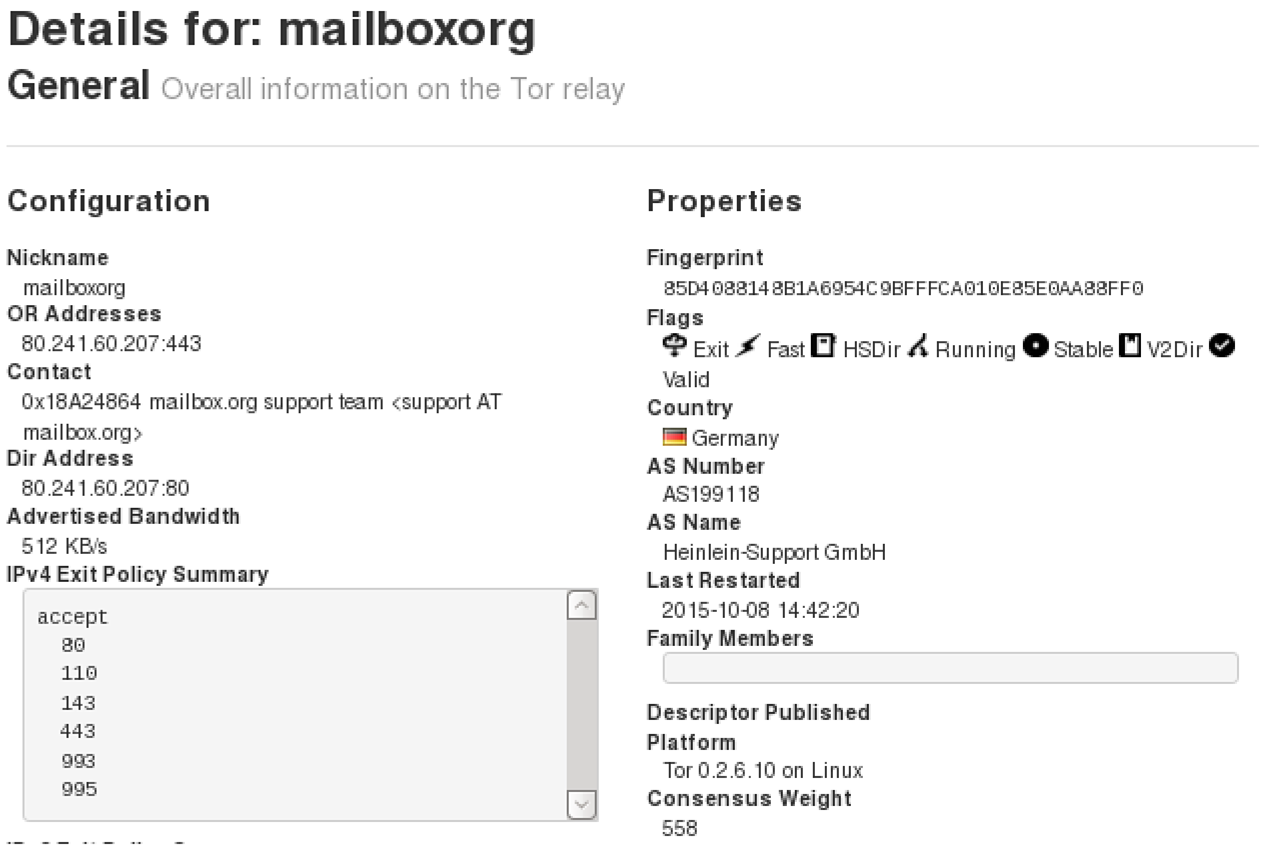
The Tor exit node of mailbox.org

In order to promote anonymity on the internet and to protect our customers against unwarranted surveillance, we decided to operate a dedicated Tor exit node in our data center. This Tor node will provide added security for our customers who are also users of the anonymisation service Tor Onion Router at the same time.



Details for: mailboxorg

General Overall information on the Tor relay

Configuration

Nickname
mailboxorg

OR Addresses
80.241.60.207:443

Contact
0x18A24864 mailbox.org support team <support AT mailbox.org>

Dir Address
80.241.60.207:80

Advertised Bandwidth
512 KB/s

IPv4 Exit Policy Summary

```
accept
  80
  110
  143
  443
  993
  995
```

Properties

Fingerprint
85D4088148B1A6954C9BFFFCA010E85E0AA88FF0

Flags
Exit Fast HSDir Running Stable V2Dir ✓ Valid

Country
Germany

AS Number
AS199118

AS Name
Heinlein-Support GmbH

Last Restarted
2015-10-08 14:42:20

Family Members

Descriptor Published

Platform
Tor 0.2.6.10 on Linux

Consensus Weight
558

In the last few years, there have been repeated reports about malicious Tor exit nodes, some of which apparently used false SSL certificates to attempt man-in-the-middle attacks on encrypted HTTPS connections (For instance, in 2013: Connections to Wikipedia or IMAPS connections).

In order to make sure such attacks won't be possible on mailbox.org services, we offer

1. a dedicated node within our data centre that all Tor users should configure as the exit server for accessing mailbox.org addresses.
2. Alternatively, you can also use the Tor Hidden Service ***kqiafglit242fygz.onion*** (v2) and **xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion** (v3) for accessing our SMTP, POP3, IMAP, or XMPP servers.

1. Add MapAddress configuration settings for the Tor daemon

Users can configure their Tor daemon to use a specific exit node for accessing particular servers in a domain. This is the way to go if you are a Tor user and also a customer of mailbox.org, because we have an exit node set up that is located within our own data centre and can therefore facilitate a secure connection to your mailbox.org services. This solution allows using mailbox.org without having to specify an Onion host name, avoids any SSL certificate validation problems, and best of all, you can use your mailbox.org Office suite in the Web browser as usual.

To start, use a text editor to open the file in path **Browser/TorBrowser/data/Tor/torrc** (see also the Tor FAQ). If you have just installed the Tor Browser Bundle, then you need to start the Tor browser at least once and then close it again to see that file. With the configuration file open, add the following lines:

```
MapAddress mailbox.org mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit MapAddress *.mailbox.org *.
mailbox.org.85D4088148B1A6954C9BFFFCA010E85E0AA88FF0.exit
```

The settings above make sure that any data traffic to the mailbox.org servers will be channelled through the Tor network to eventually exit through the node that sits in our data centre. This scenario resembles something like an anonymous VPN connection, one might say.

Note: If you use the Tor Messenger, then you need to edit the file in ***Messenger/TorMessenger/data/Tor/torrc*** to include the relevant MapAddress statements.

2. Use the Tor Hidden Service instead

As an alternative, we also offer the Tor Hidden Service ***kqiafglit242fygz.onion*** (v2) and ***xy5d2mmnh6zjnroce4yk7njlkyafi7tkrameybxu43rgsg5ywhnelmad.onion*** (v3) for our e-mail and Jabber/XMPP servers.

However, note that it is **not** possible to access the web interface of mailbox.org this way.

In Mozilla Thunderbird, you can use the Tor Hidden Service directly as an SMTP, IMAP, or POP3 server entry – here, there is no need to adjust the configuration of your Tor daemon.
In a Jabber/XMPP client, the Tor Hidden Service can be set as connect server (this setting can usually be found in the advanced options).

A distinct **disadvantage** of the Tor Hidden Service is that upon connecting, users will experience SSL errors, because the certificate used for transport security is issued for the domain mailbox.org and not the domain of the hidden service. Consequently, users need to verify the SSL certificate manually.

Related Articles

- How to use Thunderbird with Tor Onion Router
- How to configure Tor Messenger
- How to configure the Tor Browser
- The Tor exit node of mailbox.org
- How do I terminate my mailbox.org account