

Tor



Tento návod je určen pro pokročilé uživatele



Tor je rychle se rozšiřující onion routing síť, která v současnosti nemá bezpečnostní chybu, přes kterou by se dala dohledat identita uživatele. Dokáže zabezpečit vysokou úroveň anonymity a umožní vám vystupovat pod jinou IP adresou, než je vaše vlastní. Tento článek popisuje instalaci Tor klienta pod Ubuntu.



Před instalací Toru je nutné si uvědomit, k čemu jej plánujete používat. Síť Tor NENÍ určena k tomu, aby se přes ni stahoval Warez a toto použití je nejen nepohodlné (pomalé), ale také velice bezohledné. Tor nemá dostatek konektivity k zabezpečení plynulého toku takového objemu dat a síť takové používání přetěžuje a znemožňuje použití těm, kteří ji doopravdy potřebují (například politicky nepohodlné osoby v Číně). Na stahování torrentů nebo velkých souborů z internetu NIKDY nepoužívejte, ve snaze vyhnout se případným trestním sporům ohledně autorských práv, síť Tor. K těmto účelům slouží například síť [Kademlia](#) nebo program [WASTE](#).

Instalace



V oficiálních zdrojích Ubuntu Universe se sice nachází balík Tor, ale je zastaralý a chybový, proto ho nepoužívejte!



Následující repozitář je z důvodu vyšší bezpečnosti [podepsán](#) GPG klíčem [886DDD89](#). Přidejte si ho mezi důvěryhodné pomocí [příkazu](#)

```
sudo apt-key adv --keyserver keys.gnupg.net --recv-keys 886DDD89
```



Podle vašeho [vydání](#) Ubuntu si do zdrojů softwaru [přidejte](#) jednu z následujících řádek:

```
deb http://deb.torproject.org/torproject.org oneiric main #Tor (Ubuntu 11.10)
deb http://deb.torproject.org/torproject.org lucid main #Tor (Ubuntu 10.04)
deb http://deb.torproject.org/torproject.org karmic main #Tor (Ubuntu 9.10)
deb http://deb.torproject.org/torproject.org jaunty main #Tor (Ubuntu 9.04)
deb http://deb.torproject.org/torproject.org intrepid main #Tor (Ubuntu
```

8.10)

```
deb http://deb.torproject.org/torproject.org hardy main #Tor (Ubuntu 8.04)
```



Poté **nainstalujte** balíky **tor** a **privoxy**.

Nastavení

Pro správnou funkci Toru je potřeba upravit soubor `/etc/privoxy/config`, což uděláte například **příkazem**

```
gksudo gedit /etc/privoxy/config
```

V souboru naleznete sekci **5.2** a v podsekci **Examples** odstraňte mřížku `#` na začátku následující řádky

```
# forward-socks5 / 127.0.0.1:9050 .
```

Dále v sekci **2.6** naleznete řádek

```
logfile logfile
```

a na jeho začátek mřížku `#` přidejte a soubor uložte.

Nyní už jen následujícím **příkazem** restartujte *privoxy*

```
sudo /etc/init.d/privoxy restart
```

Použití Toru



Použití *Toru* s sebou nese konfiguraci proxy serverů v příslušných programech. Pokud nějaký program nakonfigurujete pro spolupráci s *Privoxy* a potažmo použití *Toru*, nezapomeňte prosím vrátit po skončení používání *Toru* tuto konfiguraci zpět, jinak byste se mohli divit, proč ten internet leze jako šnek 😊. Navíc byste zbytečně vytěžovali již tak dost vytíženou síť *Tor* jejím běžným používáním.

Obecně



Síť *Tor* je přístupná pomocí lokálního proxy serveru *Privoxy*. Lze ji proto používat v jakémkoli programu, který podporuje proxy servery. Data pro konfiguraci „klienta proxy“ jsou následující:

Protokol	Server	Port
HTTP	localhost	8118
SSL	localhost	8118
Socks v5	localhost	9050

Přes konfiguraci proxy - Firefox

1. **Úpravy** → **Předvolby**
2. **Rozšířené** → **záložka Síť** → **tlačítko Nastavení připojení...**
3. Zaškrtnout **Ruční konfigurace proxy**
4. Vyplnit podle předešlé tabulky



Pro snadnou obsluhu si můžete nainstalovat [doplněk Torbutton](#).

Tipy

Ověření funkčnosti

1. Zjistěte si svou IP adresu. Bez použití *Privoxy* najedte Firefoxem na <http://www.whatsmyip.net> a poznamenejte si svou IP.
2. Nastavte svůj prohlížeč pro použití *Privoxy* a předešlý krok opakujte. Pokud se adresy liší, patrně jste postupovali správně.

Získání nové IP

Nejjednodušší způsob jak si vynutit přidělení nové adresy je restart démona *tor*. Provedete ho pomocí příkazu

```
sudo /etc/init.d/tor restart
```

Detekce veřejné IP adresy

Na ubuntuforums.org se objevil zajímavý způsob jak z příkazové řádky detekovat veřejnou IP adresu:

- První příkaz nasměruje *wget* přes *Privoxy* do TOR sítě
- Druhý příkaz ukáže (přes *wget*) veřejnou IP adresu, pod kterou je vidět prohlížeč surfující přes TOR síť
- Třetí příkaz ukáže (přes *wget*) veřejnou IP adresu, pod kterou je vidět prohlížeč surfující napřímo

```
export http_proxy="http://127.0.0.1:8118"
```

```
wget -q -O - checkip.dyndns.org|sed -e 's/.*Current IP Address: //' -e 's/<.*$//'  
wget --no-proxy -q -O - checkip.dyndns.org|sed -e 's/.*Current IP Address: //' -e 's/<.*$//'
```

Skript pro získání nové IP adresy

Pro použití v download managerech (např. [jdownloader](#)) je dobré mít skript, který provede obnovu veřejné IP adresy automaticky.

Alt+F2 otevře okno, do kterého vepište

```
gedit torinit.sh
```

v editoru zadejte následující text a uložte (# odstraňte jen pro účely testování, jinak budou všechny vaše TOR adresy logovány.)

```
sudo /etc/init.d/tor restart 2>&1 >/dev/null  
sudo /etc/init.d/privoxy start 2>&1 /dev/null  
#export http_proxy="http://127.0.0.1:8118"  
#echo ----- >> /tmp/tor.log  
#date >> /tmp/tor.log  
#wget -q -O - checkip.dyndns.org|sed -e 's/.*Current IP Address: //' -e 's/<.*$//' >> /tmp/tor.log
```

Alt+F2 otevře okno, do kterého vepište

```
chmod +x torinit.sh
```

Pro potlačení výzvy na zadání hesla je třeba autorizovat příkazy pomocí **visudo**





```
sudo visudo
```

a vložit na konec řádku příkazy

```
ALL ALL=NOPASSWD:/etc/init.d/tor *  
ALL ALL=NOPASSWD:/etc/init.d/privoxy *
```

Skript je k nalezení v domovské složce ~/torinit.sh

Odkazy

- [Domovská stránka programu](#) 
- [Pokyny k instalaci v Ubuntu](#) 
- [Tor - The Onion Router](#) 
- [Návod na serveru Root.cz](#) 

Rozšíření: Tento návod je příliš stručný. Pomozte Ubuntu Wiki tým, že jej rozšíříte. [Více...](#)

From:

<https://wiki.ubuntu.cz/> - **Ubuntu CZ/SK**

Permanent link:

<https://wiki.ubuntu.cz/tor>

Last update: **2019/02/25 18:20**

