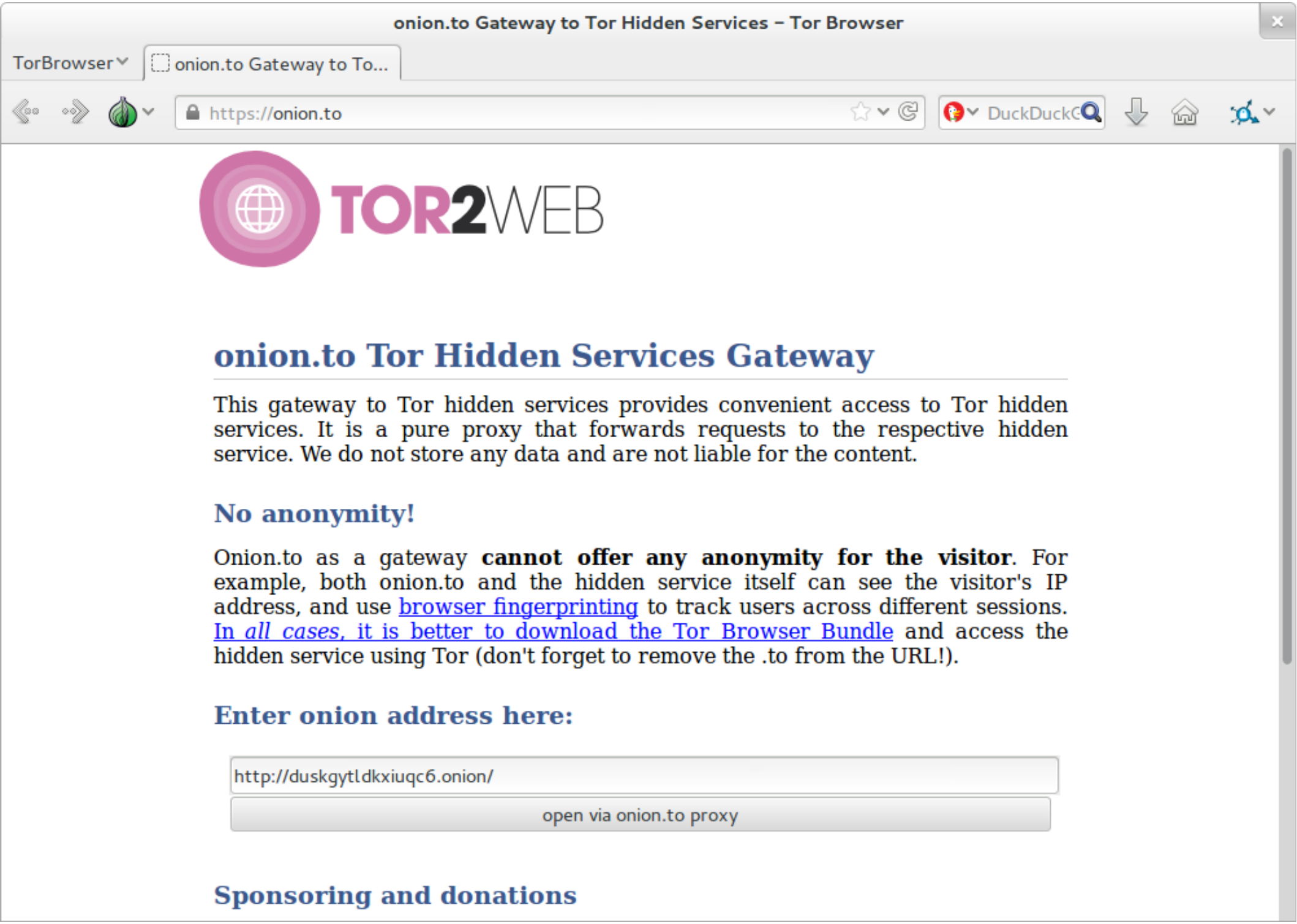
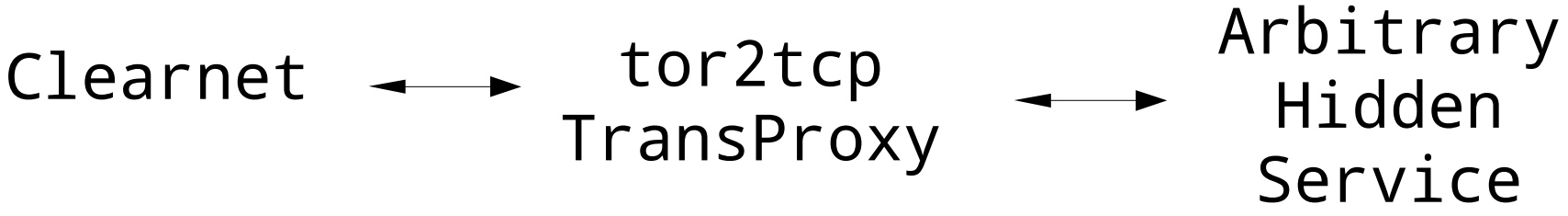

<erno> hm. I've lost a machine.. literally _lost_. It responds to ping, it works completely, I just can't figure out where in my apartment it is.

m@niij.org
0AA7 9AE2 D160 71DF 98AD  3B07 6CAC 7102 0AF5 D60D


onion.to Gateway to Tor Hidden Services – Tor Browser
TorBrowser
onion.to Gateway to To...
https://onion.to
DuckDuckG
TOR2WEB
onion.to Tor Hidden Services Gateway
This gateway to Tor hidden services provides convenient access to Tor hidden services. It is a pure proxy that forwards requests to the respective hidden service. We do not store any data and are not liable for the content.
No anonymity!
Onion.to as a gateway cannot offer any anonymity for the visitor. For example, both onion.to and the hidden service itself can see the visitor's IP address, and use browser fingerprinting to track users across different sessions. In all cases, it is better to download the Tor Browser Bundle and access the hidden service using Tor (don't forget to remove the .to from the URL!).
Enter onion address here:
http://duskgytldkxiuqc6.onion/
open via onion.to proxy
Sponsoring and donations

# tor2tcp Goals




- Have a public facing service that actually connects you to a hidden service
- Do TLS handshakes with a .onion from the clearnet, enabling safe transport and storage
- Proxy machine a tiny VPS with no information at all, except for configuration files and public ssh keys

# Proof of Concept!

- … HTTPS servers are so easy to configure it's too boring …
- Hmm, actually, I'd like my email to be stored in a safe-ish trusted environment (not on a machine that has a public facing IP)

# Proof of Concept!

- … HTTPS servers are so easy to configure it's too boring …
- Hmm, actually, I'd like my email to be stored in a safe-ish trusted environment (not on a machine that has a public facing IP)

Throw your hands in the air for SMTP!

# Incoming connections

- So simple it's awkward:

**torrc:**

```
TransPort 1.2.3.4:25
MapAddress 1.2.3.4 doge5sovanitywow.onion
Tor2webMode 1 # when ./configure --enable-tor2web-mode
```

**For multiple ports via iptables:**

```
$ iptables -t nat -A PREROUTING -p tcp -d 1.2.3.4
--dport 587 -j REDIRECT --to-ports 25
```

```
Return-Path: <mzeltner@niij.org>
X-Original-To: mzeltner@poum.niij.org
Delivered-To: mzeltner@poum.niij.org
Received: from toam.niij.org (localhost [127.0.0.1])
     (using TLSv1 with cipher ECDHE-RSA-AES256-SHA (256/256 bits))
     (No client certificate requested)
     by poam.niij.org (Postfix) with ESMTPS id 4FD8E1DFC83
     for <mzeltner@poum.niij.org>; Sat,  9 Nov 2013 18:57:49 -0500 (EST)
Received: by toam.niij.org (Postfix, from userid 1000)
     id 181F19CC06D3; Sun, 10 Nov 2013 00:50:33 +0100 (CET)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=niij.org; s=tuom;
     t=1384041033; bh=xgWZ+d5zeRJx40Sj/i20aaNAbBZa5g8CkjpJhRHqB88=;
     h=Date:From:To:Subject:From;
     b=ohAeHoaOPEkIxmeMqstBQamww8t6QBaBDWw3dUFC8DnVpmylRaOm9/aEczDDdt1qL
      K6C6JSiw1zaEwJnNCwwId+Rf9LhPjfkSumXp9yOOIIHrb72CrdOM9aNa2xvEOclVNU
      lq6+hDxsu9vLiBBvmU8poMwnDY2izqo/fmby5JhY=
Date: Sat, 9 Nov 2013 18:50:27 -0500
From: Michael Zeltner <m@niij.org>
To: mzeltner@poum.niij.org
Subject: Hello World
Message-ID: <20131109235027.GA32328@eaon.acumenwifi.com>
MIME-Version: 1.0
Content-Type: multipart/signed; micalg=pgp-sha512;
     protocol="application/pgp-signature"; boundary="h31gzZEtNLTqOjlF"
Content-Disposition: inline
User-Agent: mutt --with-notmuch (1.5.21)


--h31gzZEtNLTqOjlF
Content-Type: text/plain; charset=utf-8
Content-Disposition: inline
Content-Transfer-Encoding: quoted-printable

such dark.
very hackathon.
much hide.
wow.
--=20
https://niij.org/
```

```
--h31gzZEtNLTqOjlF
Content-Type: application/pgp-signature

-----BEGIN PGP SIGNATURE-----

iQIcBAEBCgAGBQJSfso7AAoJEE419lhGyPfaSKsP/2KjQekXPleMHJiYTBmbFpgK
DBtB8uw6HY67qrmbTdIgAw7ns/nqOOaEtF0lEK1j6cePBL1u5y+Km2KFD0I9jJCm
LcBJrTIkof7OG4rMVNh2pbXWQ5bsGmg4w8cWQCJWVBxtN/c+wBJglvon6t10T8mb
Y8nJvAlRlXIJgHQrefI0omSnJS8y8dc95EKHF05QWQJUYUY46+W6/ZQwXC0sbdPM
fGKw4OgoXLOK/bAegfi6kBpr3atlKrLwUOIVCyBAAaZplrPVTiOM75sRCetTiEWd
7EAm6CE1Al/SsfUfhJFOdO3oelhsmdnio1jOn4BfXd+LxOeL78JoJohR3MWaVJv8
i1+4a0fN+FguN9JLuQcq4HOS4SE08wqbJkZO9bm+qJSuRjL0XLKMxO5jYAdWPgFf
pzNzvLTDucN/jGUu2FoFiHgjx3rOLobvUwJCKPglqwNNOA5sVkq/wUUybc3TJ/OQ
NMb+s6eJ6s7aqjNwiOh6osZgSyLTpHVpChgHf99CTSshK12ZxAAjdMDmd4a1DzF8
O6W4I4Yf9I5UemMzt4j+KhEEys6MUPszHAY1EmWyTmEXZFjrHP51VDtTNGPNac5v
7laX7A6GMIzlYgKPQklBC0KLMwQmEoNS1eWDvTTJaOj2x8Wzwy8NY2dqU2Zzubc/
V0W212J21t+JpWdW+5O7
=d0OC
-----END PGP SIGNATURE-----

--h31gzZEtNLTqOjlF--
```

# Outgoing connections

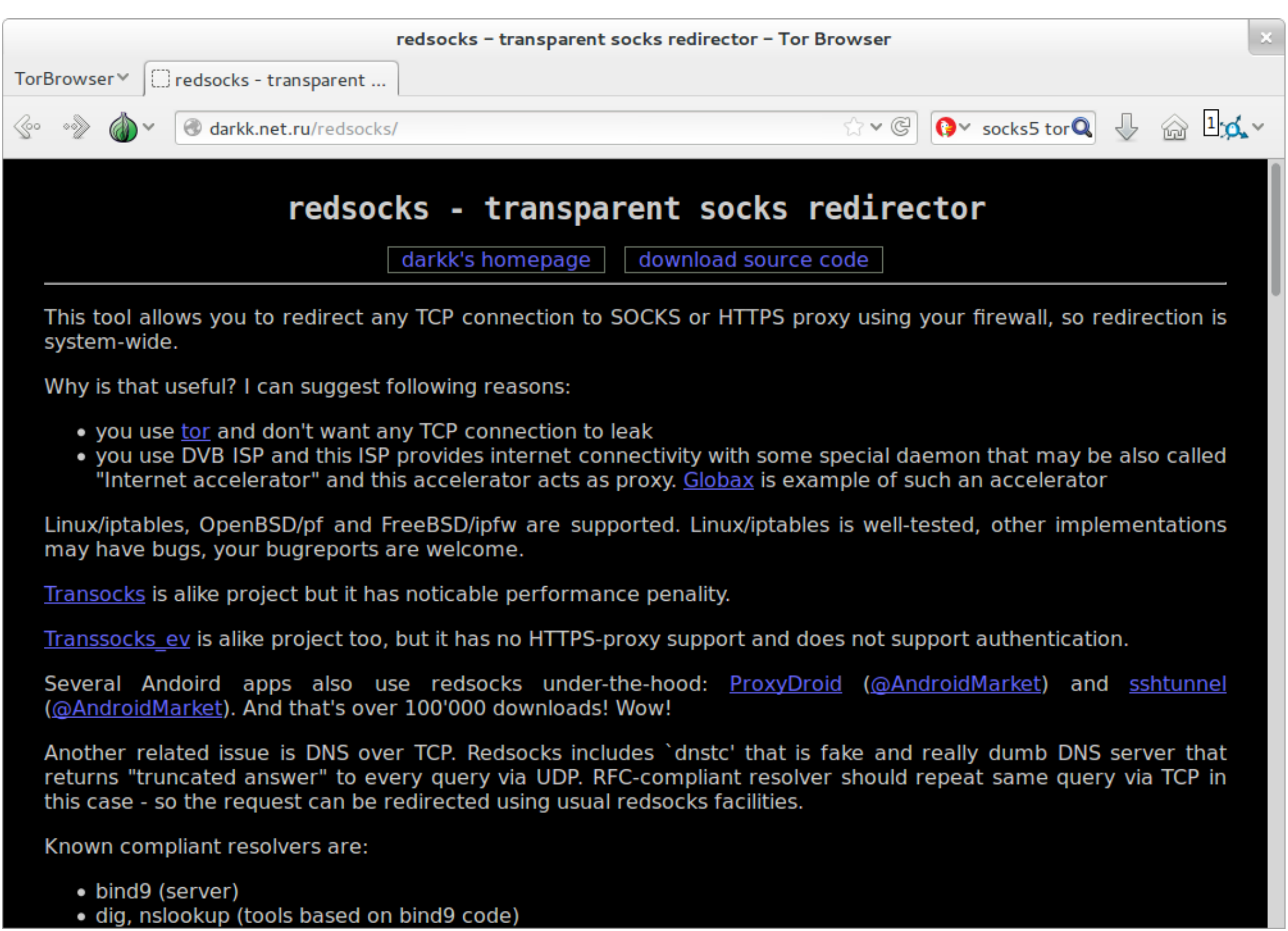
- We don't want to be **** SPAM **** by sending emails via Tor exit nodes
- Hence 1.2.3.4 should also be the origin of the emails we want to send

# Outgoing connections

- We don't want to be **** SPAM **** by sending emails via Tor exit nodes
- Hence 1.2.3.4 should also be the origin of the emails we want to send

**So we tunnel from our hidden service to our VPS via Tor:**

```
$ tmux new-session -d 'torsocks autossh
-D 1080 doge@1.2.3.4'
```




# redsocks - transparent socks redirector

darkk's homepage | download source code

---

This tool allows you to redirect any TCP connection to SOCKS or HTTPS proxy using your firewall, so redirection is system-wide.

Why is that useful? I can suggest following reasons:

- you use tor and don't want any TCP connection to leak
- you use DVB ISP and this ISP provides internet connectivity with some special daemon that may be also called "Internet accelerator" and this accelerator acts as proxy. Globax is example of such an accelerator

Linux/iptables, OpenBSD/pf and FreeBSD/ipfw are supported. Linux/iptables is well-tested, other implementations may have bugs, your bugreports are welcome.

Transocks is alike project but it has noticable performance penality.

Transsocks_ev is alike project too, but it has no HTTPS-proxy support and does not support authentication.

Several Andoird apps also use redsocks under-the-hood: ProxyDroid (@AndroidMarket) and sshtunnel (@AndroidMarket). And that's over 100'000 downloads! Wow!

Another related issue is DNS over TCP. Redsocks includes `dnstc' that is fake and really dumb DNS server that returns "truncated answer" to every query via UDP. RFC-compliant resolver should repeat same query via TCP in this case - so the request can be redirected using usual redsocks facilities.

Known compliant resolvers are:

- bind9 (server)
- dig, nslookup (tools based on bind9 code)

# Outgoing connections

- Wait… Shit: Tor does not support DNS requests for MX records
- … and Postfix seems to fuck up without UDP based DNS?
- … also, we don't want to leak DNS requests from our trusted machine

# DNS SOCKS Proxy

A simple dns proxy to tunnel DNS requests over a socks proxy (for example, over ssh or Tor). This can come in handy when setting up transparent proxies.

It chooses a random DNS server for each request from the file "resolv.conf" which is a newline delimited list of DNS servers.

The daemon must be run as root in order for it to bind to port 53.

## Usage

Usage: ./dns-proxy [options]

With no parameters, the configuration file is read from 'dns_proxy.conf'.

- -n -- No configuration file (socks: 127.0.0.1:9050, listener: 0.0.0.0:53).
- -h -- Print this message and exit.
- config_file -- Read from specified configuration file.

## Configuration

# Outgoing connections

## More iptables!

```
$ iptables -t nat -A OUTPUT ! -o lo -p tcp -m owner
--uid-owner postfix -m tcp -j REDIRECT --to-ports 12345
$ iptables -t nat -A OUTPUT ! -o lo -p udp -m owner
--uid-owner postfix -m udp --dport 53 -j REDIRECT
--to-ports 53
$ iptables -t filter -A OUTPUT -p tcp -m owner
--uid-owner postfix -m tcp --dport 12345 -j ACCEPT
$ iptables -t filter -A OUTPUT -p udp -m owner
--uid-owner postfix -m udp --dport 53 -j ACCEPT
$ iptables -t filter -A OUTPUT ! -o lo -m owner
--uid-owner postfix -j DROP
```


#thereifixedit

```
Return-Path: <mzeltner@poum.niij.org>
X-Original-To: m@niij.org
Delivered-To: m@niij.org
Received: from localhost (localhost [127.0.0.1])
        by toam.niij.org (Postfix) with ESMTP id 096319CC028E
        for <m@niij.org>; Wed, 13 Nov 2013 17:01:49 +0100 (CET)
Received: from toam.niij.org ([127.0.0.1])
        by localhost (niij.org [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id DqzdV0CjkHDI for <m@niij.org>;
        Wed, 13 Nov 2013 17:01:47 +0100 (CET)
X-Greylist: delayed 349 seconds by postgrey-1.34 at niij; Wed, 13 Nov 2013
17:01:45 CET
Received: from poam.niij.org (unknown [46.246.28.219])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by toam.niij.org (Postfix) with ESMTPS id 02A3C9CC025E
        for <m@niij.org>; Wed, 13 Nov 2013 17:01:45 +0100 (CET)
Received: by poam.niij.org (Postfix, from userid 1000)
        id 54BD41DFD6B; Wed, 13 Nov 2013 10:54:47 -0500 (EST)
Subject: Testmail
From: mzeltner@poum.niij.org
Message-Id: <20131113155447.54BD41DFD6B@poam.niij.org>
Date: Wed, 13 Nov 2013 10:54:47 -0500 (EST)

Hello there, from the darknet! Take two...
```

```
Return-Path: <mzeltner@poum.niij.org>
X-Original-To: m@niij.org
Delivered-To: m@niij.org
Received: from localhost (localhost [127.0.0.1])
        by toam.niij.org (Postfix) with ESMTP id 096319CC028E
        for <m@niij.org>; Wed, 13 Nov 2013 17:01:49 +0100 (CET)
Received: from toam.niij.org ([127.0.0.1])
        by localhost (niij.org [127.0.0.1]) (amavisd-new, port 10024)
        with ESMTP id DqzdV0CjkHDI for <m@niij.org>;
        Wed, 13 Nov 2013 17:01:47 +0100 (CET)
X-Greylist: delayed 349 seconds by postgrey-1.34 at niij; Wed, 13 Nov 2013
17:01:45 CET
Received: from poam.niij.org (unknown [46.246.28.219])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by toam.niij.org (Postfix) with ESMTPS id 02A3C9CC025E
        for <m@niij.org>; Wed, 13 Nov 2013 17:01:45 +0100 (CET)
Received: by poam.niij.org (Postfix, from userid 1000)
        id 54BD41DFD6B; Wed, 13 Nov 2013 10:54:47 -0500 (EST)
Subject: Testmail
From: mzeltner@poum.niij.org
Message-Id: <20131113155447.54BD41DFD6B@poam.niij.org>
Date: Wed, 13 Nov 2013 10:54:47 -0500 (EST)

Hello there, from the darknet! Take two...
```

many location anonymous.

such secure store.

very spam workaround.

wow.

# Issues

- SPAM protection: IP filtering not possible, all connections come from 127.0.0.1
- Leaks? Did not audit
- Not sure how much to trust redsocks
- Even more unsure about the DNS TCP SOCKS Proxy

# Future

- Enabling .onion to .onion communication within the same setup
  - Authentication of .onion origins with DKIM (using the .onions RSA key)
  - .onion only mailinglists
- Test with XMPP

# That's it!

- Documentation + Slides:
  https://poum.niij.org/

m@niij.org
0AA7 9AE2 D160 71DF 98AD  3B07 6CAC 7102 0AF5 D60D

Thanks to: Abel Luck, ra_, @MacLemon, Aaron Swartz Hackathon NYC, FUBAR Labs, Metalab, naif, Moritz Bartl