

Outproxies in I2P

What is an outproxy?

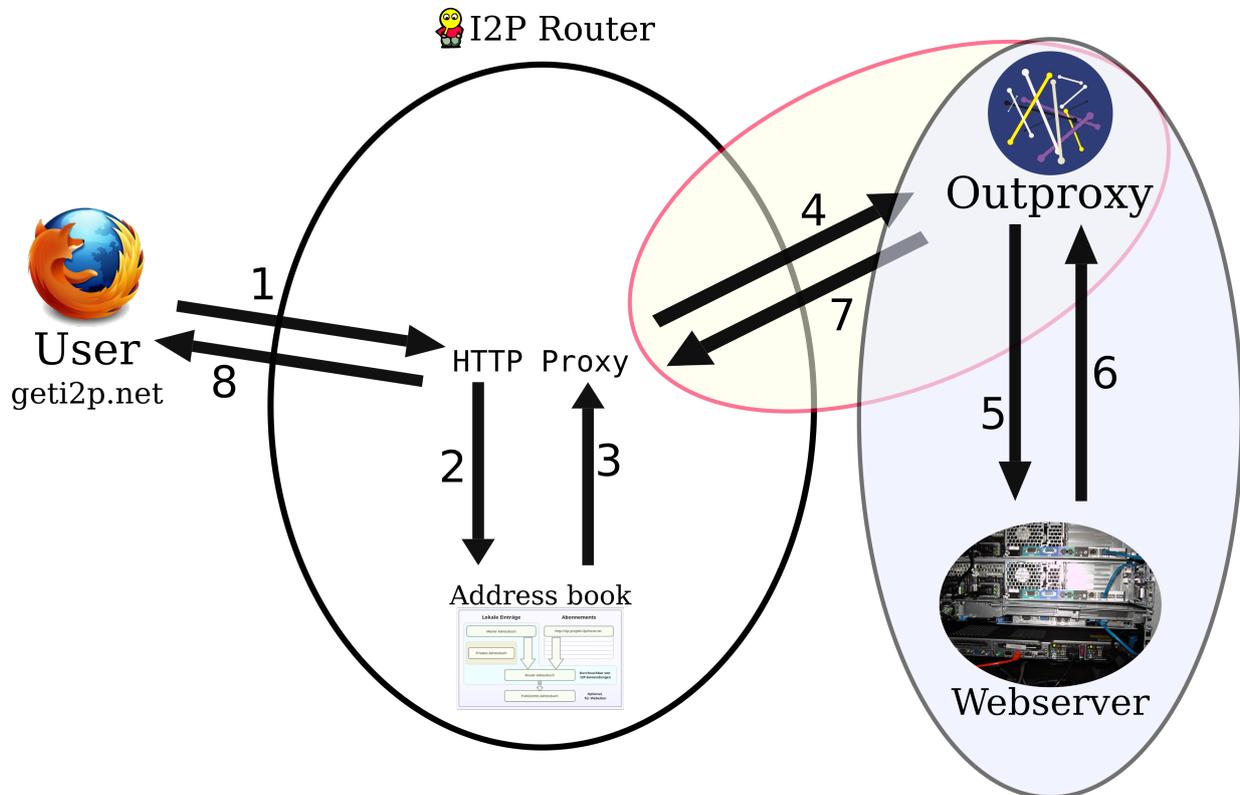
I2P itself is an internal network. This means that it cannot connect to other networks without help. So you can only access internal pages known as eepsites. So you cannot communicate and access the Internet or the Tor network without help. An outproxy therefore acts as an aid so that I2P can communicate with other networks.

How does an outproxy work?

If you try to access an eepsite, I2P looks in the address book for the corresponding address. The telephone book is analogous to this. You know the name (eepsite) and you try to find the phone number (destination). [see also DNS on the WWW] Next, I2P tries to contact the eepsite and you can surf. This does not work with Clearnet sites.

So that you can still surf the Clearnet, there are outproxies:

If you try to access a Clearnet page, I2P recognizes this by the extension and checks whether one or more outproxies have been set up. If not, I2P issues an error message. If so, I2P looks in the address book for the address of the outproxy and contacts them. Next, the request (e.g. to Twitter or DuckDuckGo) is sent to the Outproxy. The latter then contacts the website instead of the user and receives a response. It forwards this to the user. The outproxy operator can also cut, censor or manipulate the user's traffic.



1. The browser sends the request to the HTTP proxy of the I2P router.
2. The I2P router looks for the destination for the outproxy in the address book
3. The address book returns the destination
4. The request is sent to the outproxy
5. The Outproxy transmits the request to the web server
6. The web server answers the outproxy
7. The outproxy routes the request back to the HTTP proxy
8. The HTTP proxy transfers the request to the browser and thus to the user

Repetition:

The user wants to access the `geti2p.net` site via the I2P network with the help of an outproxy. He enters the address into a configured browser and the browser creates a request. It sends this to the HTTP proxy of the I2P router (point 1). The I2P router now checks whether an outproxy is set. Next, the router gets the destination (comparable to an IP address in Clearnet) from the address book. At point 2 he sends the request to the address book and at point 3 he gets the answer. The router can then contact the outproxy. After the connection has been successfully established, he sends the request to the outproxy (point 4). The outproxy in turn forwards the request to the corresponding web server (point 5). The web server answers the outproxy (point 6) and thinks that it was not the actual user but the outproxy who wanted the request. After the outproxy has received the answer, it forwards it to the I2P router (point 7). The I2P router in turn forwards the request back to the browser (point 8). The user has now received the page.

How do I set up an outproxy?

First you need the address of the outproxy. Unfortunately there are very few outproxies at the moment. These include: `outproxy.bandura.i2p`, `false.i2p`, `outproxy-tor.meeh.i2p`

All three route requests through the Tor network. This means that the requests at points 5 and 6 are routed through the Tor network. One of the reasons why outproxy operators do this is because it gives them legal certainty.

First go to the tunnel list in the I2P interface. This can usually be found at `http://127.0.0.1:7657/i2ptunnelmgr`. There you select the tunnel for which you want to configure the outproxy. There you choose the `zahrat`  to work on the tunnel.

Next you will find a text box under "Outproxies" or "SSL Outproxies". *Outproxies* are the outproxies that I2P uses for HTTP connections; *SSL Outproxies* are the outproxies that are used for HTTPS connections. There you enter the corresponding outproxies.

It is also possible to enter several outproxies. You separate them with a comma. When requesting an outproxy, the router randomly selects an outproxy.

Then save the tunnel settings and you're done!

Make sure that the outproxy is entered in the address book. The best way to check it is to go to the address of the outproxy. If the message appears that

the address was not found in the address book, a jumper can be used. Otherwise you can use the outproxy immediately.

What is the danger when using outproxies?

There is a risk that the outproxy operator is malicious and records the requests or answers, i.e. logs them, or manipulates the answers. He can also censor pages, which is not that bad.

There is roughly the same risk as when using the Tor network. The only difference is that the Tor network has more exit nodes than I2P outproxies. It is therefore recommended that you use Tor to surf the Clearnet.

Glossary

Eepsite - An I2P internal site. These domains always have the extension .i2p

Destination - Comparable to the IP address in Clearnet. The outproxy is identified here with the aim

Request - This is an HTTP request. This contains e.g. the page, the desired language and the time

Response - This is the response to the HTTP request. This contains the code for the page later displayed in the browser

Web server - This is the name of the computer on which one or more websites are located.

Clearnet - This term denotes that "normal" internet; by also having Twitter or DuckDuckGo at home.