Tor-Nodes einfach betreiben, jetzt

Senf
https://senf.space/

Chemnitzer Linux-Tage 2025
2025-03-25, 12:00-13:00 Uhr, V6

Senf

- Seit 2010 Interesse an Amateurfunk
- Seit 2013 eigener Mailserver, XMPP-Server
- Seit 2014 Betrieb von Freifunk-Nodes (FFMD, FFBS)
- Seit ca. 2018 Betrieb von Tor-Nodes (bisher keine Exits)
- Viele Jahre in der Jugendarbeit tätig gewesen (u.a. Jufo)
- Mitglied u.a. im FifF e. V.
- Alles ein Gefrickel!

Tor

- Overlay-Netzwerk für TCP
- Verteiltes Netz mit dynamischer Routenwahl (Tor: 3)
- Daten werden *zwiebelartig* verschlüsselt
- Zweck: Anonymisierung und Zensurresistenz
  (Forschungen hierzu seit $>$ 40 Jahren)
- Annahme: Niemand kann Großteil des Clearnet überwachen

Größe des Netzes

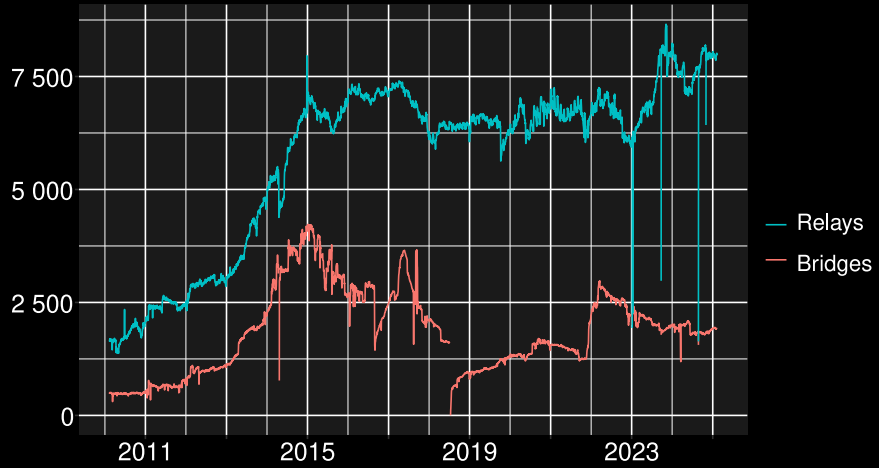

Abbildung 1: https://metrics.torproject.org/networksize.html

Top-10 countries by relay users

United States	415950	18.00 %
Germany	328300	14.20 %
Finland	124335	5.38 %
India	103557	4.48 %
Netherlands	70158	3.04 %
Indonesia	65597	2.84 %
United Kingdom	62096	2.69 %
France	57860	2.50 %
Republic of Korea	53923	2.33 %
Lithuania	48650	2.10 %

Tabelle 1:
https://metrics.torproject.org/userstats-relay-table.html;
Start: 2024-11-12; End: 2025-02-10

Top-10 countries by bridge users

Russia	64122	49.24 %
Iran	12515	9.61 %
United States	11485	8.82 %
Germany	4667	3.58 %
United Kingdom	2721	2.09 %
Netherlands	2685	2.06 %
China	2566	1.97 %
France	2556	1.96 %
India	1541	1.18 %
Canada	1158	0.89 %

Tabelle 2:
https://metrics.torproject.org/userstats-bridge-table.html;
Start: 2024-11-12; End: 2025-02-10

Problem: Bad relays

- Betrifft hauptsächlich Exits
- Traffic-Analysen → Deanonymisierung (Nutzende und hidden services)
- Auslassen von `MyFamily`-Inhalten
- (Bei Exit: Mitlesen von unverschlüsseltem Traffic, Manipulationen)
- „Please let us know by sending `bad-relays@lists.torproject.org`“ (Kriterien)

Zu wenige Nodes? (Kapazitäten)

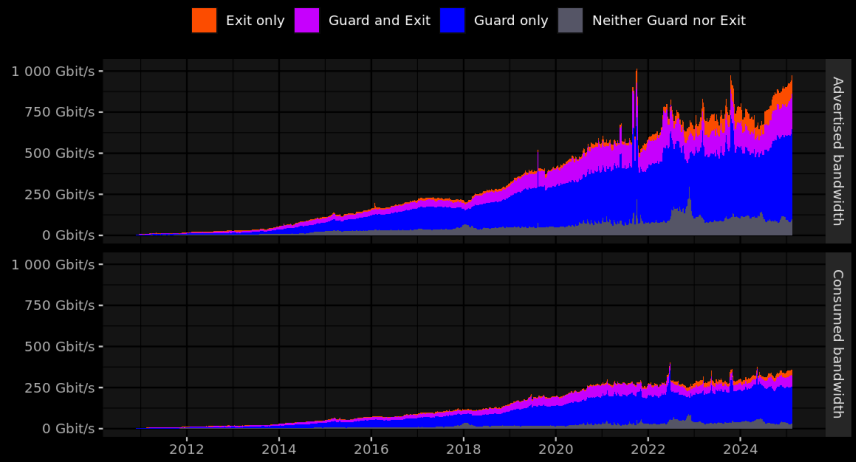

Abbildung 2: https://metrics.torproject.org/bandwidth-flags.html

Zu wenige Nodes?

- Kapazitäten müssen aktiven Störungen (z.B. (D)Dos) standhalten
- Erinnerung: **Verteiltes** Netzwerk ($\neg$ Mixkaskaden)
- Erinnerung: Niemand soll Großteil des Netzes besitzen

Problem: Konzentration auf wenige AS

„It is best to avoid hosts where many Tor relays are already hosted“(https://community.torproject.org/relay/technical-considerations/)

AS	Guard %	Middle %	Exit %
Hetzner (AS24940)	22.50	20.06	0
OVH (AS16276)	12.09	8.49	1.20
netcup (AS197540)	5.50	4.89	1.77
Sum	40.09	33.44	2.97

Tabelle 3: https://metrics.torproject.org/rs.html#aggregate/as

Problem: Konzentration auf wenige Staaten

Country	Guard %	Middle %	Exit %
Germany	40.08	33.53	30.48
Netherlands	11.13	18.96	26.13
Sweden	2.00	1.97	11.50
France	6.79	5.56	2.92
United States	3.52	7.29	4.35
Sum	63.52	55.71	75.38

Tabelle 4: https://metrics.torproject.org/rs.html#aggregate/cc

Fast alle Nodes mit Linux (1)

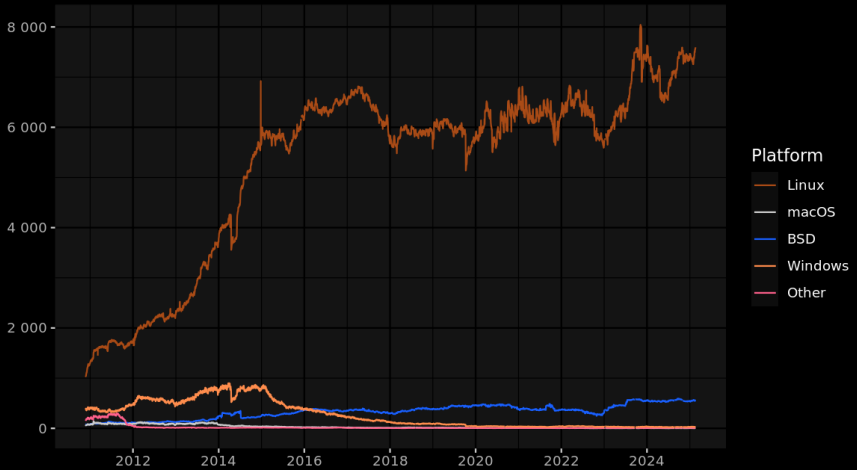

Abbildung 3: https://metrics.torproject.org/platforms.html

Fast alle Nodes mit Linux (2)

„We recommend using the operating system you are most familiar with, but if you're able, **the network would most benefit from BSD and other non-Linux based relays**. Most relays currently run on Debian."
(`https://community.torproject.org/relay/technical-considerations/`)

- Monokultur → SPOF
  (z.B. Debian RNG, aber auch gezielte Angriffe)

Verhaltensänderung durch Überwachung (1)

- Wenig erforscht, vorwiegend Kriminalitätsprävention
- Überwachung verlagert Kriminalität in nicht überwachte Bereiche
- Überwachte Gebiete als Orte der Kriminalität wahrgenommen
- Generalverdacht entsteht (*Wer Anonymität will, handelt kriminell*)
- Grenzen zwischen konformen Handeln und Straftaten sinkt

(https://soztheo.de/stadtsoziologie/videoueberwachung/)

Augenbilder bringen Geld

Videoüberwachung verändert Verhalten

Überwacht bis in die Kaffeeküche

Gefühlte Überwachung beginnt schon, bevor eine Kamera montiert ist. Doch was fehlt, sind unter anderem Langzeitstudien. Die sollen klären, wie Menschen damit umgehen.

Schon ein Warnschild reicht aus, damit die sich beobachtet fühlenden Menschen sich anders verhalten. Bild: ap

Öko / Wissenschaft 23. 4. 2010, 02:00 Uhr

SVENJA BERGT
Redakteurin für Wirtschaft und Umwelt

SVENJA BERGT
Redakteurin für Wirtschaft und Umwelt

Verhaltensänderung durch Überwachung (3)

- Michel Foucault: *Überwachen und Strafen: Die Geburt des Gefängnisses*, 1975
- Untersuchung von **Macht**- und Wahrheitsstrukten in Gefängnissen
- Überwachung alltäglich ($\rightarrow$ Macht als etwas Ungreifbares)

(https://www.deutschlandfunkkultur.de/michel-foucault-ueberwachen-und-strafen-wie-die-macht-das-html)

Panopticon (1)

Abbildung 5:
https://de.wikipedia.org/wiki/Datei:Presidio-modelo2.JPG,
User: Friman, 2022-12-05

Panopticon (2)

- Entworfen von Jeremy Bentham, 1791
- Überwachungsdruck $\rightarrow$ regelkonformes Verhalten
- Sozialdarwinismus: Überwachung setzt sich durch: erhöht Produktivität, senkt Aufwand für Autorität

Einfluss von Zensur auf Verhalten

- Sprachökonmie in autoritären Systemen verbreitet (*Neusprech*)
- Sapir-Whorf-Hypothese (1954): Eigenschaften der Sprache beeinflussen Denken
- Verhindert Zensur unerwünschtes Verhalten?
- Tritt auch hier Normierung auf? ($\rightarrow$ Selbstzensur)

Eigenen Node aufsetzen und Teil des Tor werden!

Voraussetzungen für ein Relay

- Aus Clearnet erreichbarer TCP-Port
- Viele Verbindungen aufbaubar ($\rightarrow$ 7k Relays)
- $>=$ 512 MB RAM; 200 MB disk storage; AESNI-CPU empfohlen
- Upload: $>=$ 10 Mbps (16 Mbps empfohlen), $>=$ 100 GB/month ($>=$ 2TB/m empfohlen)
- Korrekte Zeit (NTP, GPS)
- IPv4 notwendig; NAT, IPv6 empfohlen
- IP-Adressen müssen mind. 3h stabil sein
- Hypervisor zulässig

Good providers

- https://community.torproject.org/relay/community-resources/good-bad-isps/
- Zusätzlich AGB lesen
- Bridges lassen sich problemlos zuhause betreiben

Eigene Erfahrungen (ISP)

- netcup: Kaum Ausfälle, aber *BSD nicht nutzbar
- Durch Zufall: Einziger Node bei active-servers.de, aber: „Running Tor nodes in the main network (AS) is not prohibited but network speed is limitted to 1MB/s“
- (VP-)Server in anderen Ländern recht teuer; ändert sich inzwischen
- Gcore: Eigene Images nur auf teuren Servern; default firewall blockt vieles weg
- HostHatch, 1984.network: TODO

Installation: [GNU|BSD*]/Linux

- Einige Distributionen (Deb, RHEL) haben eigenes Tor-Repo
- Automatische Updates aktivieren (z.B. `dnf-automatic`)
- `[apt | dnf | zypper] install tor` oder äquivalent

Installation: OpenBSD

- Automatische Updates bauen (Anleitung)
- `pkg_add tor` (und evtl. `obfs4proxy`)
- Anzahl offener Dateien je Prozess erhöhen (je Relay eine):
  `/etc/login.conf`: `openfiles-max=13500; tc=daemon`
  `echo kern.maxfiles=16000 | tee -a /etc/sysctl.conf`
- `rcctl enable tor`
- `pledge` afaik noch nicht implementiert

Eigene Erfahrungen (OS)

- Debian, Devuan (init freedom), Alma, Rocky, Alpine, Void, OpenWRT: Keine Probleme bei der Einrichtung, kaum Ausfälle
- FreeBSD, **OpenBSD**: genauso
- Raspberry Pi (2) zu schmal
- zusätzlicher Wartungsaufwand: öhm, keiner?
- Anleitungen auf `https://community.torproject.org/relay/` erklären alles

torrc (allgemein)

- Immer hilfreich: `man tor`
- `DataDirectory`
  Verzeichnis für Daemon (enthält Keys, etc.)
- `Log` (`notice`, `debug`)
  Speicherort für Logs (`file`, `syslog`)
- `ContactInfo`
  Kontaktinformationen zum Betreiber, optional: GPG-Fingerprint; alt. Spez: `https://nusenu.github.io/ContactInfo-Information-Sharing-Specification/`
- `Nickname`
  Name des Nodes (`[a-zA-Z0-9]`)

torrc (allgemein, Netzwerk)

- `SocksPort`, `SocksPolicy`
  SOCKS-Proxy im geschlossenen Netz (localhost, LAN)
- `ORPort`
- `Address`
  (Leave commented out and Tor will guess)
- `AccountingMax`
- `RelayBandwidthRate`, `RelayBandwidthBurst`

torrc (Weiteres für Relay)

- Keinen SOCKSPort nutzen (Download $\neq$ Upload)
- `MyFamily`
  Fingerprints weiterer Nodes
- `ExitPolicy reject *:*`
  Relay ist explizit non-exit
- `DirPort`
  Metadaten zu Netzwerk teilen (auch TODO für mich)

Bridges

- Liste an Relays systembedingt öffentlich
- $\rightarrow$ können leicht gesperrt werden
- Bridge: Client teilt seine Verbindung mit anderen
- User $\rightarrow$ Bridge Relay $\rightarrow$ Middle Relay $\rightarrow$ Exit Relay
- Erreichbarkeit der Bridge wird versteckt
- Erweiterung: `obfs4proxy`, implementiert Verwirrungstechniken
- Auch möglich: Webtunnel, Verwirrung durch HTTPS

Aufsetzen einer Bridge

- Voraussetzung: >= 1 Mbps
- Optional: Informationen an `mailto:frontdesk@torproject.org` senden
  They will share your bridge with people who really need it!

Aufsetzen einer Bridge unter FreeBSD

- Demo; Vorbereitung :
  - `ORPort=3333/tcp; obfs4 port=6666/tcp` in Firewall öffnen
  - FreeBSD installiert
  - `pkg install curl vim screen`
  - SSH-Pubkey in `.ssh/authorized_keys`
- Anleitung: https://community.torproject.org/relay/setup/bridge/freebsd/

Node zuhause betreiben

- Bisher nur mit Bridges getestet, Relays tun angeblich auch
- Andere Clients im LAN nutzen Bridge mit (`SocksPort`, `SocksPolicy`)
- Empfehlung: isoliertes System (VM, Thinclient)

Für Faule: Script

- Plan: `sh`-Script soll Aufsetzen interaktiv vereinfachen
- Realität: noch nicht fertig
- Versprechen: liefere ich nach!
- Ansible: `http://github.com/nusenu/ansible-relayor`

Monitoring

- Logs lesen (Empfehlung: `Log notice file ...`)
- Öffentliche Informationen: https://metrics.torproject.org/
- E-Mail-Notify bei Anomalien: https://weather.torproject.org
- CLI-Tool (mit PNG-Export): vnstat

Weitere Schutzmaßnahmen

- `https://community.torproject.org/relay/setup/post-install/`
- Backups, insb. von `DataDir`, anlegen
- System härten (z.B. SSH: `PasswordAuthentication no`)
- Automatische Updates einführen
- Wenn möglich: physischer Schutz

Rechtliches: Eigene Erfahrungen

- Keine juristischen Verfahren
- . . . auch bei leichter Fehlkonfiguration
- Abuse-Meldungen (Relay): kurze Mail an ISP reichte
- Vereinzelt: Blacklists
- An alle Node-Betreiber: Großes Lob
  („wir machen uns öffentlich, damit andere anonym sein können“)

Digitale Selbstverteidigung

Auch, wenn ihr keine Tor-Services betreibt:

- Härtet Systeme, auch physisch!
  (FLOSS wo geht, encrypted BD, hidden Backups, HW-Tokens, . . .)
- Propagiert dezentrale Systeme und Kommunikationsprotokolle!
- Sorgt aktiv für Datensparsamkeit! ($\rightarrow$ verschickt DSGVO-Anfragen)
- Wählt keine Parteien, die Überwachung oder Zensur wollen!
- Seid smart und werft endlich diese „Smart“phones weg!
- **Nutzt und propagiert Tor!** (mehr Nutzende $\rightarrow$ höhere Anonymität)
- Und werbt/helft in eurem Bekanntenkreis dafür!

Privacy-Handbuch

- Seit Dezember 2024 bei mir
- Wird in den nächsten Monaten überarbeitet (dringendes TODO für mich)
- **Suche Mithilfe für Firefox-`user.js`**
- URL clearnet: `https://privacy-handbuch.de/`
- hidden service: `http://pcuuisbefrw2vp3kp2z5c5rexzx3gfpa4lfbu6qxuw2gdlecl4ydw6ad.onion/`

Nodes von/mit Senf

Lassen sich in `torrc` mit `EntryNodes` setzen

- Senfrelay; **EOL: 2025**; `relay.senf.space:443`
  `33753E702B8F2BC2FF0EA99D322B07198A3F2C8F`
- Senfkekse; FreeBSD; active-servers; **nur 1MB/s**
  `kekse.senf.space:1994`
  `D01C6B5AC88CAB5CE294759842F5BA4BC69621D9`
- privacyandbuch; Alpine Linux; netcup;
  `privacy-handbuch.de:9091`
  `086765190E937746208F92F1882B402C87A9FE4A`
- senftashkent; Alpine Linux; Gcore; `tashkent.senf.space:8443`
  `68EA568AFFA96730BF30FD27EB6D4AA5D2A260B1`
- catgirl; Debian GNU/Linux; netcup; `catgirl.senf.space:9001`
  `B6B842FB52E5C4FD0CAD432ADB6C7F46E8112A55`

Bridges von Senf

- Können persönlich erfragt werden
- Details liegen hier ausgedruckt vor
- Jede Person bekommt maximal eine Bridge
- Grund: Einrichten von Sperren vermeiden

Zitat aus Privacy-Handbuch

Die unbeobachtete, private Kommunikation schafft keine rechtsfreien Räume im Internet, wie Demagogen des Überwachungsstaates immer wieder behaupten.

Sie ist ein grundlegendes Menschenrecht, das uns zusteht. Nach den Erfahrungen mit der Diktatur Mitte des letzten Jahrhunderts findet man dieses Grundrecht in allen übergeordneten Normenkatalogen, von der UN-Charta der Menschenrechte bis zum Grundgesetz der BRD.