

Zu Bridges

Ein Bild, das Text enthält.

Automatisch generierte BeschreibungEin Bild, das Text enthält.

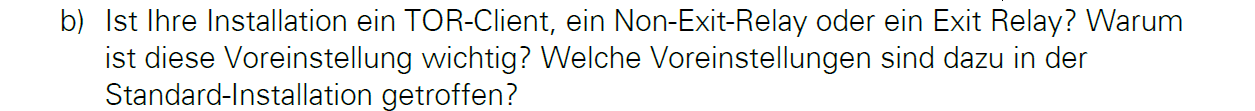
Automatisch generierte Beschreibung

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.



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



Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

3



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

Ein Bild, das Tisch enthält.

Automatisch generierte Beschreibung

Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Ein Bild, das Tisch enthält.

Automatisch generierte BeschreibungEin Bild, das Text enthält.

Automatisch generierte Beschreibung

Öffnen mit editor

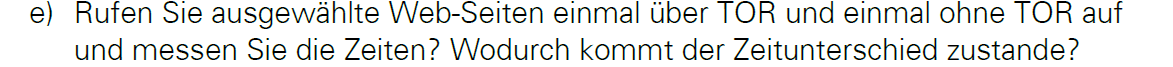
Ein Bild, das Text enthält.

Automatisch generierte Beschreibung

Entsprechende EntryNode wählen und das reinschreiben:

Ein Bild, das Text enthält.

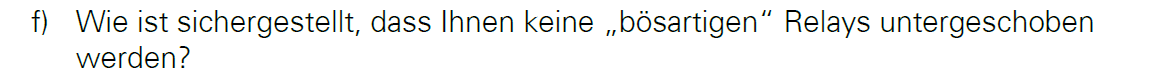
Automatisch generierte Beschreibung



Ohne Tor ca 2s

Mit Tor 15s

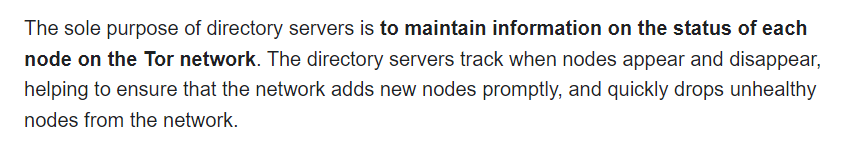
Weil wir bei TOR eine Schicht mehr haben, also 3 statt 2, ist der Aufwand entsprechend höher.



„Einige Exit-Knoten (englisch: Nodes) werden von Menschen mit bösen Absichten aufgestellt, um die Daten, die über sie an den richtigen Webserver gehen, mitzuschneiden. Tor kann dies nicht verhindern. Daher sollte man, wenn man wichtige Daten wie Login-Daten und Passwörter per Tor versendet, eine End-to-End-Verschlüsselung wie [SSL](https://de.wikipedia.org/wiki/Transport_Layer_Security) benutzen. Die meisten Anwendungen und Webseiten erlauben dies, und so wird das Surfen mit Tor sicherer.“

Neben dieser Empfehlung, kann man böse Relays reporten. Außerdem sucht Tor selber nach diesen um sie auszusortieren.





Es gibt 9Ein Bild, das Tisch enthält.

Automatisch generierte Beschreibung



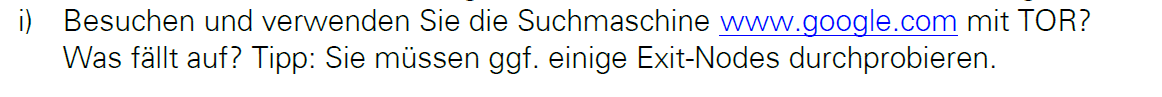
TLD=Top-Level-Domain, **höchste Ebene der Namensauflösung**

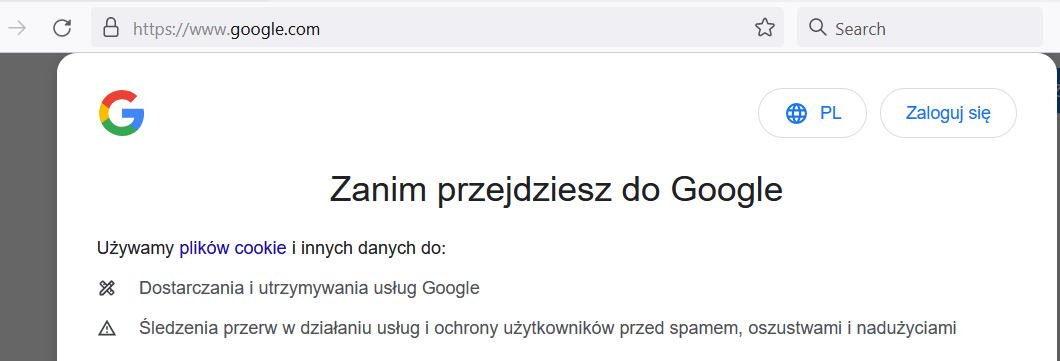
-Die Namensauflösung für .onion wird von den Directory Servern gemacht.

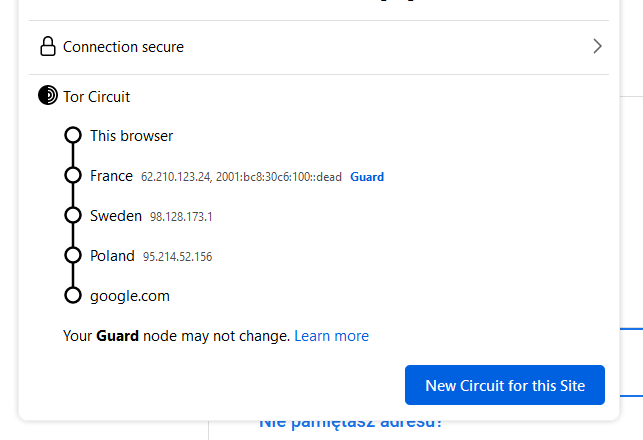
-Für alle anderen TLDs wird der Ausgangsknoten die DNS-Auflösung übernehmen.

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 Netzanwednungen zurückleitet



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



Exit-Node Polen