Tor (Русский)

**[Tango-preferences-desktop-locale.png](https://wiki.archlinux.org/index.php/File:Tango-preferences-desktop-locale.png)Эта статья или раздел нуждается в**[**переводе**](https://wiki.archlinux.org/index.php/ArchWiki:Contributing_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.9F.D0.B5.D1.80.D0.B5.D0.B2.D0.BE.D0.B4)**[Tango-preferences-desktop-locale.png](https://wiki.archlinux.org/index.php/File:Tango-preferences-desktop-locale.png)**

**Примечания:** Перевод устарел. (обсуждение: [**Talk:Tor (Русский)#**](https://wiki.archlinux.org/index.php/Talk:Tor_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)))

**[Tango-preferences-desktop-locale.png](https://wiki.archlinux.org/index.php/File:Tango-preferences-desktop-locale.png)Эта страница нуждается в сопроводителе[Tango-preferences-desktop-locale.png](https://wiki.archlinux.org/index.php/File:Tango-preferences-desktop-locale.png)**

Статья не гарантирует актуальность информации. Помогите русскоязычному сообществу поддержкой подобных страниц. См. [**Команда переводчиков ArchWiki**](https://wiki.archlinux.org/index.php/%D0%9A%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%B0_%D0%BF%D0%B5%D1%80%D0%B5%D0%B2%D0%BE%D0%B4%D1%87%D0%B8%D0%BA%D0%BE%D0%B2_ArchWiki)

[**Tor**](https://ru.wikipedia.org/wiki/Tor) - открытая реализация анонимной сети [**луковой маршрутизации**](https://ru.wikipedia.org/wiki/%D0%9B%D1%83%D0%BA%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BC%D0%B0%D1%80%D1%88%D1%80%D1%83%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) 2-го поколения. Он может пригодится тем, кто хочет сохранить анонимность в интернете, а также защитить трафик от третьей стороны (провайдера и других любопытных). Также, использование подобного программного обеспечения актуально для стран в которых есть [**интернет-цензура**](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D1%86%D0%B5%D0%BD%D0%B7%D1%83%D1%80%D0%B0).

**Contents**

 [hide]

* [1Принцип работы](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9F.D1.80.D0.B8.D0.BD.D1.86.D0.B8.D0.BF_.D1.80.D0.B0.D0.B1.D0.BE.D1.82.D1.8B)
* [2Установка](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.A3.D1.81.D1.82.D0.B0.D0.BD.D0.BE.D0.B2.D0.BA.D0.B0)
* [3Настройка](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0)
  + [3.1Настройка Tor Relay](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_Tor_Relay)
* [4Запуск Tor в Chroot](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.97.D0.B0.D0.BF.D1.83.D1.81.D0.BA_Tor_.D0.B2_Chroot)
* [5Запуск Tor в systemd-nspawn контейнере с виртуальным сетевым интерфейсом](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.97.D0.B0.D0.BF.D1.83.D1.81.D0.BA_Tor_.D0.B2_systemd-nspawn_.D0.BA.D0.BE.D0.BD.D1.82.D0.B5.D0.B9.D0.BD.D0.B5.D1.80.D0.B5_.D1.81_.D0.B2.D0.B8.D1.80.D1.82.D1.83.D0.B0.D0.BB.D1.8C.D0.BD.D1.8B.D0.BC_.D1.81.D0.B5.D1.82.D0.B5.D0.B2.D1.8B.D0.BC_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81.D0.BE.D0.BC)
  + [5.1Установка и настройка хоста](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.A3.D1.81.D1.82.D0.B0.D0.BD.D0.BE.D0.B2.D0.BA.D0.B0_.D0.B8_.D0.BD.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_.D1.85.D0.BE.D1.81.D1.82.D0.B0)
    - [5.1.1Виртуальный сетевой интерфейс](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.92.D0.B8.D1.80.D1.82.D1.83.D0.B0.D0.BB.D1.8C.D0.BD.D1.8B.D0.B9_.D1.81.D0.B5.D1.82.D0.B5.D0.B2.D0.BE.D0.B9_.D0.B8.D0.BD.D1.82.D0.B5.D1.80.D1.84.D0.B5.D0.B9.D1.81)
    - [5.1.2Запуск и включение systemd-nspawn](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.97.D0.B0.D0.BF.D1.83.D1.81.D0.BA_.D0.B8_.D0.B2.D0.BA.D0.BB.D1.8E.D1.87.D0.B5.D0.BD.D0.B8.D0.B5_systemd-nspawn)
  + [5.2Настройка контейнера](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_.D0.BA.D0.BE.D0.BD.D1.82.D0.B5.D0.B9.D0.BD.D0.B5.D1.80.D0.B0)
    - [5.2.1Запуск и включение systemd-networkd](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.97.D0.B0.D0.BF.D1.83.D1.81.D0.BA_.D0.B8_.D0.B2.D0.BA.D0.BB.D1.8E.D1.87.D0.B5.D0.BD.D0.B8.D0.B5_systemd-networkd)
  + [5.3Настройка Tor](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_Tor)
* [6Использование](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.98.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5)
* [7Веб-сёрфинг](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.92.D0.B5.D0.B1-.D1.81.D1.91.D1.80.D1.84.D0.B8.D0.BD.D0.B3)
  + [7.1Firefox](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Firefox)
  + [7.2Chromium](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Chromium)
* [8Tor и HTTP прокси](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Tor_.D0.B8_HTTP_.D0.BF.D1.80.D0.BE.D0.BA.D1.81.D0.B8)
  + [8.1Polipo](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Polipo)
  + [8.2Privoxy](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Privoxy)
    - [8.2.1Tor и Privoxy в Firefox](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Tor_.D0.B8_Privoxy_.D0.B2_Firefox)
    - [8.2.2Tor и Privoxy в других приложениях](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Tor_.D0.B8_Privoxy_.D0.B2_.D0.B4.D1.80.D1.83.D0.B3.D0.B8.D1.85_.D0.BF.D1.80.D0.B8.D0.BB.D0.BE.D0.B6.D0.B5.D0.BD.D0.B8.D1.8F.D1.85)
* [9Запуск сервера Tor](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.97.D0.B0.D0.BF.D1.83.D1.81.D0.BA_.D1.81.D0.B5.D1.80.D0.B2.D0.B5.D1.80.D0.B0_Tor)
  + [9.1Настройка](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9D.D0.B0.D1.81.D1.82.D1.80.D0.BE.D0.B9.D0.BA.D0.B0_2)
* [10TorDNS](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#TorDNS)
* [11"Торификация"](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.22.D0.A2.D0.BE.D1.80.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D1.8F.22)
* [12Решение проблем](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.A0.D0.B5.D1.88.D0.B5.D0.BD.D0.B8.D0.B5_.D0.BF.D1.80.D0.BE.D0.B1.D0.BB.D0.B5.D0.BC)
  + [12.1Проблема с пользовательским значением](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.9F.D1.80.D0.BE.D0.B1.D0.BB.D0.B5.D0.BC.D0.B0_.D1.81_.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D1.82.D0.B5.D0.BB.D1.8C.D1.81.D0.BA.D0.B8.D0.BC_.D0.B7.D0.BD.D0.B0.D1.87.D0.B5.D0.BD.D0.B8.D0.B5.D0.BC)
* [13Внешние ссылки](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#.D0.92.D0.BD.D0.B5.D1.88.D0.BD.D0.B8.D0.B5_.D1.81.D1.81.D1.8B.D0.BB.D0.BA.D0.B8)

Принцип работы

Пользователи сети Tor запускают прокси на своей машине. Это приложение соединяется с сетью и формирует цепочку из трех серверов, которая периодически меняется. Передаваемые данные шифруются несколько раз на вашем компьютере и передаются на цепь серверов, каждый из которых последовательно снимает свой "луковый" слой шифрования. На последнем сервере ваша инфорамция приобретает первоначальный вид. Большое количество промежуточных узлов значительно замедляет скорость работы сети.

Tor предоставляет SOCKS интерфейс, через который могут направлять трафик совместимые приложения. Происходит т.н. "торификация" соединения.

**Важно:**Учтите, что недобросовестные владельцы конечных серверов (нод в цепочке) могут перехватывать ваш трафик, так что озаботьесь дополнительным шифрованием, для предотвращения перехвата личной информации и паролей.

**Важно:**Tor сам по себе не обеспечивает анонимности: он не дает определить *откуда* произошла передача данных, но все ещё остается возможность идентификации личности по их содержимому (см. [**Want Tor to really work?**](https://www.torproject.org/download/download.html.en#warning)).

Кроме описанных, есть и другие ограничения. Будет лучше, если вы ознакомитесь с ними на сайте проекта **до** использования.

Установка

Установим Tor. Его пакет расположен в [community].

# pacman -S tor

Пакет [**arm**](https://www.archlinux.org/packages/?name=arm) (Anonymizing Relay Monitor) представляет собой консольный монитор состояния использования пропускной способности сети, сведения о соединении и другое. Вы также можете использовать для настройки и управление графический клиент [**vidalia**](https://aur.archlinux.org/packages/vidalia/)AUR - это Qt GUI для Tor. Кроме конфигурирования и контроля над процессом работы вы также получаете возможность видеть статус сети Tor, монитор трафика, просматривать фильтровать и искать логи.

Настройка

По умолчанию, Tor читает конфигурацию из файла /etc/tor/torrc. Опции подробно расписаны в [**tor(1)**](https://jlk.fjfi.cvut.cz/arch/manpages/man/tor.1) и на [**сайте проекта**](https://www.torproject.org/docs/tor-manual.html.en). Конфигурационный файл по умолчанию подойдет для большинства пользователей.

Имеется неколько потенциальных конфликтов конфигурации в /etc/tor/torrc и tor.service.

* В torrc, RunAsDaemon должен быть, как и по умолчаниию, установлен в 0, так как Type=simple установлен в разделе [Service] в tor.service.
* В torrc, User не должен быть указан, пока User= указан как root в разделе [Service] в tor.service.

Установить значение дескриптора ulimits можно изменив переменную TOR\_MAX\_FD в конфигурационном файле /etc/conf.d/tor.

**Настройка Tor Relay**

Максимальное количество файловых дескрипторов, которое может быть открыто Tor устанавливается параметром LimitNOFILE в tor.service. Быстрые ретранляторы могут увеличить это значение.

Если на вашем компьютере не запущен веб-сервер, и вы не установили значение AccountingMax, рассмотрите возможность установки параметра ORPort в значение 443 и/или DirPort в значение 80. Многие пользователи Tor находятся за файрволами, и это позволит им бороздить просторы интернета, так как такая настройка позволит им использовать ваш Tor relay. Если же вы уже используете порты 80 и 443, другие пригодные порты: 22, 110 и 143.[**[1]**](https://www.torproject.org/docs/tor-relay-debian) Однако данные порты системные, поэтому Tor должен быть запущен от пользователя root, с помощью параметров User=root в tor.service и User tor в torrc.

Будет полезно прочесть [**Жизненый цикл новых Tor Relay**](https://blog.torproject.org/blog/lifecycle-of-a-new-relay) документации Tor.

Запуск Tor в Chroot

**Warning:** Подключение по telnet на локальный ControlPort окажется невозможным если Tor запущен в chroot

По соображениям безопасности, желательно запускать Tor в [**chroot**](https://wiki.archlinux.org/index.php/Chroot). Следующие скрипты создадут подходящий chroot в /opt/torchroot:

~/torchroot-setup.sh

#!/bin/bash

export TORCHROOT=/opt/torchroot

mkdir -p $TORCHROOT

mkdir -p $TORCHROOT/etc/tor

mkdir -p $TORCHROOT/dev

mkdir -p $TORCHROOT/usr/bin

mkdir -p $TORCHROOT/usr/lib

mkdir -p $TORCHROOT/usr/share/tor

mkdir -p $TORCHROOT/var/lib

ln -s /usr/lib $TORCHROOT/lib

cp /etc/hosts $TORCHROOT/etc/

cp /etc/host.conf $TORCHROOT/etc/

cp /etc/localtime $TORCHROOT/etc/

cp /etc/nsswitch.conf $TORCHROOT/etc/

cp /etc/resolv.conf $TORCHROOT/etc/

cp /etc/tor/torrc $TORCHROOT/etc/tor/

cp /usr/bin/tor $TORCHROOT/usr/bin/

cp /usr/share/tor/geoip\* $TORCHROOT/usr/share/tor/

cp /lib/libnss\* /lib/libnsl\* /lib/ld-linux-\*.so\* /lib/libresolv\* /lib/libgcc\_s.so\* $TORCHROOT/usr/lib/

cp $(ldd /usr/bin/tor | awk '{print $3}'|grep --color=never "^/") $TORCHROOT/usr/lib/

cp -r /var/lib/tor $TORCHROOT/var/lib/

chown -R tor:tor $TORCHROOT/var/lib/tor

sh -c "grep --color=never ^tor /etc/passwd > $TORCHROOT/etc/passwd"

sh -c "grep --color=never ^tor /etc/group > $TORCHROOT/etc/group"

mknod -m 644 $TORCHROOT/dev/random c 1 8

mknod -m 644 $TORCHROOT/dev/urandom c 1 9

mknod -m 666 $TORCHROOT/dev/null c 1 3

if [[ "$(uname -m)" == "x86\_64" ]]; then

cp /usr/lib/ld-linux-x86-64.so\* $TORCHROOT/usr/lib/.

ln -sr /usr/lib64 $TORCHROOT/lib64

ln -s $TORCHROOT/usr/lib ${TORCHROOT}/usr/lib64

fi

После запуска скрипта от пользователя root, Tor может быть запущен [**chroot**](https://wiki.archlinux.org/index.php/Chroot) командой:

# chroot --userspec=tor:tor /opt/torchroot /usr/bin/tor

или если вы используете systemd [**отредактируйте**](https://wiki.archlinux.org/index.php/Systemd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.A0.D0.B5.D0.B4.D0.B0.D0.BA.D1.82.D0.B8.D1.80.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D0.BF.D1.80.D0.B5.D0.B4.D0.BE.D1.81.D1.82.D0.B0.D0.B2.D0.BB.D0.B5.D0.BD.D0.BD.D1.8B.D1.85_.D0.BF.D0.B0.D0.BA.D0.B5.D1.82.D0.B0.D0.BC.D0.B8_.D1.84.D0.B0.D0.B9.D0.BB.D0.BE.D0.B2_.D1.8E.D0.BD.D0.B8.D1.82.D0.BE.D0.B2) tor.service:

/etc/systemd/system/tor.service.d/chroot.conf

[Service]

User=root

ExecStart=

ExecStart=/usr/bin/sh -c "chroot --userspec=tor:tor /opt/torchroot /usr/bin/tor -f /etc/tor/torrc"

KillSignal=SIGINT

Запуск Tor в systemd-nspawn контейнере с виртуальным сетевым интерфейсом

В этом примере мы создадим [**systemd-nspawn**](https://wiki.archlinux.org/index.php/Systemd-nspawn) контейнер называющийся tor-exit с виртуальным macvlan сетевым интерфейсом.

Смотри [**Systemd-nspawn**](https://wiki.archlinux.org/index.php/Systemd-nspawn) и [**systemd-networkd**](https://wiki.archlinux.org/index.php/Systemd-networkd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)) для полного ознакомления.

**Установка и настройка хоста**

В этом примере контейнер находится в /srv/container:

# mkdir /srv/container/tor-exit

[**установите**](https://wiki.archlinux.org/index.php/Pacman_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.A3.D1.81.D1.82.D0.B0.D0.BD.D0.BE.D0.B2.D0.BA.D0.B0_.D0.BE.D0.BF.D1.80.D0.B5.D0.B4.D0.B5.D0.BB.D0.B5.D0.BD.D0.BD.D1.8B.D1.85_.D0.BF.D0.B0.D0.BA.D0.B5.D1.82.D0.BE.D0.B2) [**arch-install-scripts**](https://www.archlinux.org/packages/?name=arch-install-scripts).

Установите [**base**](https://www.archlinux.org/groups/x86_64/base/), [**tor**](https://www.archlinux.org/packages/?name=tor) и [**arm**](https://www.archlinux.org/packages/?name=arm) и отмените [**linux**](https://www.archlinux.org/packages/?name=linux), подробнее [**Systemd-nspawn#Installation with pacstrap**](https://wiki.archlinux.org/index.php/Systemd-nspawn#Installation_with_pacstrap)[[**broken link**](https://wiki.archlinux.org/index.php/ArchWiki:Requests#Broken_section_links): invalid section]:

# pacstrap -i -c -d /srv/container/tor-exit base tor arm

Создайте каталог, если он отсутствует:

# mkdir /var/lib/container

Создайте символическую ссылку для регистрации контейнера на хосте, подробнее [**Systemd-nspawn#Boot your container at your machine startup**](https://wiki.archlinux.org/index.php/Systemd-nspawn#Boot_your_container_at_your_machine_startup)[[**broken link**](https://wiki.archlinux.org/index.php/ArchWiki:Requests#Broken_section_links): invalid section]:

# ln -s /srv/container/tor-exit /var/lib/container/tor-exit

**Виртуальный сетевой интерфейс**

Создайте каталог для редактирования файла .service контейнера:

# mkdir /etc/systemd/system/systemd-nspawn@tor-exit.service.d

/etc/systemd/system/systemd-nspawn@tor-exit.service.d/tor-exit.conf

[Service]

ExecStart=

ExecStart=/usr/bin/systemd-nspawn --quiet --keep-unit --boot --link-journal=guest --network-macvlan=$INTERFACE --private-network --directory=/var/lib/container/%i

LimitNOFILE=32768

--network-macvlan=$INTERFACE --private-network автоматически создаст macvlan называющийся mv-$INTERFACE внутри контейнера, который невидим с хоста. --private-networkподразумевает --network-macvlan= в соответсвии с [**systemd-nspawn(1)**](https://jlk.fjfi.cvut.cz/arch/manpages/man/systemd-nspawn.1).

LimitNOFILE=32768 для[**#Raise maximum number of open file descriptors**](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Raise_maximum_number_of_open_file_descriptors)[[**broken link**](https://wiki.archlinux.org/index.php/ArchWiki:Requests#Broken_section_links): invalid section].

Настройте [**systemd-networkd**](https://wiki.archlinux.org/index.php/Systemd-networkd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)) в соответствии с вашими сетевыми настройками /srv/container/tor-exit/etc/systemd/network/mv-$INTERFACE.network.

**Запуск и включение systemd-nspawn**

[**Запустите/Включите**](https://wiki.archlinux.org/index.php/Systemd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.98.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D1.8E.D0.BD.D0.B8.D1.82.D0.BE.D0.B2) systemd-nspawn@tor-exit.service.

**Настройка контейнера**

# machinectl login tor-exit вход в контейнер, смотрите [**Systemd-nspawn#machinectl command**](https://wiki.archlinux.org/index.php/Systemd-nspawn#machinectl_command)[[**broken link**](https://wiki.archlinux.org/index.php/ArchWiki:Requests#Broken_section_links): invalid section].

# mv /srv/container/tor-exit/etc/securetty /srv/container/tor-exit/etc/securetty.bak если вы получаете ошибки описанные в [**Systemd-nspawn#Troubleshooting**](https://wiki.archlinux.org/index.php/Systemd-nspawn#Troubleshooting).

**Запуск и включение systemd-networkd**

[**Запустите/Включите**](https://wiki.archlinux.org/index.php/Systemd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.98.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D1.8E.D0.BD.D0.B8.D1.82.D0.BE.D0.B2) systemd-networkd.service. networkctl отобразит интерфейсы, если systemd-networkd настроен корректно.

**Настройка Tor**

Смотри [**#Running a Tor server**](https://wiki.archlinux.org/index.php/Tor_%28%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9%29#Running_a_Tor_server)[[**broken link**](https://wiki.archlinux.org/index.php/ArchWiki:Requests#Broken_section_links): invalid section].

**Tip:** Удобнее редактировать файлы в контейнере с хоста, вашим любимым редактором.

Использование

[**Запустите/Включите**](https://wiki.archlinux.org/index.php/Systemd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)#.D0.98.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5_.D1.8E.D0.BD.D0.B8.D1.82.D0.BE.D0.B2) tor.service используя [**systemd**](https://wiki.archlinux.org/index.php/Systemd_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)). Или запустите с помощью vidalia, или sudo -u tor /usr/bin/tor.

Для использования программы через Tor, настройте её на использование 127.0.0.1 или localhost в качестве SOCKS5 прокси, порт 9050 (Tor со стандартными настройками) или порт 9051 (Настройка с помощью vidalia, стандартные настройки).

Чтобы проверить, работает ли Tor, посетите страницу [**Tor**](https://check.torproject.org/), [**Harvard**](http://serifos.eecs.harvard.edu/cgi-bin/ipaddr.pl?tor=1) или [**Xenobite.eu**](https://torcheck.xenobite.eu/).

Веб-сёрфинг

**Примечание:**В связи со сложностями обеспечения анонимности (cookies, javascripts, etc), проект Torproject рекомендует использовать свою версию Firefox для анонимного серфинга. Мы вас предупреждали. [**[2]**](http://www.opennet.ru/opennews/art.shtml?num=30449)

[**Firefox**](https://wiki.archlinux.org/index.php/Firefox_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)) и [**Chromium**](https://wiki.archlinux.org/index.php/Chromium_(%D0%A0%D1%83%D1%81%D1%81%D0%BA%D0%B8%D0%B9)) позволяют без проблем направлять трафик через Tor.

**Firefox**

Вы можете просто добавить Tor в качестве SOCKS прокси ("localhost", порт "9050"), открыв браузер и перейдя в **Настройки** > **Дополнительные** > **Вкладка "Сеть"** > **Настроить**. Чтобы перенаправить все DNS-запросы Firefox через прокси (иначе они пойдут не через Tor и будут доступны, например, провайдеру), откройте новую вкладку и введите about:config. Измените переменную *network.proxy.socks\_remote\_dns* на *yes*.

Можно также использовать дополнения, позволяющие переключаться между множественными прокси (например, вы можете использовать Tor в связке с "ssh -D"). В качестве примера можно привести "[**FoxyProxy**](https://addons.mozilla.org/en-us/firefox/addon/foxyproxy-standard/)".

Также можно установить дополнение [**TorButton**](https://www.torproject.org/torbutton/), выполняющий и другие функции, который, однако, более не подерживается.

**Chromium**

Просто запустите:

$ chromium --proxy-server="socks://localhost:9050"

Tor и HTTP прокси

Если вам требуется какой-либо HTTP-прокси.

**Примечание:**На данный момент командой разработчиков Tor рекомендуется прокси-сервер Polipo.

**Polipo**

Polipo это маленький и быстрый HTTP-прокси. Установите и настройте его в соответствии со статьёй [**Polipo**](https://wiki.archlinux.org/index.php/Polipo). Также вы можете воспользоваться [**готовой конфигурацией**](https://gitweb.torproject.org/torbrowser.git/blob_plain/HEAD:/build-scripts/config/polipo.conf) опубликованной на сайте Torproject.

Обратите внимание, что polipo не требуется если вы хотите использовать прокси SOCKS 5, который доступен на порту 9050 после запуска Tor. Если вы хотите использовать Chromium через сеть Tor вам не требуется пакет polipo. Об использовании см. выше.

**Privoxy**

Privoxy - это HTTP-прокси, который использует SOCKS4a и может фильтровать html/cookie. Установить и настроить его поможет статья [**Privoxy**](https://wiki.archlinux.org/index.php/Privoxy).

Добавьте

forward-socks4a / localhost:9050 . # Не забудте точку в конце

в файл /etc/privoxy/config. Убедитесь,

chown privoxy:privoxy /etc/privoxy/config

что на него выставлены нужные права.

Выполните следующие команды:

mkdir /var/log/privoxy

touch /var/log/privoxy/errorfile

touch /var/log/privoxy/logfile

chown -R privoxy:adm /var/log/privoxy

Удостоверьтесь, что имя компьютера, записаное в /etc/rc.conf (параметр HOSTNAME) совпадает с именем, записанным в /etc/hosts.

Запустите демоны tor и privoxy

/etc/rc.d/tor start

/etc/rc.d/privoxy start

Также, их можно добавить в автозапуск в файл /etc/rc.conf

DAEMONS=(syslog-ng ... privoxy tor)

**Tor и Privoxy в Firefox**

Настройте прокси в Firefox:

Hostname: 127.0.0.1 Port: 8118

Можно также добавить необходимые исключения.

**Tor и Privoxy в других приложениях**

Вы можете использовать Privoxy для интернет-пейджеров (Jabber, IRC) и прочих приложений. Просто укажите IP-адрес и номер порта (127.0.0.1 port 8118).

Чтобы использовать SOCKS прокси напрямую вы можете указать приложению на Tor непосредственно (127.0.0.1 port 9050). Недостатоком методя является возможность самостоятельной посылки DNS-запросов приложением в обход Tor. Рассмотрите возможность использования SOCKS4A (например, через Privoxy) вместо нее.

Запуск сервера Tor

**Настройка**

Вы должны иметь скорость доступа в интернет не менее 20кб/с:

Nickname <tornickname>

ORPort 9001

BandwidthRate 20 KB # Замедлить трафик до 20кб/с

BandwidthBurst 50 KB # Но позволить всплески до 50кб/с

Allow irc ports 6660-6667 to exit from node:

ExitPolicy accept \*:6660-6667,reject \*:\* # Разрешить IRC порты, но не более

Run Tor as an exit node:

ExitPolicy accept \*:119 # Принимать nntp тажке как и политики выходных нод по умолчанию

Run Tor as middleman ( a relay):

ExitPolicy reject \*:\*

TorDNS

Tor версий 0.2.x имеет встроенный механизм перенаправления DNS-запросов. Чтобы включить его, добавьте следующую строку в конфигурационный файл:

/etc/tor/torrc

DNSPort 9053

AutomapHostsOnResolve 1

AutomapHostsSuffixes .exit,.onion

И перезапустите Tor, чтобы он подхватил новые настройки:

/etc/rc.d/tor restart

Это позволит Tor принимать запросы (например слушать 9053 порт в этом примере) как обычному DNS-серверу, и разрешать домены по сети Tor. Недостатком является то, что становится возможным разрешать только A-записи; MX и NS запросы будут проигнорированы. См. [**документацию для Debian**](https://techstdout.boum.org/TorDns/).

DNS запросы могут быть осуществлены средствами коммандного интерпретатора, используя tor-resolve. For example:

$ tor-resolve archlinux.org

66.211.214.131

"Торификация"

"Торификация" (torify) позволяет использовать приложение через сеть Tor без каких либо дополнительных настроек в самом приложении. Выдержка из man page:

torify - это простая оболочка, вызывающая tsocks с конфигурационным файлом

tsocks представляет собой оболочку между библиотекой tsocks и приложением, которое вы хотите соксифицировать

Пример использования:

$ torify elinks checkip.dyndns.org

$ torify wget -qO- https://check.torproject.org/ | grep -i congratulations

Учтите, что torify не будет выполнять поиск DNS через Tordns. Для этого придётся использовать его в сочетании с tor-resolve (описано выше). В этом случае процедура для первого из приведенных примеров будет выглядеть следующим образом:

$ tor-resolve checkip.dyndns.org

208.78.69.70

$ torify elinks 208.78.69.70

Решение проблем

**Проблема с пользовательским значением**

Если демон tor не запускается, выполните следующую комманду от root:

# tor

Если вы получили следующую ошибку:

May 23 00:27:24.624 [warn] Error setting groups to gid 43: "Operation not permitted".

May 23 00:27:24.624 [warn] If you set the "User" option, you must start Tor as root.

May 23 00:27:24.624 [warn] Failed to parse/validate config: Problem with User value. See logs for details.

May 23 00:27:24.624 [err] Reading config failed--see warnings above.

Она означает проблемы с пользовательскими значениями. Приступим к решению проблемы.

Узнайте права доступа к папке /var/lib/tor:

# ls -l /var/lib/

Если права /var/lib/tor такие же как указанные ниже, то это значит, что директория является собственностью пользователя *tor* группы *tor*.

drwx------ 2 tor tor 4096 May 12 21:03 tor

Измените владельца и группу:

# chown -R root:root /var/lib/tor

Теперь права доступы должны быть такими:

drwx------ 2 root root 4096 May 12 21:03 tor

Теперь откройте /etc/tor/torrc и найдите следующие строки:

## Uncomment this to start the process in the background... or use

## --runasdaemon 1 on the command line.

RunAsDaemon 1

User tor

Group tor

Закомментируйте строки *User tor* и *Group tor*:

## Uncomment this to start the process in the background... or use

## --runasdaemon 1 on the command line.

RunAsDaemon 1

#User tor

#Group tor

Сохраните и перезапустите демон **tor**. Теперь всё должно работать.

# /etc/rc.d/tor restart

Внешние ссылки

* [**Official Website**](https://www.torproject.org/)
* [**Unix-based Tor Articles**](https://trac.torproject.org/projects/tor/wiki#Unixish)
* [**Software commonly integrated with Tor**](https://trac.torproject.org/projects/tor/wiki/doc/SupportPrograms)
* [**How to set up a Tor *Hidden Service***](https://www.torproject.org/docs/tor-hidden-service.html.en)