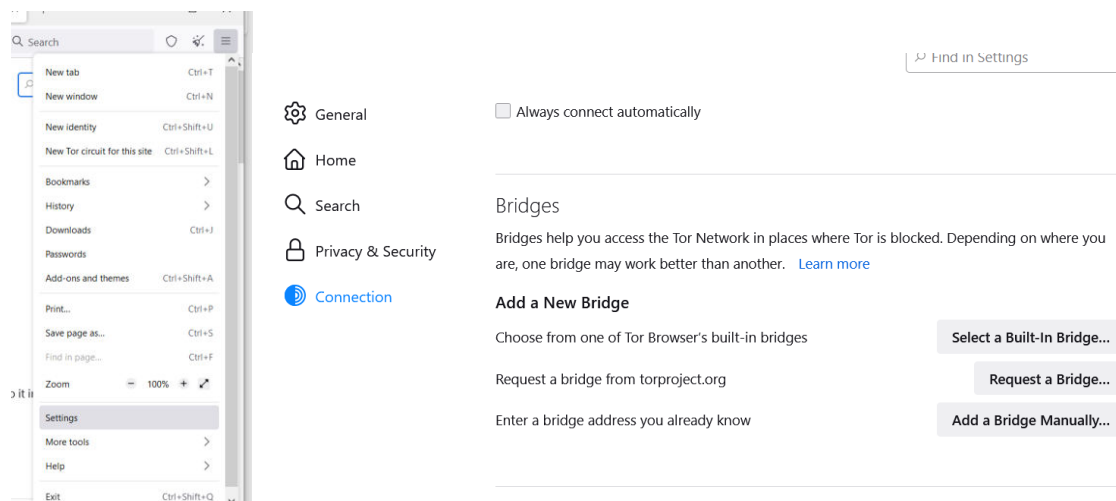


3. Übungsaufgabe: Praktische Übungen zu TOR

Verwenden Sie das aktuelle TOR Browser Bundle und beantworten Sie dann folgende Fragen bzw. führen Sie die Anweisungen aus. Dokumentieren Sie, dass Sie die Anweisungen ausgeführt haben, z.B. durch Screenshots:

- a) Aus wie vielen ORs (auch Relays genannt) können Sie bei der Erstellung eines Circuits wählen? Woher erhält der TOR-Client die Liste aller Relays?

Zu Bridges



Entrynodes d) Exitnodes funktioniert analog zu d)

Für den Mittleren braucht man eine externe Software

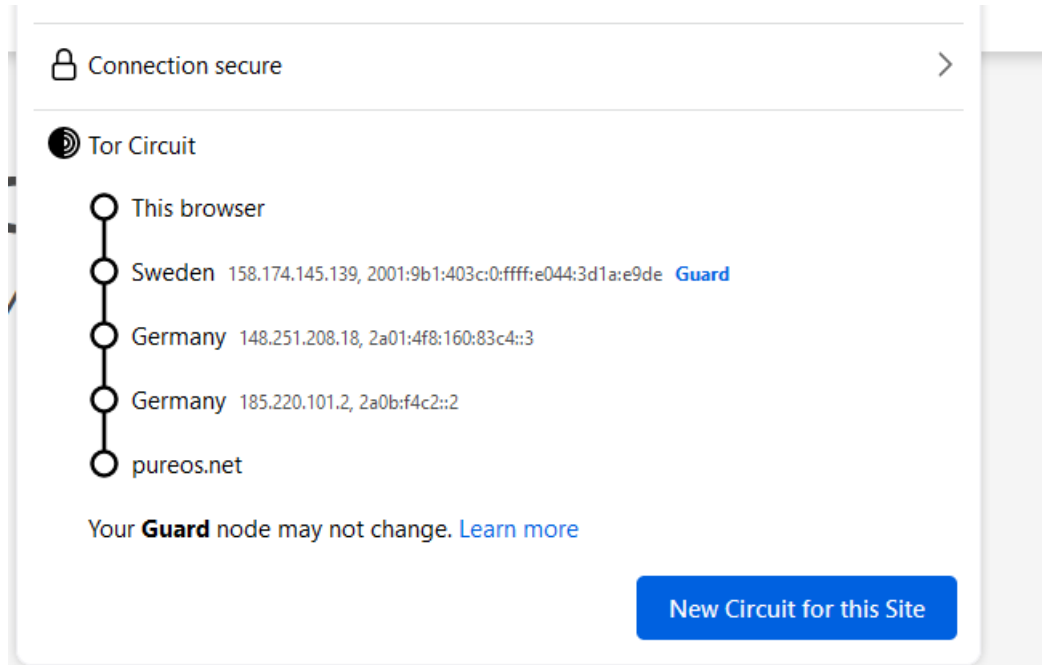
Es werden immer mindestens drei Knoten verwendet. Insgesamt stehen laut <https://torstatus.rueckgr.at/> derzeit 6.650 Tor-Knoten zur Verfügung, davon 1.415 Exit-Knoten.

Im Tor-Netzwerk gibt es Verzeichnisserver, die die Liste vorrätig halten. Von diesen wird die Liste beim Verbindungsaufbau abgefragt.

- b) Ist Ihre Installation ein TOR-Client, ein Non-Exit-Relay oder ein Exit Relay? Warum ist diese Voreinstellung wichtig? Welche Voreinstellungen sind dazu in der Standard-Installation getroffen?

Einfach nur ein TOR-Client. Das ist wichtig, weil man sich sonst eventuell unbeabsichtigt an illegale Aktivitäten beteiligt (Exit Relay)

Standard-Installation geöffnet:
 c) Aus wie vielen Hops besteht ein TOR Circuit?



3

d) Wie können Sie bestimmte EntryNodes auswählen?

-Speicherort TOR Öffnen, TORBrowser, Data, Tor, torrc Datei suchen

defaults	09.12.2022 18:32	Dateiordner	
fonts	09.12.2022 18:32	Dateiordner	
TorBrowser	09.12.2022 18:33	Dateiordner	
Accessible.tlb	01.01.2000 01:00	TLB-Datei	3 KB
AccessibleHandler.dll	01.01.2000 01:00	Anwendungserwei...	330 KB
AccessibleMarshal.dll	01.01.2000 01:00	Anwendungserwei...	25 KB
application	01.01.2000 01:00	Konfigurationseins...	1 KB
d3dcompiler_47.dll	01.01.2000 01:00	Anwendungserwei...	4.245 KB
Data	09.12.2022 18:32	Dateiordner	
Docs	09.12.2022 18:32	Dateiordner	
Tor	09.12.2022 18:32	Dateiordner	
UpdateInfo	09.12.2022 19:39	Dateiordner	

Name	Änderungsdatum	Typ	Größe
Browser	09.12.2022 18:33	Dateiordner	
Tor	09.12.2022 20:13	Dateiordner	

Name	Änderungsdatum	Typ	Größe
keys	09.12.2022 18:33	Dateiordner	
onion-auth	09.12.2022 18:33	Dateiordner	
pt_state	09.12.2022 18:34	Dateiordner	
cached-certs	09.12.2022 18:33	Datei	19 KB
cached-microdesc-consensus	09.12.2022 20:12	Datei	2.066 KB
cached-microdescs	09.12.2022 18:58	Datei	7.458 KB
cached-microdescs.new	09.12.2022 20:13	NEW-Datei	26 KB
control_auth_cookie	09.12.2022 19:39	Datei	1 KB
geoip	01.01.2000 01:00	Datei	3.970 KB
geoip6	01.01.2000 01:00	Datei	6.132 KB
lock	09.12.2022 19:39	Datei	0 KB
state	09.12.2022 20:13	Datei	8 KB
torrc	09.12.2022 20:07	Datei	1 KB
torrc.orig.1	01.01.2000 01:00	1-Datei	0 KB
torrc-defaults	01.01.2000 01:00	Datei	1 KB
unverified-microdesc-consensus	09.12.2022 18:33	Datei	2.065 KB

Öffnen mit editor

```

torrc - Editor
Datei Bearbeiten Format Ansicht Hilfe
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1, and Tor will ignore it

ClientOnionAuthDir C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\onion-auth
DataDirectory C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor
GeoIPFile C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip
GeoIPv6File C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6

```

Entsprechende EntryNode wählen und das reinschreiben:

```

torrc - Editor
Datei Bearbeiten Format Ansicht Hilfe
# This file was generated by Tor; if you edit it, comments will not be preserved
# The old torrc file was renamed to torrc.orig.1, and Tor will ignore it

ClientOnionAuthDir C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\onion-auth
DataDirectory C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor
GeoIPFile C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip
GeoIPv6File C:\Users\Tim\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\geoip6

```

EntryNodes {fr} StrictNodes 1

Wir wählen die
EntryNode von
Frankreich, weil wir
Baguette so gerne
mögen

Wir wollen auf jeden Fall
über fr gehen

Man kann auch mehrere
angeben, falls fr
wegfallen sollte

h) Wie läuft die Namensauflösung über TOR? Welche DNS-Server werden genutzt?

TLD=Top-Level-Domain, **höchste Ebene der Namensauflösung**

-Die Namensauflösung für .onion wird von den Directory Servern gemacht.

-Für alle anderen TLDs wird der Ausgangsknoten die DNS-Auflösung übernehmen.

Die Übermittlung der DNS-Anfragen an das Tor-Netzwerk erfolgt über SOCKS 4a Protokoll

Bei Nutzung eines SOCKS Proxy ist für alle Netzanwendungen und -dienste der SOCKS Proxy der „Ansprechspartner“, die Netzanwendungen verbinden sich immer zum SOCKS Proxy und dessen Port, der die Anfragen durch die Firewall zum Zielrechner weiterleitet und umgekehrt die Antworten an die Netzanwendungen zurückleitet

i) Besuchen und verwenden Sie die Suchmaschine www.google.com mit TOR?
Was fällt auf? Tipp: Sie müssen ggf. einige Exit-Nodes durchprobieren.

Google benutzt die Sprache der Exit-Nodes und nicht der Sprache in der mein Browser eingestellt ist (Englisch). Hier polnische Sprache



Exit-Node Polen

Connection secure

Tor Circuit

This browser

France 62.210.123.24, 2001:bc8:30c6:100::dead **Guard**

Sweden 98.128.173.1

Poland 95.214.52.156

google.com

Your **Guard** node may not change. [Learn more](#)

New Circuit for this Site

nie pamiętasz adresu: