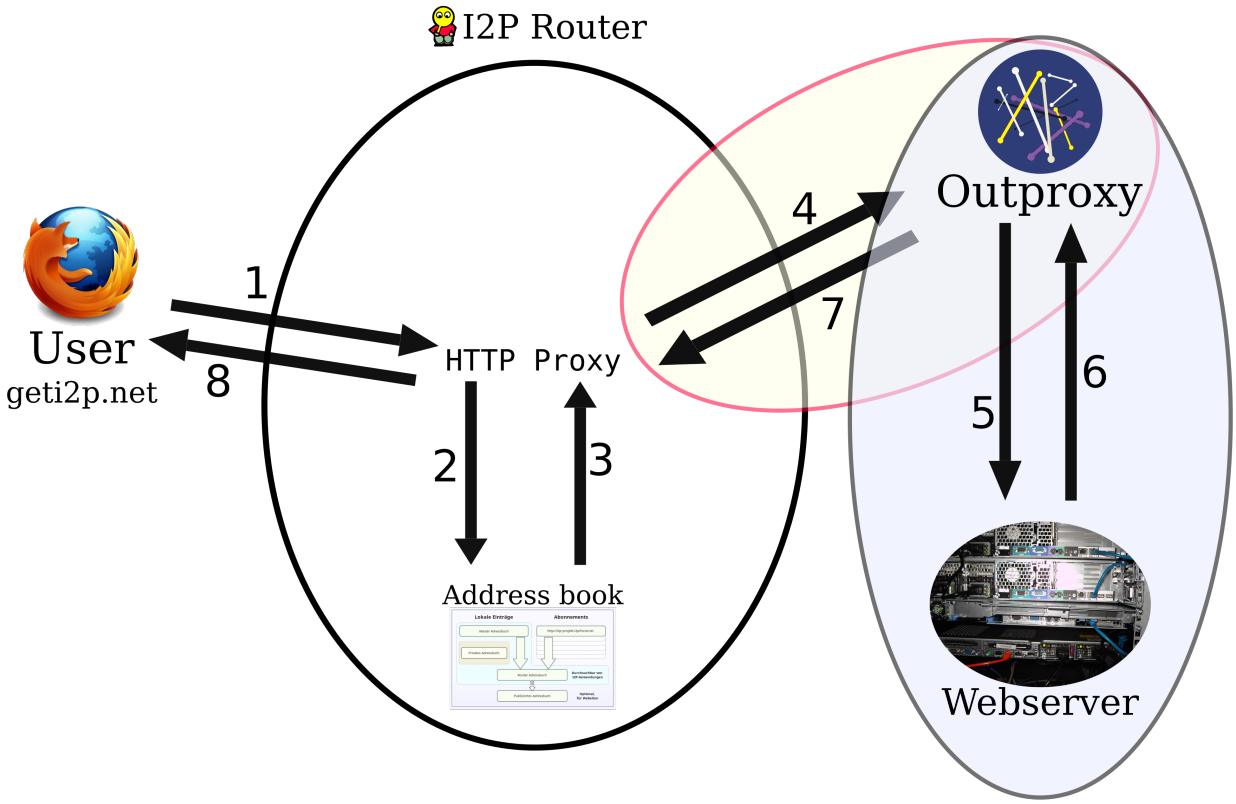
Outproxies in I2P

Was ist ein Outproxy?

I2P an sich ist ein internes Netzwerk. Dies bedeutet, dass es ohne Hilfe keine Verbindung mit anderen Netzwerken aufbauen kann. Man kann also nur auf interne Seiten sogenannte Eepsites zugreifen. Man kann also ohne Hilfe auch nicht mit dem Internet oder dem Tor-Netzwerk kommunizieren und darauf zugreifen. Ein Outproxy fungiert also als Hilfe, damit I2P mit anderen Netzwerken kommunizieren kann.

Wie funktioniert ein Outproxy?

Versucht man eine Eepsite aufzurufen, schaut I2P im Adressbuch nach der entsprechenden Adresse. Analog dazu ist das Telefonbuch. Man weiß den Namen (Eepsite) und man versucht die Telefonnummer (Ziel) zu finden. [siehe auch DNS im WWW] Als nächstes versucht I2P die Eepsite zu kontaktieren und man kann surfen. Dies funktioniert so bei Clearnet-Seiten nicht.
Damit man trotzdem im Clearnet surfen kann, gibt es Outproxies:
Wenn man versucht, eine Clearnet Seite aufzurufen, erkennt I2P dies an der Endung und schaut nach ob ein oder mehrere Outproxies eingerichtet wurden sind. Wenn nein, gibt I2P eine Fehlermeldung aus. Wenn ja, schaut I2P im Adressbuch nach der Adresse des Outproxies und kontaktiert diesen. Als nächstes wird die Anfrage (z. B. an Twitter oder DuckDuckGo) an den Outproxy gesendet. Dieser kontaktiert dann an Stelle des Benutzers die Website und empfängt eine Antwort. Diese leitet er an den Benutzer weiter. Der Outproxybetreiber hat also auch die Möglichkeit, den Verkehr des Benutzer mit zuschneiden, zu zensieren oder zu manipulieren.



1. Der Browser sendet die Anfrage an den HTTP Proxy des I2P Routers.
2. Der I2P Router sucht im Adressbuch nach dem Ziel für den Outproxy
3. Das Adressbuch übergibt das Ziel zurück
4. Die Anfrage wird an den Outproxy gesendet
5. Der Outproxy übermittelt im Auftrag die Anfrage an den Webserver
6. Der Webserver antwortet dem Outproxy
7. Der Outproxy leitet die Anfrage zurück an den HTTP Proxy
8. Der HTTP Proxy übergibt die Anfrage an den Browser und somit an den Benutzer

Wiederholung:
Der Benutzer möchte die Seite geti2p.net über das I2P Netzwerk mit Hilfe eines Outproxies aufrufen. Er gibt an einen konfigurierten Browser die Adresse ein und der Browser erstellt eine anfrage. Diese sendet er zum HTTP Proxy des I2P Router (Punkt 1). Der I2P Router schaut nun nach ob ein Outproxy eingestellt ist. Als nächstes holt der Router sich das Ziel (vergleichbar mit einer IP-Adresse im Clearnet) vom Adressbuch. Bei Punkt 2 sendet er die Anfrage an das Adressbuch und bei Punkt 3 bekommt er die Antwort. Als nächstes kann der Router den Outproxy kontaktieren. Nachdem die Verbindung erfolgreich hergestellt worden ist, sendet er die Anfrage an den Outproxy (Punkt 4). Der Outproxy wiederum leitet die Anfrage an den entsprechenden Webserver weiter (Punkt 5). Der Webserver antwortet dem Outproxy (Punkt 6) und denkt, dass nicht der eigentliche Nutzer sondern der Outproxy die Anfrage wollte. Nachdem der Outproxy die Antwort erhalten hat, leitet er diese an den I2P Router weiter (Punkt 7). Der I2P Router wiederum

leitet die Anfrage an den Browser zurück (Punkt 8). Damit hat der Benutzer die Seite erhalten.

Wie richte ich einen Outproxy ein?

Als erstes braucht man die Adresse des Outproxies. Leider gibt es im Moment sehr wenige Outproxies. Zu diesen gehören: *outproxy.bandura.i2p*, *false.i2p*, *outproxy-tor.meeh.i2p*
Alle drei leiten die Anfragen über das Tor-Netzwerk. Dies bedeutet das die Anfrage bei Punkt 5 und 6 durch das Tor-Netzwerk geleitet werden. Einer der Gründe, warum Outproxybetreiber dies tun, ist das es ihnen Rechtssicherheit gibt.
Als erstes geht im in die Tunnelliste im I2P Interface. Diese ist im Normalfall unter http://127.0.0.1:7657/i2ptunnelmgr zu finden. Dort wählt man den Tunnel aus, für welchen man den Outproxy konfigurieren möchte. Dort wählt man das Zahnrat⚙, um den Tunnel zu bearbeiten.
Als nächstes findet man unter „Ausgehende Proxies“ (*Outproxies*) bzw. „SSL-Ausgangsproxies“ (*SSL Outproxies*) eine Textbox. *Ausgehende Proxies* sind die Outproxies, welche I2P bei HTTP Verbindungen benutzt; *SSL-Ausgangsproxies* sind die Outproxies, welche bei HTTPS-Verbindungen benutzt werden. Dort trägt man die entsprechenden Outproxies ein.
Es ist auch möglich mehrere Outproxies einzutragen. Diese trennt man dann mit einem Komma. Bei einer Anfrage an einen Outproxy wählt der Router zufällig einen Outproxy aus.
Danach speichert man die Tunneleinstellungen und fertig!

***Achte darauf**, dass der Outproxy im Adressbuch eingetragen ist. Am besten kannst du es überprüfen, indem du die Adresse des Outproxies aufrufst. Erscheint die Meldung, dass die Adresse nicht im Adressbuch gefunden worden ist, kann man einen Jumper verwenden. Sonst kann man den Outproxy sofort benutzen.*

Welche Gefahr besteht bei der Nutzung von Outproxies?

Es besteht die Gefahr, dass der Outproxybetreiber böswillig ist und die Anfragen oder Antworten mitschneidet, also protokolliert, oder die Antworten manipuliert. Er kann aber auch, was nicht so schlimm ist, Seiten zensieren.

Es besteht in etwa die gleiche Gefahr wie bei der Nutzung des Tor-Netzwerkes. Der Unterschied besteht nur darin, dass das Tor-Netzwerk mehr Exit-Nodes hat als I2P Outproxies. Es wird daher empfohlen, dass wenn man im Clearnet surfen möchte, man Tor benutzt.

Glossar
Eepsite – Eine I2P interne Seite. Diese Domains haben immer die Endung .i2p
Ziel – Vergleichbar mit der IP-Adresse im Clearnet. Mit dem Ziel wird hier der Outproxy identifiziert

Anfrage – Dabei handelt es sich hier um eine HTTP-Anfrage. Diese enthält z. B. die Seite, die gewünschte Sprache und die Uhrzeit
Antwort – Dabei handelt es sich hier, um die Antwort auf die HTTP-Anfrage. Diese enthält den Code für die später im Browser dargestellte Seite
Webserver – Damit bezeichnet man die Computer, auf denen eine oder mehrere Webseiten liegen.
Clearnet – Dieser Begriff bezeichnet, dass „normale“ Internet; indem auch Twitter oder DuckDuckGo zu Hause sind.