Jak správně nastavit Tor server

Vložil/a cm3l1k1 [1], 13 Prosinec, 2011 - 10:36

- Anonymita [2]
- GNU/Linux a BSD [3]

V tomto článku shrnu "best practices" při nastavení Tor serveru v režimu Exit Node. Zde popsané nastavení používám i na svém serveru, který do bandwidthu Tor sítě přidává 2MB/s. Aktualně síť Tor tvoří cca 2500 serverů s celkovou kapacitou okolo 1TB/s.

Pro ty co neznají Tor bych doporučil si nejdříve přečíst tento článek [4].

Začal bych vysvětlením proč se zapojuji do sítě Tor. Tor nepoužívají jen spameři, lamy a warezáci, ale především osoby, které potřebují skrýt svou identitu před vládou, agenty, ISP apod. Jedná se o velmi široké spektrum uživatelů od soukromých osob, přes novináře, po osoby hlídané vládou, protože jsou pro ni potenciální hrozbou (Čína, Severní Korea apod.)

Prostě občas Tor potřebuje každý z nás, ať už třeba jen jako šifrovaný přístup přes nezabezpečenou WiFi. Pokud máte zájem o podrobnější vysvětlení, tak vás nasměruji sem: https://www.torproject.org/about/torusers.html.en [5]

Exit node vs Bridge node

- **Exit node** - je server, který je schopen přímo kontaktovat servery na Internetu, tj. pokud tvoří poslední část řetězce, tak iniciuje spojení a předává výsledky zpět. Bez exit nodů byste se nebyli schopni připojit k žádnému zdroji na Internetu a mohli byste jen používat služby sítě Tor (např. hidden services [6])
- **Bridge node** - tento typ serveru není viditelný ve veřejném seznamu Tor serverů a slouží jako přípojný bod do Tor sítě. Používá se když váš ISP blokuje na firewallu přístup do Tor sítě. Klient je schopen najít blízký Bridge node sám, nebo si můžete vyžádat zaslání informace o něm přes email. Více informací najdete zde: https://www.torproject.org/docs/bridges [7]

Instalace Tor serveru

Tor je součástí většiny balíčkovacích systémů, takže by neměl být nejmenší problém s jeho instalací.

```
#Gentoo
emerge tor
#Debian,Ubuntu,...
sudo apt-get install tor
#...
```

Pokud se rozhodnete Tor zkompilovat, tak jen ověřte že v systému již máte knihovnu libevent [8] a zbytek je notoricky známé:
./configure && make && make install
sudo useradd -d /home/tor -s /bin/false tor

Podrobnější instrukce zde (nejsou potřeba): https://www.torproject.org/docs/tor-doc-unix.html.en [9]

Konfigurace Tor serveru

Konfigurace se nachází v souboru /etc/tor/torrc a vzorový příklad uvádím zde. Hodnoty CHANGEME

prosím upravte podle sebe.

```
User tor
PIDFile /var/run/tor/tor.pid
Log notice syslog
DataDirectory /var/lib/tor/data
SocksPort 9050
DirPort 80
DirPortFrontPage /etc/tor/tor-frontpage.html
ORPort 8443
ORListenAddress CHANGEME:8443
Nickname CHANGEME
BridgeRelay 0
BandwidthRate 2 MB
AccountingStart day 12:00
AccountingMax 10 GB

ExitPolicy accept *:20-23     # FTP, SSH, telnet
ExitPolicy accept *:43        # WHOIS
ExitPolicy accept *:53        # DNS
ExitPolicy accept *:79-81     # finger, HTTP
ExitPolicy accept *:88        # kerberos
ExitPolicy accept *:110       # POP3
ExitPolicy accept *:143       # IMAP
ExitPolicy accept *:194       # IRC
ExitPolicy accept *:220       # IMAP3
ExitPolicy accept *:443       # HTTPS
ExitPolicy accept *:464       # kpasswd
ExitPolicy accept *:531       # IRC/AIM
ExitPolicy accept *:543-544   # Kerberos
ExitPolicy accept *:563       # NNTP over SSL
ExitPolicy accept *:706       # SILC
ExitPolicy accept *:749       # kerberos
ExitPolicy accept *:873       # rsync
ExitPolicy accept *:902-904   # VMware
ExitPolicy accept *:981       # Remote HTTPS management for firewall
ExitPolicy accept *:989-995   # FTP over SSL, telnets, IMAP over SSL, ircs, POP3 over
SSL
ExitPolicy accept *:1194      # OpenVPN
ExitPolicy accept *:1220      # QT Server Admin
ExitPolicy accept *:1293      # PKT-KRB-IPSec
ExitPolicy accept *:1500      # VLSI License Manager
ExitPolicy accept *:1533      # Sametime
ExitPolicy accept *:1677      # GroupWise
ExitPolicy accept *:1723      # PPTP
ExitPolicy accept *:1863      # MSNP
ExitPolicy accept *:2082      # Infowave Mobility Server
ExitPolicy accept *:2083      # Secure Radius Service (radsec)
ExitPolicy accept *:2086-2087 # GNUnet, ELI
ExitPolicy accept *:2095-2096 # NBX
ExitPolicy accept *:2102-2104 # Zephyr
ExitPolicy accept *:3128      # SQUID
ExitPolicy accept *:3389      # MS WBT
ExitPolicy accept *:3690      # SVN
ExitPolicy accept *:4321      # RWHOIS
ExitPolicy accept *:4643      # Virtuozzo
ExitPolicy accept *:5050      # MMCC
ExitPolicy accept *:5190      # ICQ
ExitPolicy accept *:5222-5223 # XMPP, XMPP over SSL
```

```
ExitPolicy accept *:5228      # Android Market
ExitPolicy accept *:5900      # VNC
ExitPolicy accept *:6660-6669 # IRC
ExitPolicy accept *:6679      # IRC SSL
ExitPolicy accept *:6697      # IRC SSL
ExitPolicy accept *:8000      # iRDMI
ExitPolicy accept *:8008      # HTTP alternate
ExitPolicy accept *:8074      # Gadu-Gadu
ExitPolicy accept *:8080      # HTTP Proxies
ExitPolicy accept *:8087-8088 # Simplify Media SPP Protocol, Radan HTTP
ExitPolicy accept *:8443      # PCsync HTTPS
ExitPolicy accept *:8888      # HTTP Proxies, NewsEDGE
ExitPolicy accept *:9418      # git
ExitPolicy accept *:9999      # distinct
ExitPolicy accept *:10000     # Network Data Management Protocol
ExitPolicy accept *:19294     # Google Voice TCP
ExitPolicy accept *:19638     # Ensim control panel
Exitpolicy reject *:*
```

Pár proměnných vysvětlím:

- **User** - uživatel pod kterým Tor server pobeží, nemělo by jít o příliš privilegovaného uživatele
- **SocksPort** - lokální SOCKS port, který mohou používat aplikace na serveru pro přístup do Tor sítě
- **DirFrontPage** - stránka, která se zobrazí pří přístupu na DirPort. Pokud je to možné, tak použijte port 80, protože pokud někdo najde vaší IP adresu v logu (útok, spam, ...), tak se může dozvědět že se jedná o Tor Exit node a jak je možné vás případně kontaktovat
- **ORPort** - port ke kterémů se budou připojovat klienti používající Tor síť. Ideálním portem je 80, nebo 443, protože nebývají blokovány na firewallech
- **ORListenAddress** - veřejná IP adresu serveru a ORport
- **Nickname** - nick serveru
- **BandwidthRate** - kolik bandwidthu může Tor maximálně použít
- **AccountingStart** - kdy se má vyresetovat statistika pro AccountingMax
- **AccountingMax** - maximum přenesených dat za časové období. Hodí se v případech kdy není možné poskytnout veškerý volný bandwidth, nebo když máte limit na počet přenesených dat. V našem příkladu je limit nastaven na 10GB denně.
- **ExitPolicy** - pravidla jako na firewallu povolující přístup na specifické porty, aby došlo k zamezení některých služeb, které vycucávají traffic a nemají na Tor síti co pohledávat (torrent například).

Vzorový soubor tor-frontpage.html přikládám na konci článku. Jen změňte text CHANGEME za vaši emailovou adresu. Originál jsem našel zde [10].

Tor v chrootu

Pro vyšší bezpečnost byste měli spustit Tor v chroot prostředí. Začněte tím, že stáhnete zdrojové kódy http://www.torproject.org/download-unix.html.en [11]

```
# add tor user
sudo useradd -d /home/tor -s /bin/false tor

# install
./configure --prefix=/tor
make
TORCHROOT=/home/tor/chroot
sudo mkdir -p $TORCHROOT
```

```
sudo make install prefix=$TORCHROOT/tor exec_prefix=$TORCHROOT/tor

# shared libraries
sudo mkdir $TORCHROOT/lib
sudo cp `ldd $TORCHROOT/tor/bin/tor | awk '{print $3}'|grep "^/"` $TORCHROOT/lib
sudo cp /lib/libnss* /lib/libnsl* /lib/ld-linux.so.2 /lib/libresolv* /usr/lib/
libnss3.so /usr/lib/libgcc_s.so.* $TORCHROOT/lib

# devices
sudo mkdir $TORCHROOT/dev
sudo mknod -m 644 $TORCHROOT/dev/random c 1 8
sudo mknod -m 644 $TORCHROOT/dev/urandom c 1 9
sudo mknod -m 666 $TORCHROOT/dev/null c 1 3

# conf files
sudo mkdir $TORCHROOT/etc
sudo sh -c "grep ^tor /etc/passwd > $TORCHROOT/etc/passwd"
sudo sh -c "grep ^tor /etc/group > $TORCHROOT/etc/group"
sudo cp /etc/nsswitch.conf /etc/host.conf /etc/resolv.conf /etc/hosts $TORCHROOT/etc
sudo cp /etc/localtime $TORCHROOT/etc

# dirs
sudo mkdir -p $TORCHROOT/var/run/tor
sudo mkdir -p $TORCHROOT/var/lib/tor
sudo mkdir -p $TORCHROOT/var/lib/tor2
sudo mkdir -p $TORCHROOT/var/log/tor
sudo chown tor:tor $TORCHROOT/var/run/tor
sudo chown tor:tor $TORCHROOT/var/lib/tor
sudo chown tor:tor $TORCHROOT/var/lib/tor2
sudo chown tor:tor $TORCHROOT/var/log/tor

# EDIT torrc configuration file

# test start
sudo chroot $TORCHROOT /tor/bin/tor
```

Více informací můžete nalézt zde: https://trac.torproject.org/projects/tor/wiki/doc/TorInChroot [12]

Další informace:
https://www.torproject.org/docs/faq.html.en [13]
https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment [14]

URL článku: https://security-portal.cz/clanky/jak-spr%C3%A1vn%C4%9B-nastavit-tor-server

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/gnu/linux-bsd
[4] http://www.security-portal.cz/clanky/tor-onion-router-syst%C3%A9m-pro-vysoce-anonymn%C3%AD-%C5%A1ifrovan%C3%BD-p%C5%99%C3%ADstup-k-internetu
[5] https://www.torproject.org/about/torusers.html.en
[6] https://www.torproject.org/docs/hidden-services.html.en
[7] https://www.torproject.org/docs/bridges
[8] http://www.monkey.org/~provos/libevent/
[9] https://www.torproject.org/docs/tor-doc-unix.html.en
[10] https://wiki.robert-marquardt.com/DirPortFrontPage
[11] http://www.torproject.org/download-unix.html.en
[12] https://trac.torproject.org/projects/tor/wiki/doc/TorInChroot
[13] https://www.torproject.org/docs/faq.html.en

[14] https://blog.torproject.org/blog/tips-running-exit-node-minimal-harassment