TOR.**

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/

http://torch4st4l57l2u2vr5wqwvwyueucvnrao4xajqr2klmcmicrv7ccaad.onion/

Russian and Ukrainian Citizens:

Connect to the internet anonymously.

Understand how to circumvent the blockade to websites and social networks imposed by the Russian government during war.

ANONYMOUS CONNECTION

A VPN connection establishes a secure connection between you and the Internet. When using a VPN, all data traffic is routed through an encrypted virtual tunnel.
This disguises the IP address you use when you are on the Internet, making your location invisible to everyone.

https://protonvpn.com/

ProtonVPN is a VPN service operated by the Swiss company Proton Technologies AG, the company behind the ProtonMail email service.

https://www.expressvpn.com/

Keeps your data private on Windows, plus it has a strict no-log policy and an automatic kill switch to protect you against accidental data leaks.

https://mullvad.net/

No registration required

It generates an account number to use as access

Primary configuration

Enable in settings > advanced > enable "Always require VPN (automatic connection)" button

RECOMMENDED NETWORKS FOR CONNECTION

Norway - All own servers
- Poland - Third Party Servers
- Romania - 3rd Party Servers
- Sweden - All own servers
- The Netherlands (The Netherlands) - Own servers & Third Party Servers
- Singapore - 3rd Party servers
- Finland - All own servers
- Belgium - 3rd Party servers
- Germany - Own servers & 3rd party servers

DECENTRALIZED SERVICES.

Mailfence is a proprietary encrypted encrypted messaging service based on the OpenPGP standard that offers both startup and digital signature.

https://mailfence.com/

FILE SHARING AND CLOUD DATA STORAGE

https://upload.disroot.org/
https://anonfiles.com/
https://github.com/xwiki-labs/cryptpad
https://cryptpad.fr/
https://pad.riseup.net/

SAFE WEB BROWSING

uBlockOrigin

uBlockOrigin is a free, open-source, cross-platform browser extension for content filtering, including ad blocking.

Decentraleyes

Decentraleyes is a free, open source browser extension used for local content distribution network emulation.

ClearURL

This extension will automatically remove URL tracking elements to help protect your privacy when surfing the Internet.

Privacy Badger

Privacy Badger automatically learns to block invisible trackers. Instead of keeping lists of what to block, Privacy Badger automatically discovers trackers based on their behavior

HTTPS Everywhere

HTTPS Everywhere is an add-on developed by the Electronic Frontier Foundation for Google Chrome, Mozilla Firefox and Opera browsers, that automatically enables the HTTPS protocol, making the browser more more secure.

TOR ONION PROJECT

Tor Browser uses the Tor network to protect your privacy and anonymity. Using the Tor network has two main properties:

Your internet service provider, and anyone watching your connection locally, will not be able to track your internet activity, including the names and addresses of the websites you visit.

The operators of the websites and services that you use, and anyone watching them, will see a connection coming from the Tor network instead of your real Internet (IP) address, and will not know who you are unless you explicitly identify yourself.

For Windows

1- Navigate to the Tor Browser download page.

2- Download the Windows .exe file.

3- (Recommended) Verify the file's signature.

4- When the download is complete, double click the .exe file. Complete the installation wizard process.

For macOS

1- Navigate to the Tor Browser download page.

2- Download the macOS .dmg file.

3- (Recommended) Verify the file's signature.

4- When the download is complete, double click the .dmg file. Complete the installation wizard process.

For GNU/Linux

1- Navigate to the Tor Browser download page.

2-Download the GNU/Linux .tar.xz file.

3- (Recommended) Verify the file's signature.

4- Now follow either the command-line method:

4.1- When the download is complete, extract the archive with the command tar -xf [TB archive].

4.2- From inside the Tor Browser directory, you can launch Tor Browser by running:

```
./start-tor-browser.desktop
```

Note: If this command fails to run, you probably need to make the file executable. From within this directory run: chmod +x start-tor-browser.desktop

TOR ONION PROJECT -> BRIDGE

Most Pluggable Transports, such as obfs4, rely on the use of "bridge" relays. Like ordinary Tor relays, bridges are run by volunteers; unlike ordinary relays, however, they are not listed publicly, so an adversary cannot identify them easily.

Using bridges in combination with pluggable transports helps to conceal the fact that you are using Tor, but may slow down the connection compared to using ordinary Tor relays.

Other pluggable transports, like meek, use different anti-censorship techniques that do not rely on bridges. You do not need to obtain bridge addresses in order to use these transports.

GETTING BRIDGE ADDRESSES

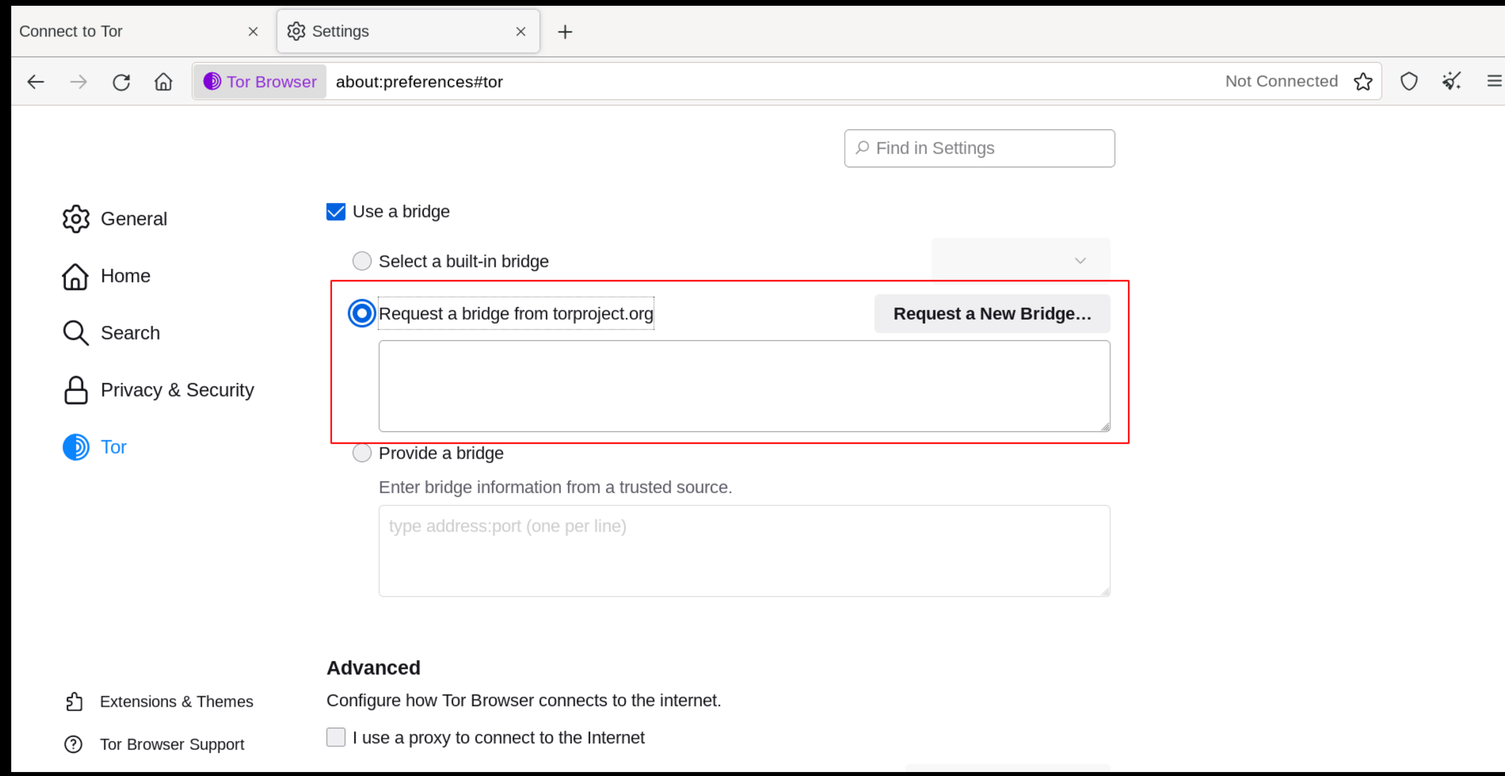
Because bridge addresses are not public, you will need to request them yourself. You have a few options:

Visit https://bridges.torproject.org/ and follow the instructions, or

Email bridges@torproject.org from a Gmail, or Riseup email address or

Use Moat to fetch bridges from within Tor Browser.

TOR ONION PROJECT -> BRIDGE



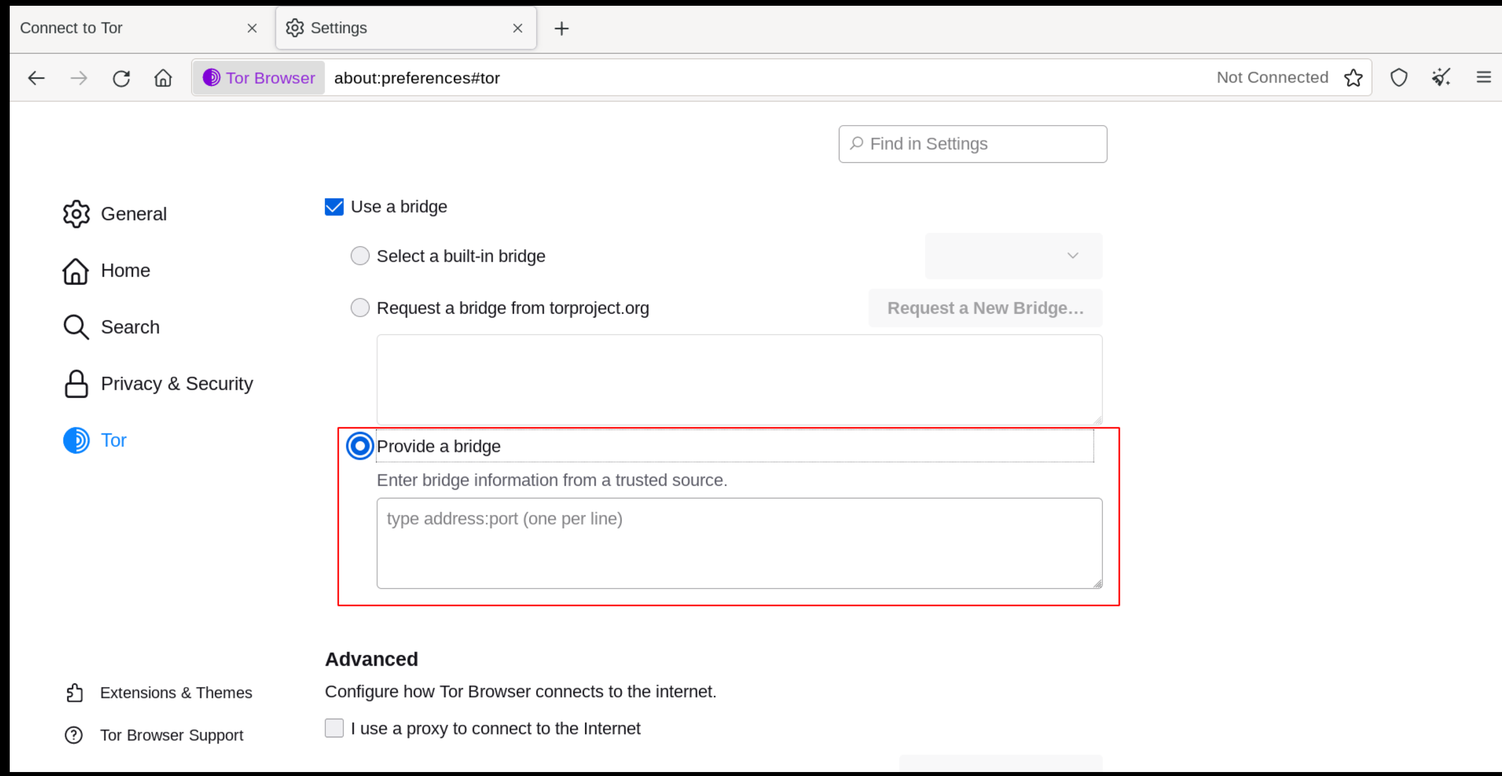
USING MOAT

If you're starting Tor Browser for the first time, click "Tor Network Settings" to open the Tor settings window. Under the "Bridges" section, select the checkbox "Use a bridge", then choose "Request a bridge from torproject.org" and click "Request a Bridge..." for BridgeDB to provide a bridge. Complete the Captcha and click "Submit". Click "Connect" to save your settings.

Or, if you have Tor Browser running, click on "Preferences" (or "Options" on Windows) in the hamburger menu ( ) and then on "Tor" in the sidebar. In the "Bridges" section, select the checkbox "Use a bridge", and from the option "Request a bridge from torproject.org", click "Request a New Bridge..." for BridgeDB to provide a bridge. Complete the Captcha and click "Submit". Your setting will automatically be saved once you close the tab.

TOR ONION PROJECT -> BRIDGE

ENTERING BRIDGE ADDRESSES



If you're starting Tor Browser for the first time, click "Tor Network Settings" to open the Tor settings window. Under the "Bridges" section, select the checkbox "Use a bridge", choose "Provide a bridge I know" and enter each bridge address on a separate line. Click "Connect" to save your settings.

Or, if you have Tor Browser running, click on "Preferences" (or "Options" on Windows) in the hamburger menu ( ) and then on "Tor" in the sidebar. In the "Bridges" section, select the checkbox "Use a bridge", and from the option "Provide a bridge I know", enter each bridge address on a separate line. Your settings will automatically be saved once you close the tab.

If the connection fails, the bridges you received may be down. Please use one of the above methods to obtain

ACCESSING SOCIAL NETWORKS INSIDE ONION/TOR.

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/

http://torch4st4l57l2u2vr5wqwvwyueucvnrao4xajqr2klmcmicrv7ccaad.onion/