Tor Solutions
CORPORATION

August 2012 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

1 C.2.1, C.2.2, C.2.3, C.2.4

1.1 August 2012

1.1.1 Exit Relays

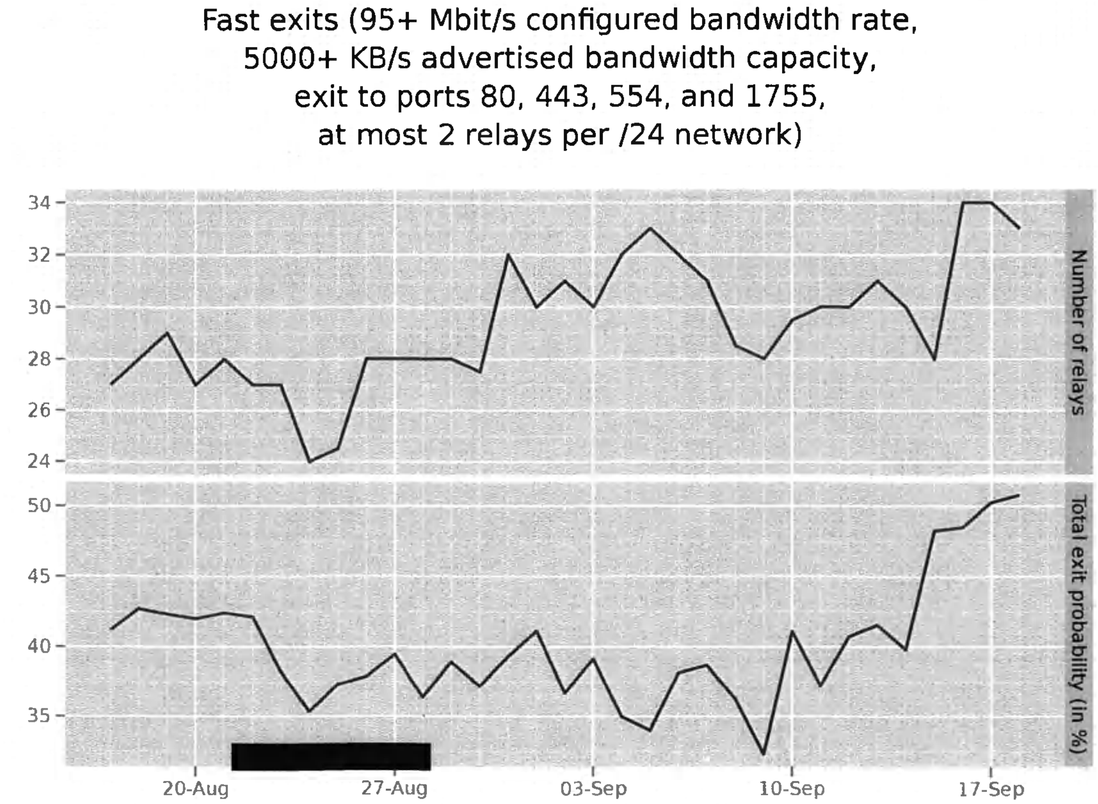
We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

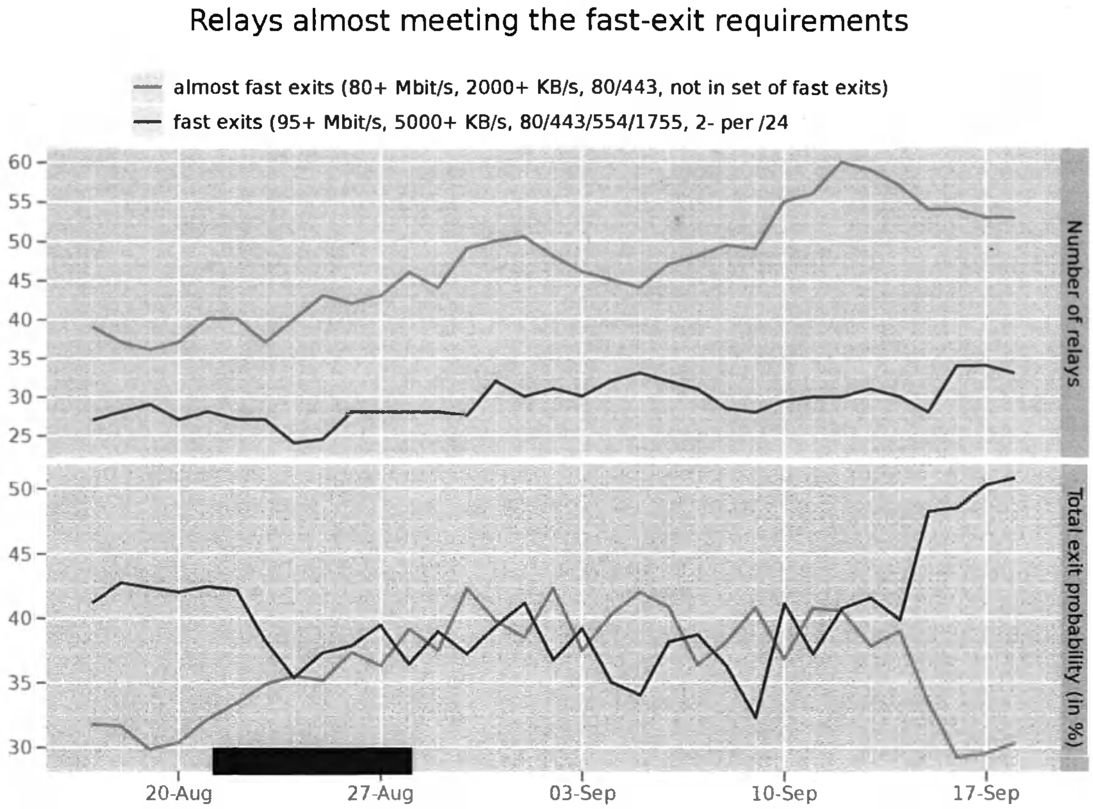
Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.



[redacted]



Karsten added `https://metrics.torproject.org/network.html#bandwidth-flags` for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: `https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags`.

1.1.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

We've set up our new "bridgeguard" tool on this bridge: `https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md`

Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL

client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

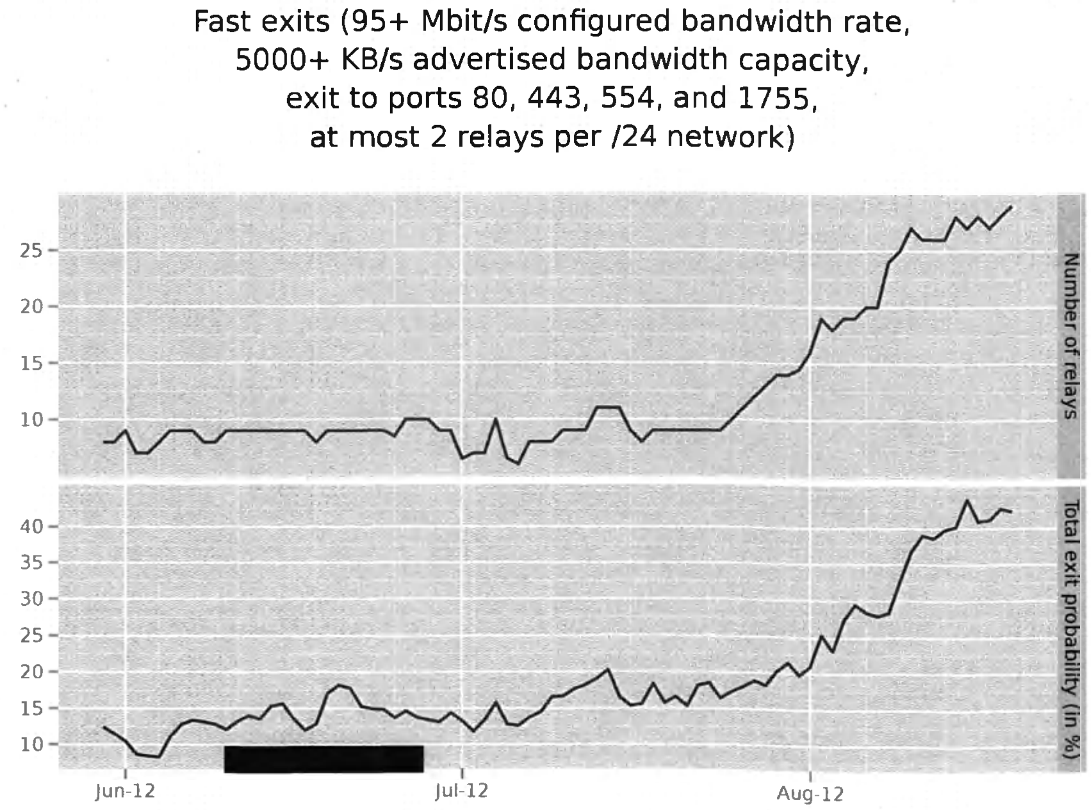
Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
`https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles` Lots of options as we go forward.

1.2 July 2012

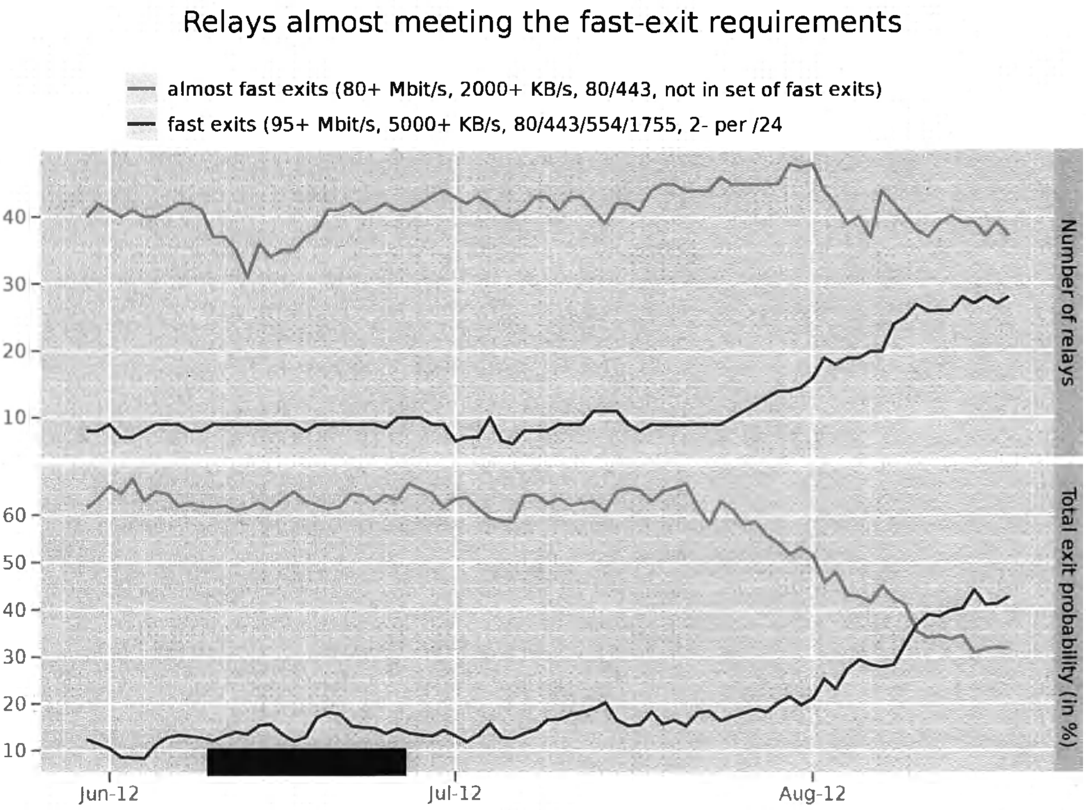
The 'fast exit count' graphs are now updated daily at `https://metrics.torproject.org/fast-exits.html` We're up to 28 or so.



[redacted]

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays

are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20% to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.3 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.2 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.3 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.2 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.3 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 August 2012

No new releases to report.

4.2 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.3 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 August 2012

No progress to report.

5.2 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.3 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 August 2012

See C.2.7 above.

6.2 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.3 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 August 2012

No progress to report.

7.2 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.3 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

Tor Solutions
CORPORATION

December 18 - January 17 2013 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

1 C.2.1, C.2.2, C.2.3, C.2.4

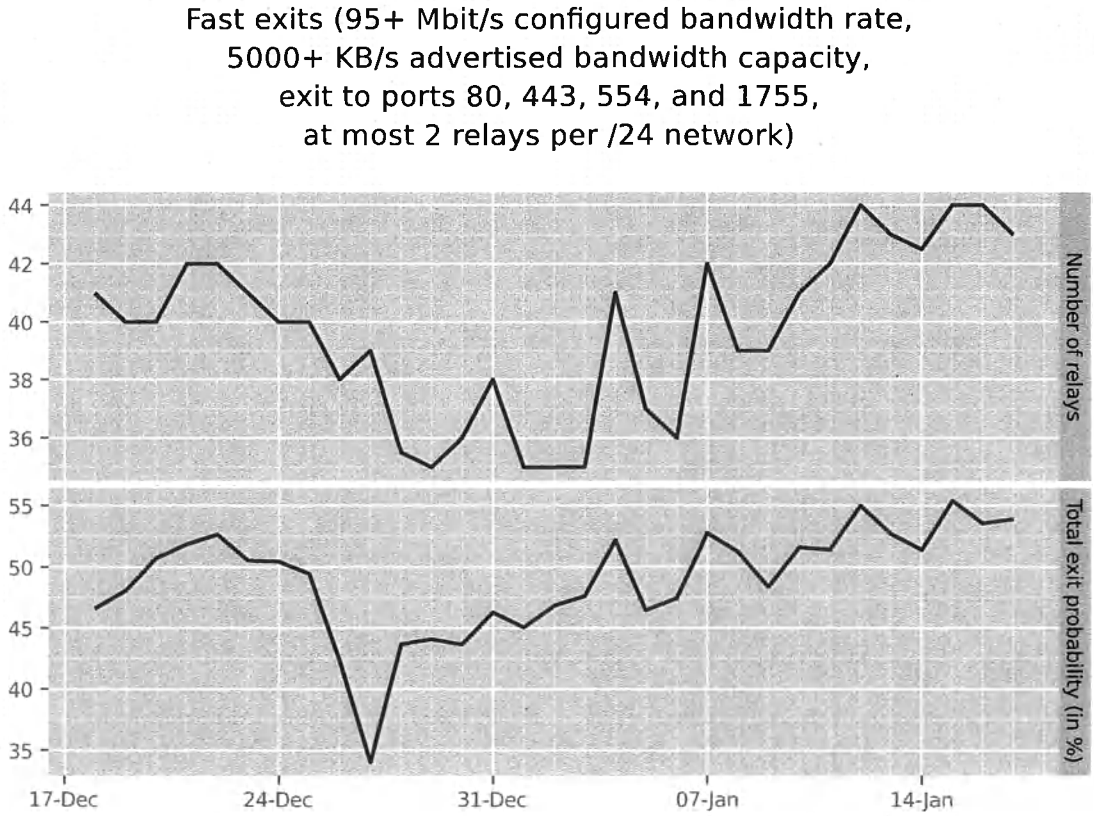
1.1 December 2012

We've hired a dedicated relay community manager. Moritz Bartl of Torservers.net is now responsible for maintaining relationships with relay operators, finding new ISPs for hosting exit relays, and growing the Tor network.

We're at 42 qualifying fast exists providing 34.88% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 54 qualifying fast exits providing 44.4391% of the bandwidth if we ignore the /24 diversity requirement.

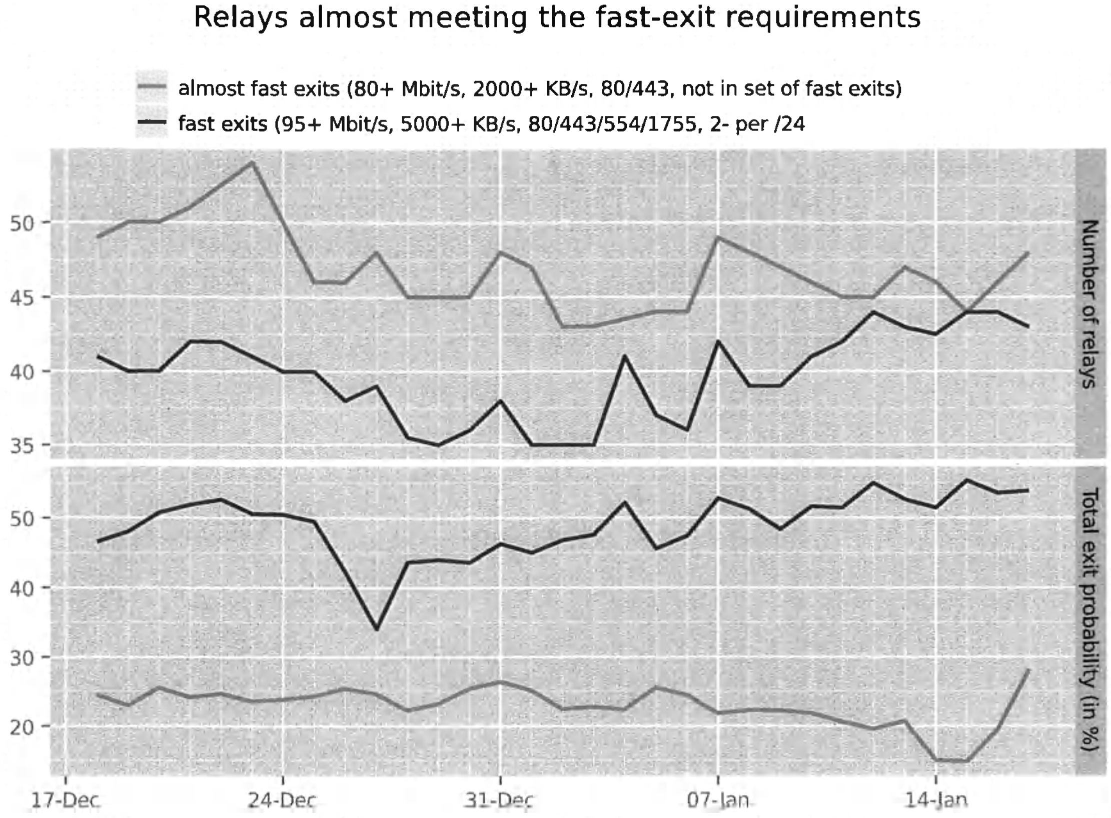
Figure 1: Relays meeting the fast-exit requirements



1.2 November 2012

We're at 38 qualifying fast exits providing 33.6749% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for

Figure 2: Relays almost meeting the fast-exit requirements



diversity.

We're at 51 qualifying fast exits providing 44.3442% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

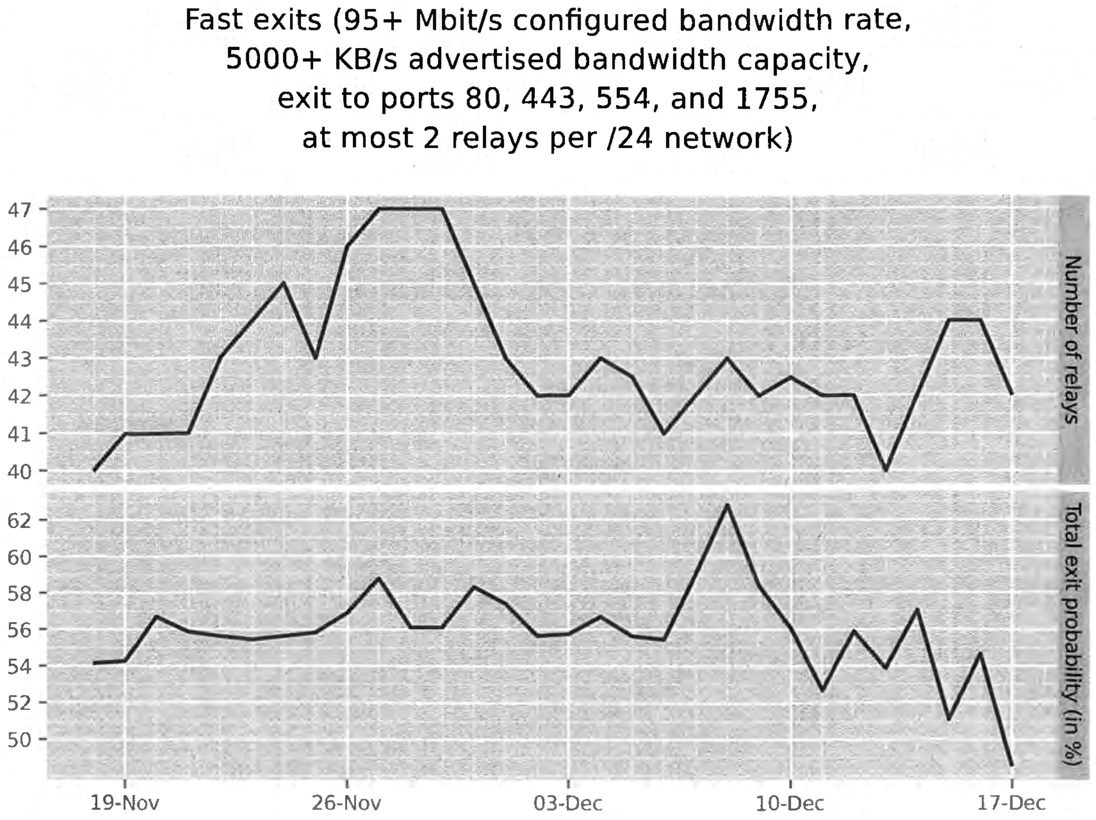
1.3 October 2012

We're up to 41 qualifying fast exits providing 22.9375% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 57 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

Discussions with lawyers continue. These discussions are blocking further progress on contracts and announcements of exit relay organizations.

Figure 3: Relays meeting the fast-exit requirements



1.4 September 2012

1.4.1 Exit Relays

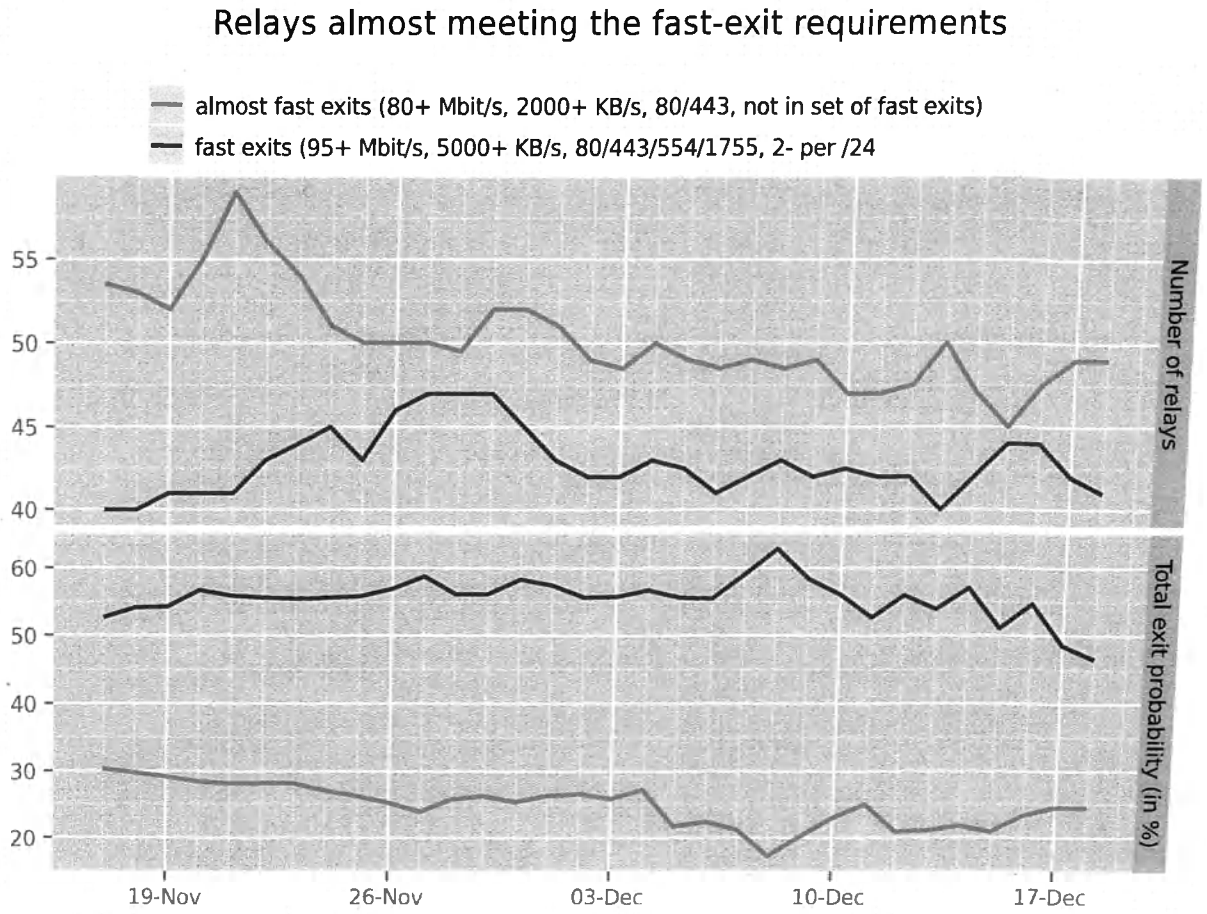
We're holding at 28 qualifying fast exits providing 16.667% of the bandwidth. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 37 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 57% of the exit probability.

We are in negotiations with three organizations running a majority of the exit relay capacity. These three orgs will be publicly announced when contracts are signed.

We are in final discussions about the Tor network and legal aspects of running a funded relay under US laws. The main concern here is not falling under the definition of Internet Service Provider or telecommunications carrier which would subject Tor to CALEA compliance regulations.

Figure 4: Relays almost meeting the fast-exit requirements



1.5 August 2012

1.5.1 Exit Relays

We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

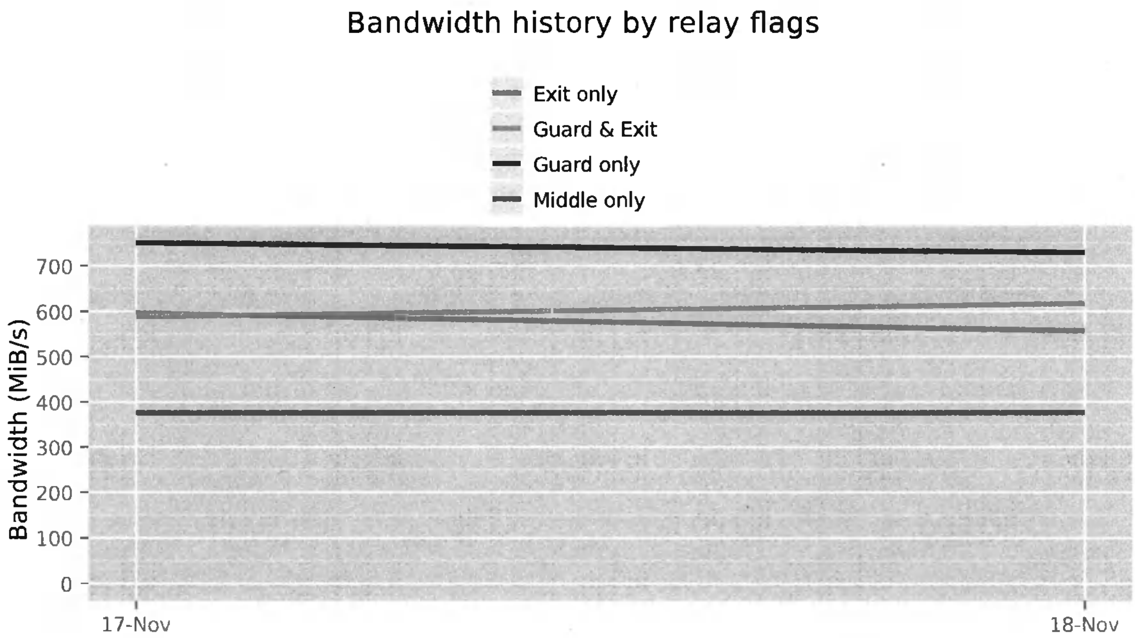
We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

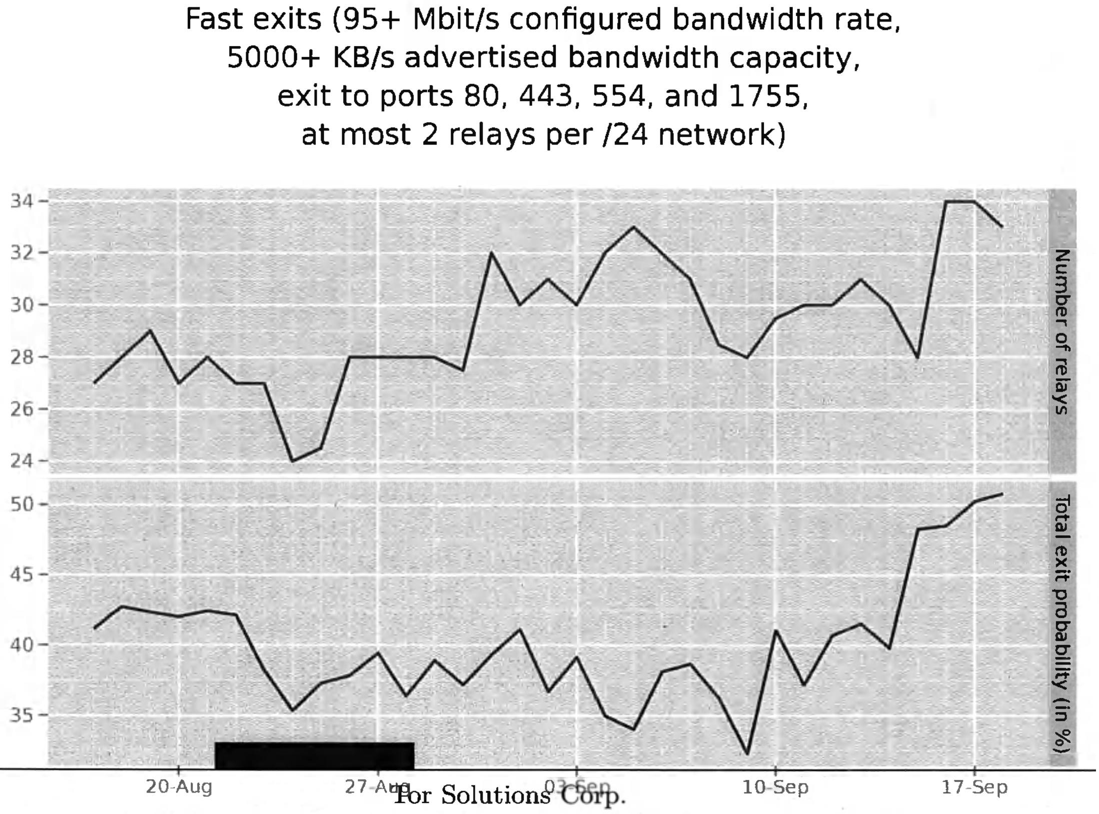
Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.

Figure 5: Relay bandwidth by Exit and/or Guard flags

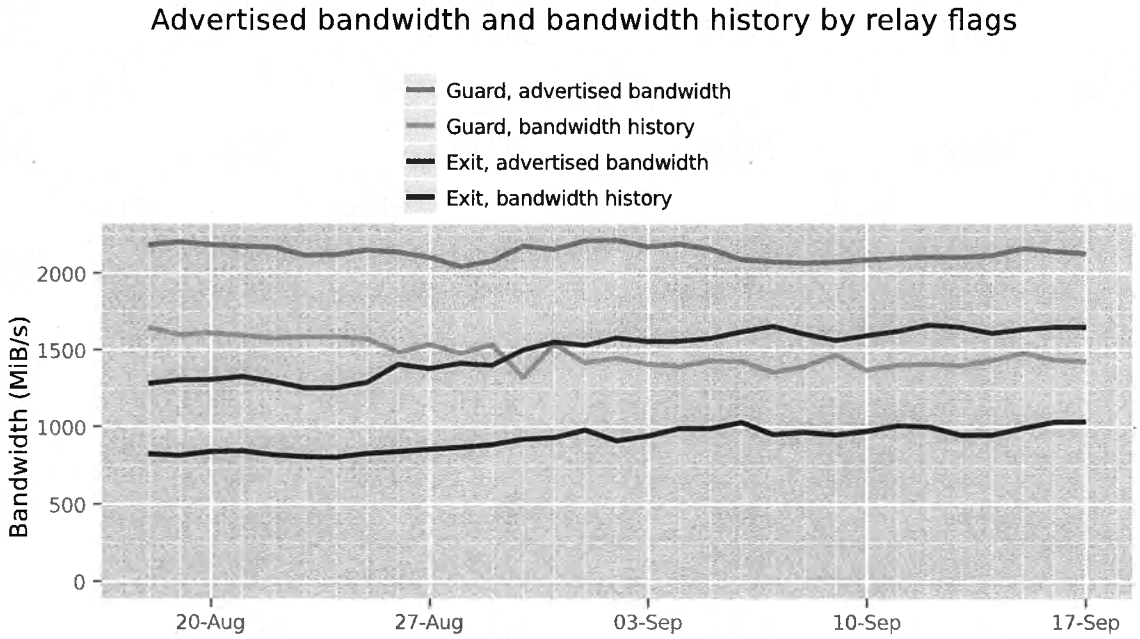


The Tor Project - https://metrics.torproject.org/

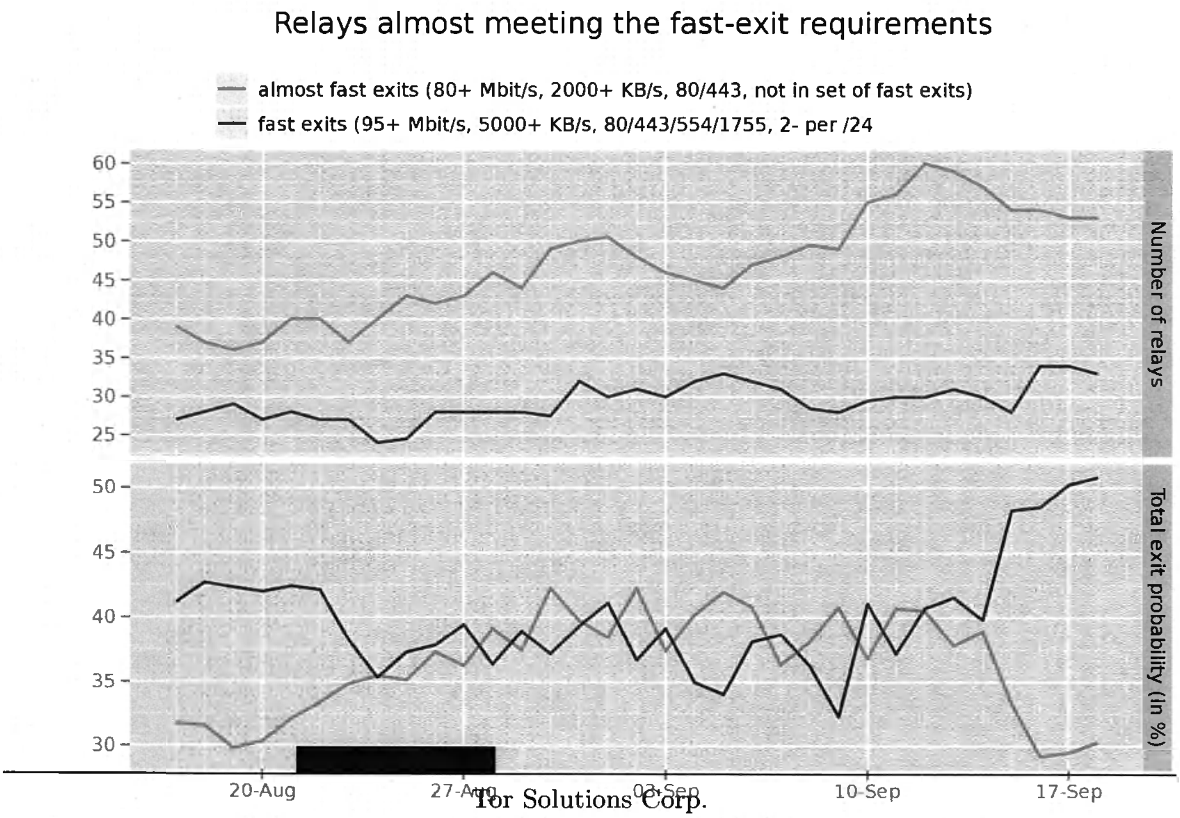


[redacted]

Figure 6: Relay bandwidth by Exit and/or Guard flags


Advertised bandwidth and bandwidth history by relay flags

The Tor Project - https://metrics.torproject.org/


Relays almost meeting the fast-exit requirements

[redacted]

Karsten added https://metrics.torproject.org/network.html#bandwidth-flags for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags.

1.5.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

We've set up our new "bridgeguard" tool on this bridge: https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md

Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

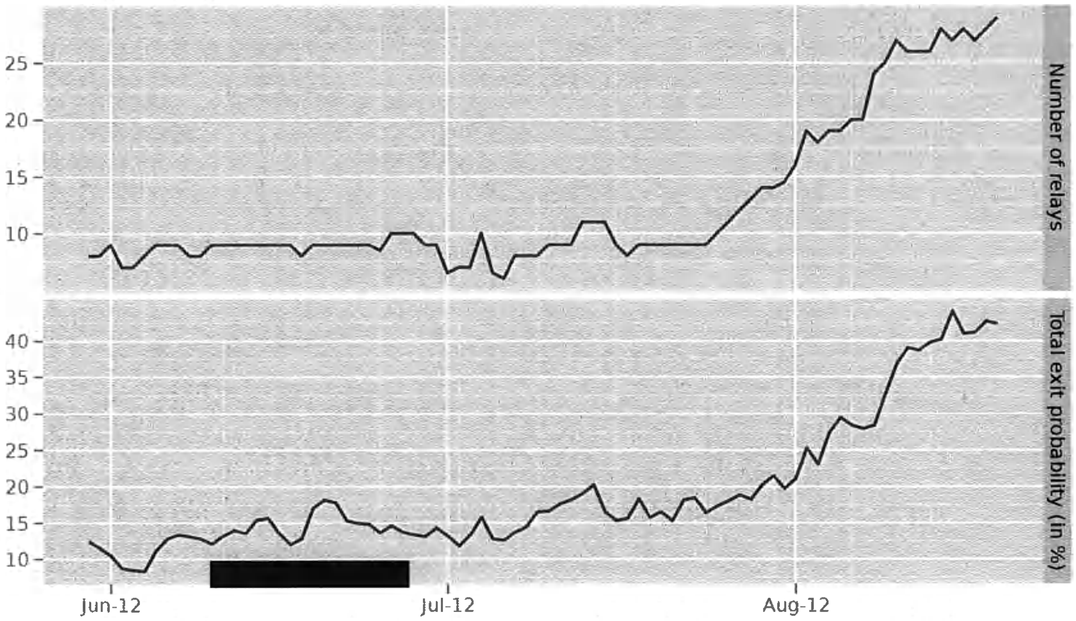
To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles Lots of options as we go forward.

1.6 July 2012

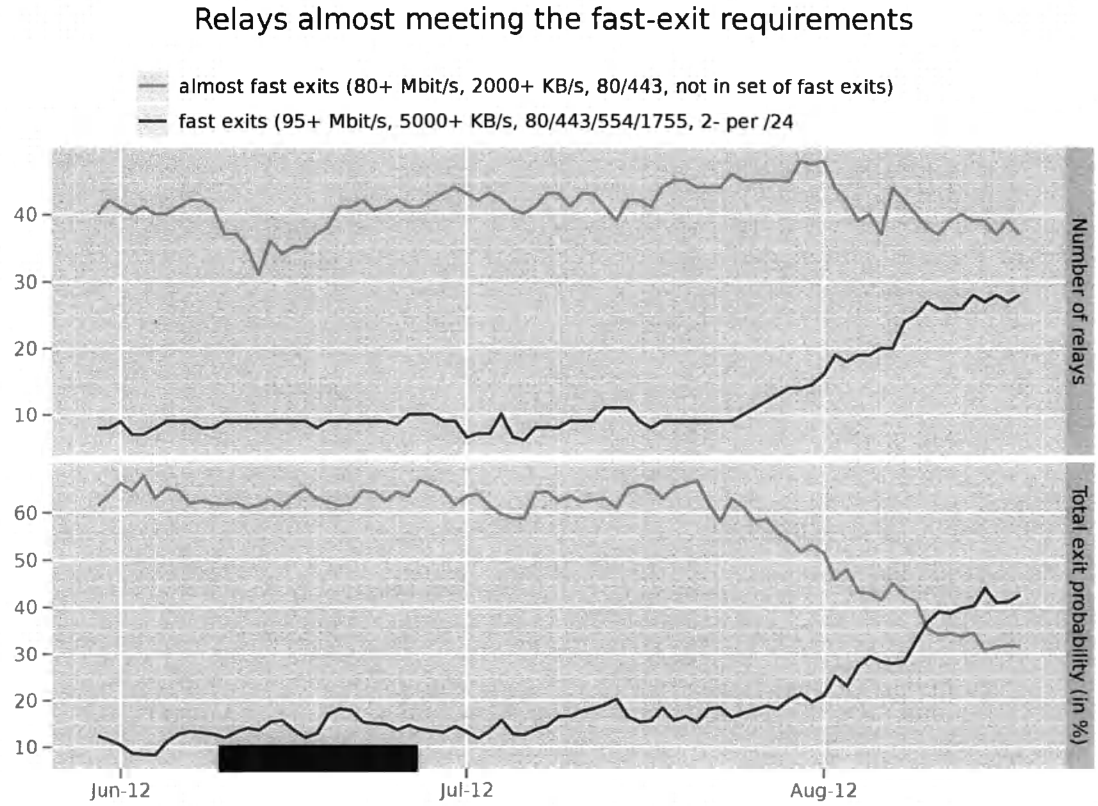
The 'fast exit count' graphs are now updated daily at https://metrics.torproject.org/fast-exits.html We're up to 28 or so.

Fast exits (95+ Mbit/s configured bandwidth rate,
5000+ KB/s advertised bandwidth capacity,
exit to ports 80, 443, 554, and 1755,
at most 2 relays per /24 network)



[redacted]

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20%

to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.7 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 December 2012

- We released updated Tor Browser Bundles to fix a certificate authority problem with Turk-Trust and to update the testing branch of Tor Browser with Tor 0.2.4.7-alpha.
- We've contracted two additional Firefox/TorBrowser developers to help address the backlog of bug fixes and enhancements. The current list of Tor Browser tickets is always available.

  We've recently closed the following tickets:

  - Ticket 6096 Perform TBB version check async on new tab
  - Ticket 6156 Rate limit of check.tpo
  - Ticket 6431 Torbutton should have a downward arrow menu
  - Ticket 6539 Image cache isolation causes assert crash
  - Ticket 7494 Create local homepage for TBB
  - Ticket 7495 Browser-based update notification mechanism (was 4238)
  - Ticket 4234 Firefox update process
  - Ticket 6564 Enable DOM Storage and isolate it to url bar domain
  - Re-base the following patches for compatibility with Firefox ESR 17:
    - Ticket 6786 0010-Limit-device-and-system-specific-CSS-Media-Queries.patch
    - Ticket 6253 0020-Add-mozIThirdPartyUtil.getFirstPartyURI-API.patch
    - Ticket 6253 0021-Add-canvas-image-extraction-prompt.patch
    - Ticket 5856 0022-Return-client-window-coordinates-for-mouse-event-scr.patch
    - Ticket 5856 0023-Do-not-expose-physical-screen-info.-via-window-and-w.patch
    - Ticket 6786 0024-Do-not-expose-system-colors-to-CSS-or-canvas.patch

2.2 November 2012

- We released a major new version of Tor Browser which is based on Tor 0.2.3-stable branch of Tor. The announcement is published.
- We released a test version of Tor Brwoser which is based on Tor 0.2.4-alpha branch of Tor. The alpha TBB announcement is published.
- Mike attended the W3C Do Not Track and Beyond workshop, and presented Tor Browser in an attempt to demonstrate that client-side Privacy by Design can solve the same problems as server-side opt-out. My paper is up at http://www.w3.org/2012/dnt-ws/agenda.html.
- Mike went further down the PathBias rabbit hole and found a few related bugs with respect to how we handle circuit timeouts for hidden services. Additionally, it appears that it's indeed possible to tag RELAY cells in such a way that failure to ”untag" these cells results only in stream timeout conditions (which we also transparently retry on new circuits) rather than full circuit destruction. Thanks to Rob Jansen for bringing this up. Luckily, aside from the hidden service issues, CircuitStreamTimeouts and other post-construction failure modes appear almost non-existent in normal conditions once a circuit gets built successfully.
- Closed 4 tickets on the schedule for November TBB task list. The 4 tickets are:
  1. Client with low CBT can't establish any circuits
  2. Perform TBB version check async on new tab
  3. Image cache isolation causes assert crash in debug builds (and other cases?)
  4. Decide which tbb-usability tickets get addressed by a bounty program

2.3 October 2012

2.4 September 2012

We re-evaluated the inclusion of Firefox 15 favoring the Firefox ESR release series. The current ESR release is well-understood and patches are being applied with each release to improve functionality. We're beginning to work on the next ESR cycle which will be based upon Firefox 17.

In order to help make progress on this front, we've hired Pearl Crescent to help improve our Tor Browser.

2.5 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.6 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.7 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 November 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.2 October 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.3 September 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.4 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.5 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.6 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 December 2012

Updated Tor Browser bundle with new Firefox release. Updated the testing branch of TBB with Tor 0.2.4.7-alpha. The bridge-by-default bundles were updated to include Tor 0.2.4.7-alpha release. Tor 0.2.4.8-alpha) was released. (Tor 0.2.4.9 was quickly released to address a bug and will soon make it into packages.

4.2 November 2012

Updated Tor Browser Bundle with new Tor stable release. Announced and launched the testing branch of Tor Browser based on alpha Tor.

4.3 October 2012

4.4 September 2012

We updated the bridge-by-default bundles to include Tor 0.2.2.39-stable release. We also updated the Tor cloud images to fix a bug found in the unattended-upgrades configuration. The normal bridge images have also been updated to include obfsproxy, which attempts to help users circumvent censorship by transforming the Tor traffic between the client and the bridge.

4.5 August 2012

No new releases to report.

4.6 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.7 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 December 2012

We released new combined flashproxy and pyobfsproxy bundles for users who need them. The bundles also includes an experimental obfs3 bridge—obfs3 is a new protocol designed to be harder to identify than the previous obfs2.

5.2 November 2012

Hired a flashproxy developer. Released flashproxy version 0.9 and version 0.10. These include binaries for the Microsoft Windows Operating System and improved documentation. Also Made the facilitator hand out more proxies by default, reducing a client's need to re-register.

5.3 October 2012

Released flashproxy version 0.8. Fixed a number of Microsoft Windows bugs. A big change is that flashproxy-client now operates as a managed proxy by default. This means that there is no longer a need to start flashproxy-client separately from Tor.

5.4 September 2012

Continued progress on flashproxy development. Released flashproxy version 0.4. This includes the ability to use HTTPS, easy instructions for getting it working in Debian Linux Operating System, fixed some command-line options, and updated the README directions.

5.5 August 2012

No progress to report.

5.6 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.7 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 December 2012

See C.2.7 above.

6.2 November 2012

See C.2.7 above.

6.3 October 2012

See C.2.7 above.

6.4 September 2012

See C.2.7 above.

6.5 August 2012

See C.2.7 above.

6.6 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.7 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 December 2012

See C.2.9 above.

7.2 November 2012

See C.2.9 above.

7.3 October 2012

See C.2.9 above.

7.4 September 2012

See C.2.9 above.

7.5 August 2012

No progress to report.

7.6 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.7 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

Tor Solutions
CORPORATION

July 2012 Progress Report for BBG Contract 50-D-11-0061

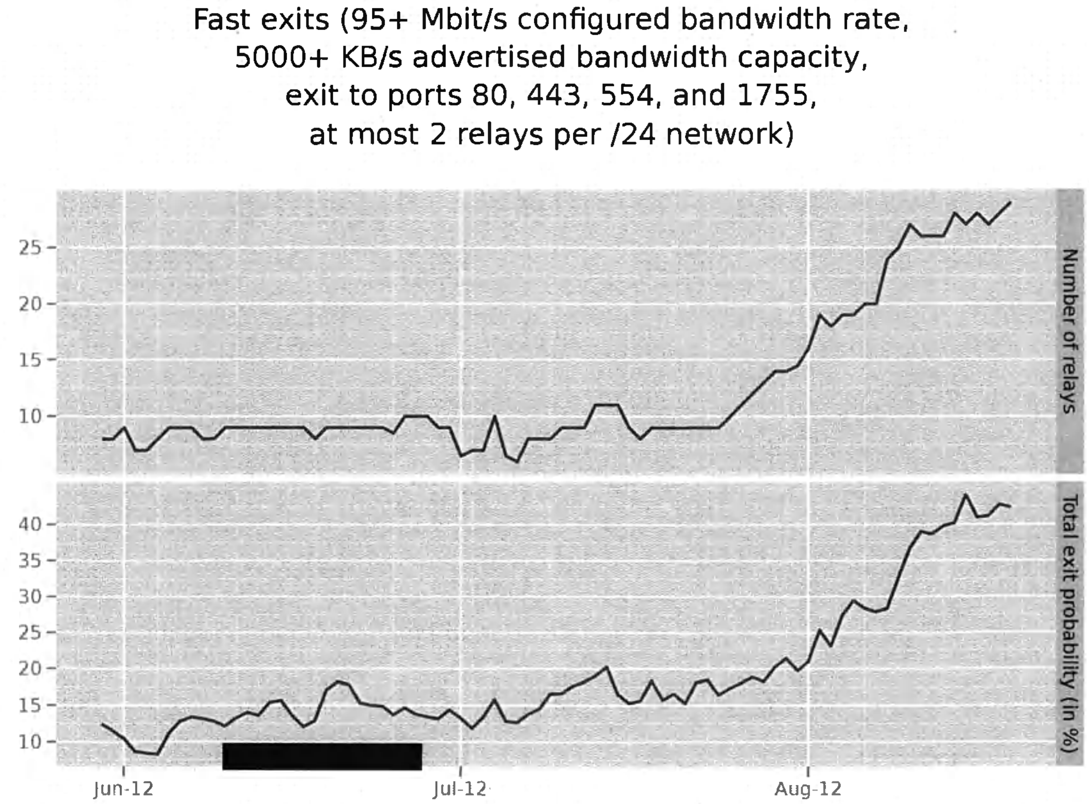
Tor Solutions Corp

Contents

1 C.2.1, C.2.2, C.2.3, C.2.4

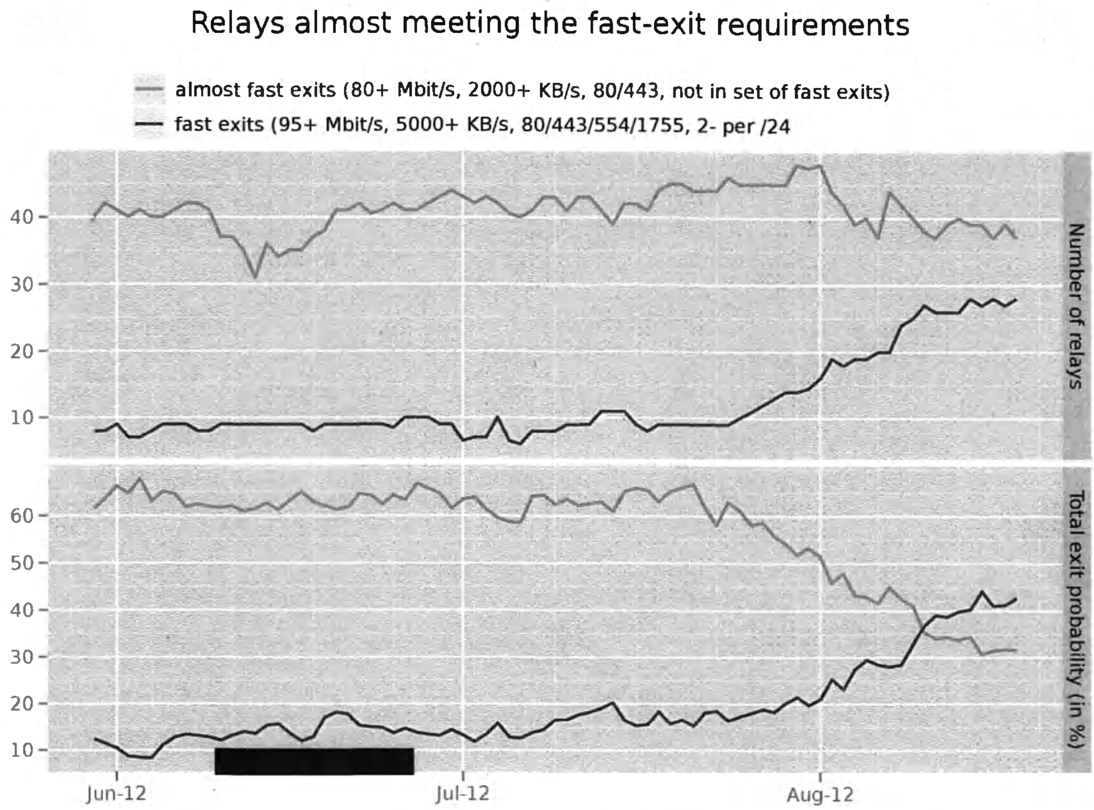
1.1 July 2012

The 'fast exit count' graphs are now updated daily at `https://metrics.torproject.org/fast-exits.html` We're up to 28 or so.


Fast exits (95+ Mbit/s configured bandwidth rate, 5000+ KB/s advertised bandwidth capacity, exit to ports 80, 443, 554, and 1755, at most 2 relays per /24 network)

[redacted]

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20%

to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.2 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.2 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.2 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.2 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.2 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.2 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.2 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

June 2012 Progress Report
for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

1 C.2.1, C.2.2, C.2.3, C.2.4

1.1 June 2012

Started to develop a plan for implmentation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 June 2012

Developing a plan to implmement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

Tor Solutions
CORPORATION

November 18 - December 17 2012 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

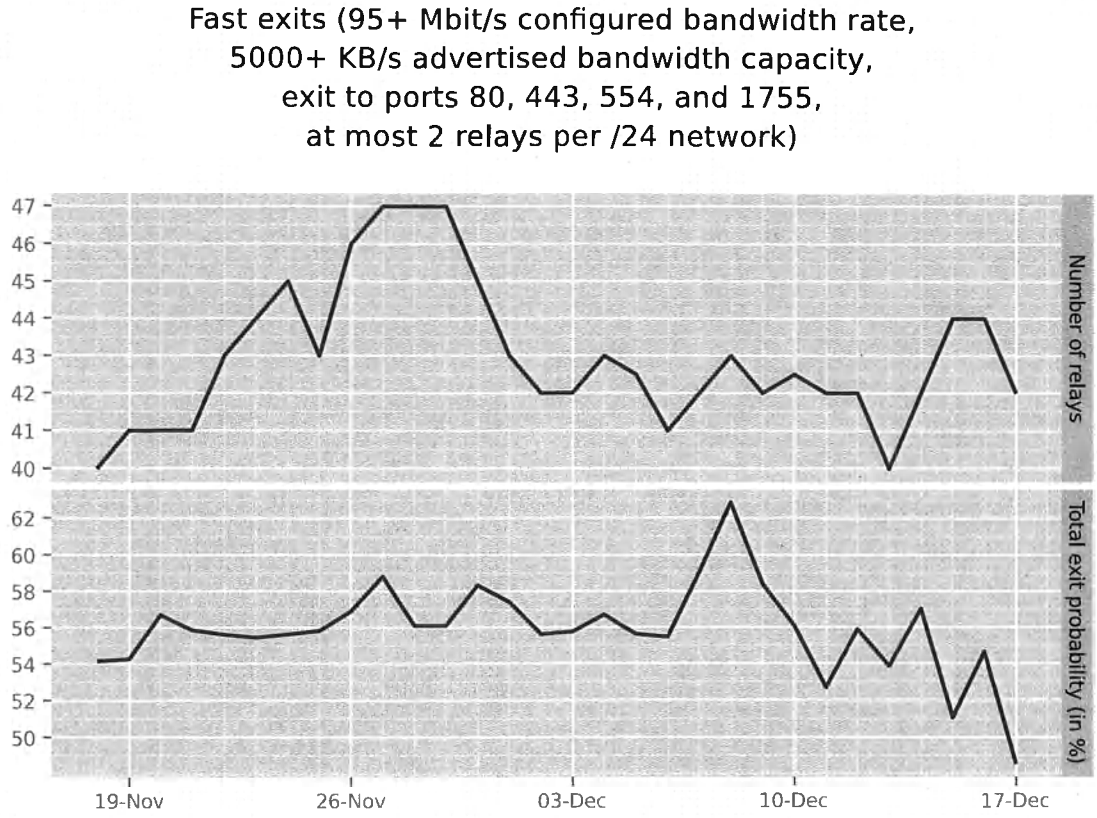
1 C.2.1, C.2.2, C.2.3, C.2.4

1.1 November 2012

We're at 38 qualifying fast exits providing 33.6749% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 51 qualifying fast exits providing 44.3442% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

Figure 1: Relays meeting the fast-exit requirements

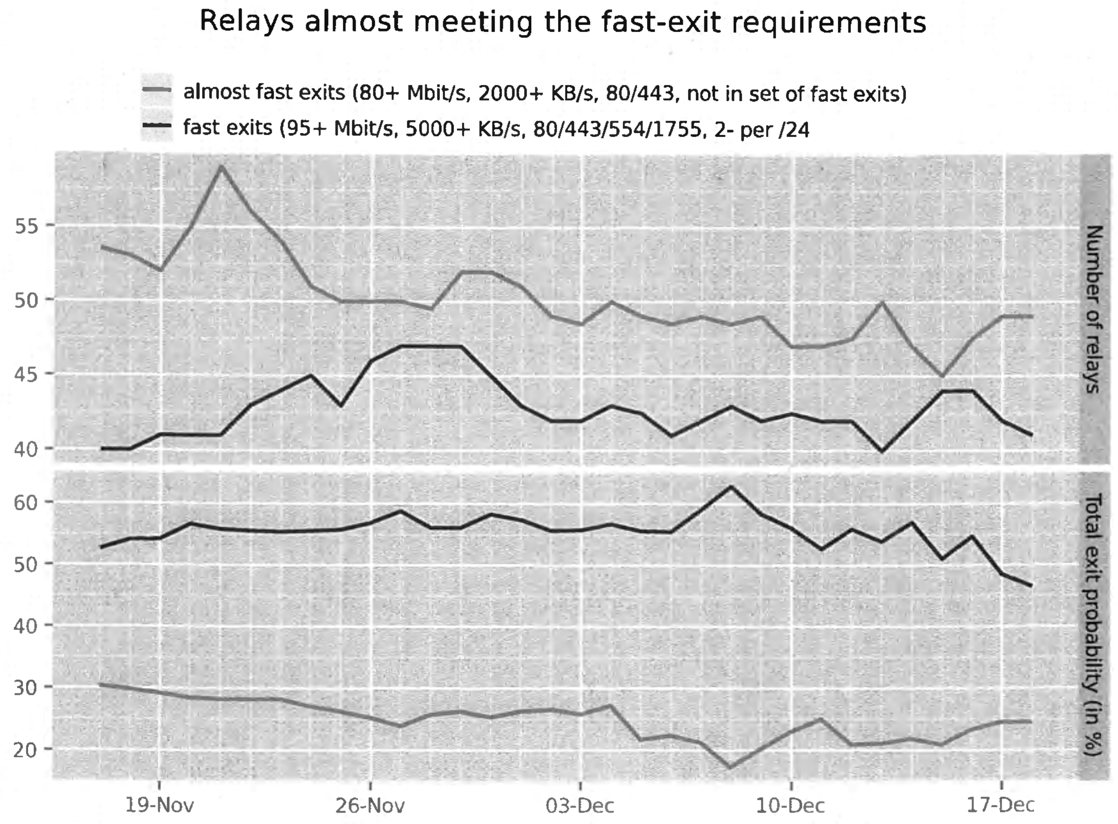


1.2 October 2012

We're up to 41 qualifying fast exits providing 22.9375% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 57 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24

Figure 2: Relays almost meeting the fast-exit requirements



diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

Discussions with lawyers continue. These discussions are blocking further progress on contracts and announcements of exit relay organizations.

1.3 September 2012

1.3.1 Exit Relays

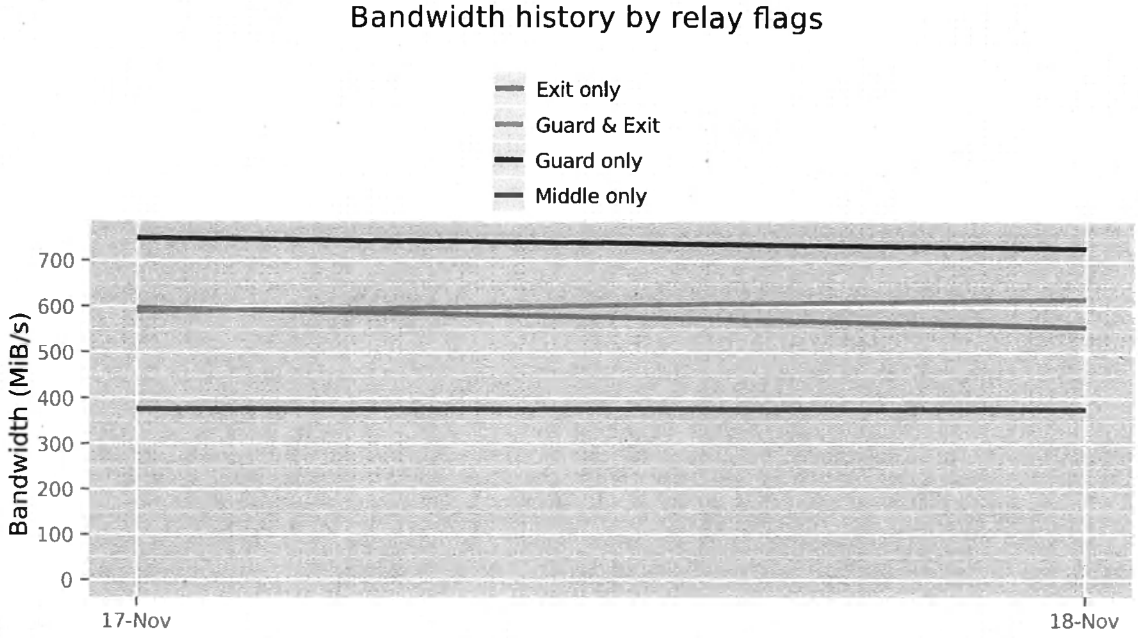
We're holding at 28 qualifying fast exits providing 16.667% of the bandwidth. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 37 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 57% of the exit probability.

We are in negotiations with three organizations running a majority of the exit relay capacity. These three orgs will be publicly announced when contracts are signed.

We are in final discussions about the Tor network and legal aspects of running a funded relay under US laws. The main concern here is not falling under the definition of Internet Service Provider

Figure 3: Relay bandwidth by Exit and/or Guard flags



Bandwidth history by relay flags

The Tor Project - https://metrics.torproject.org/

or telecommunications carrier which would subject Tor to CALEA compliance regulations.

1.4 August 2012

1.4.1 Exit Relays

We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

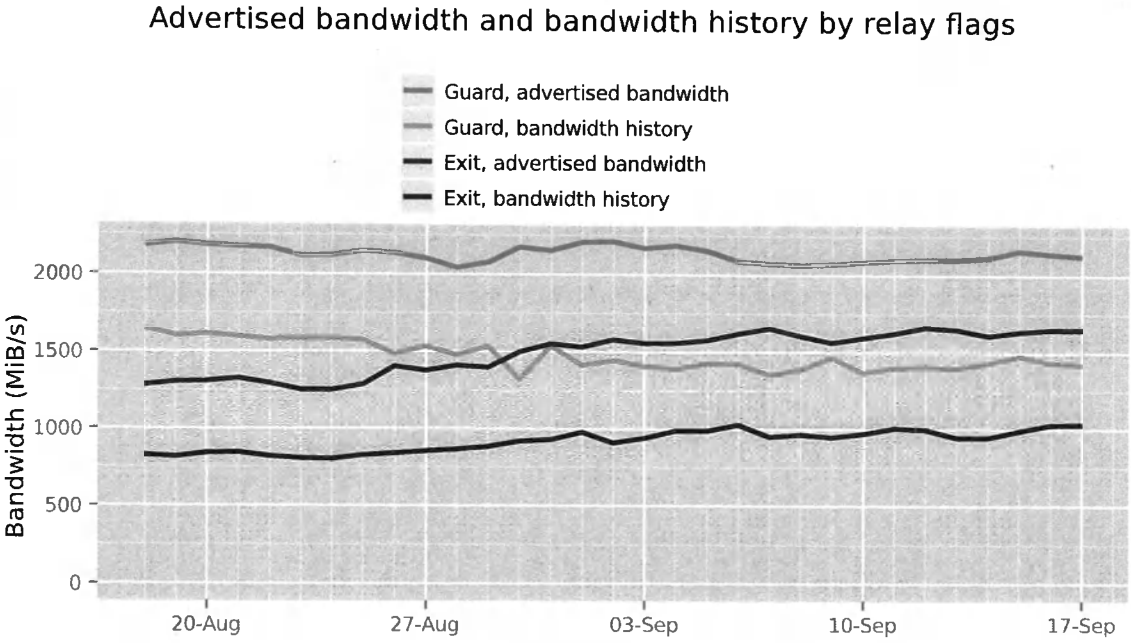
We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

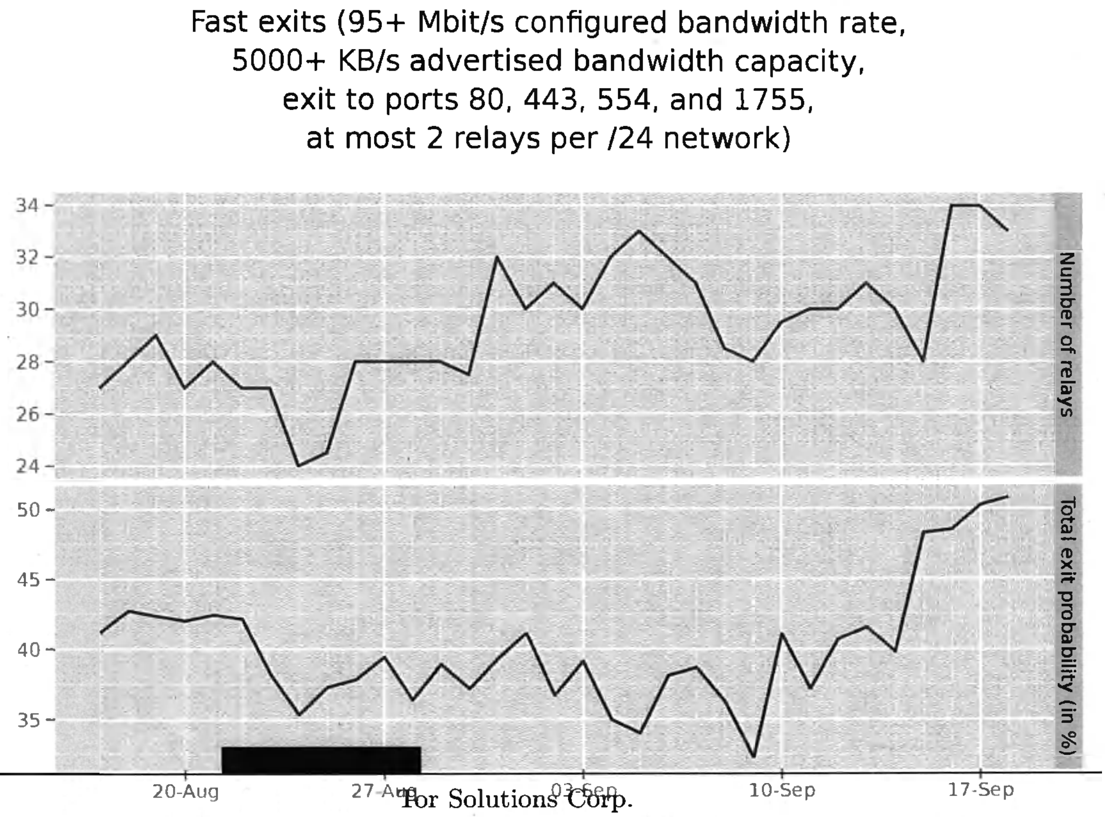
Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

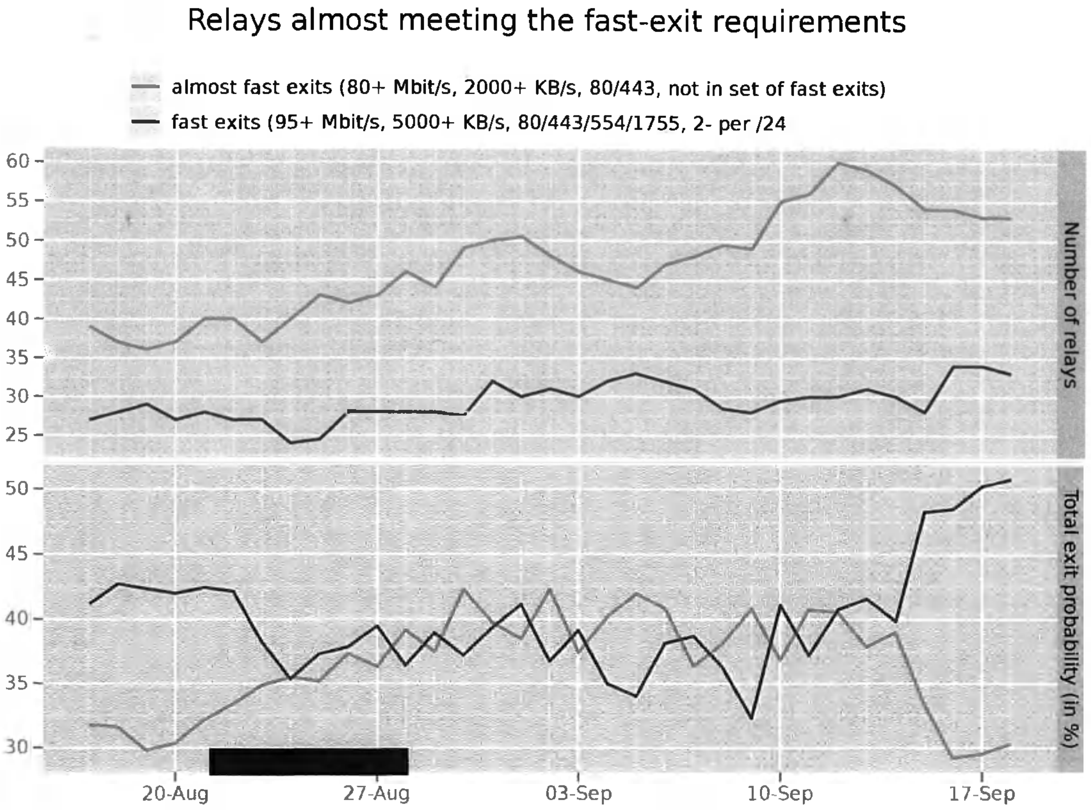
Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.

Figure 4: Relay bandwidth by Exit and/or Guard flags



The Tor Project - https://metrics.torproject.org/





Karsten added `https://metrics.torproject.org/network.html#bandwidth-flags` for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: `https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags`.

1.4.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

We've set up our new "bridgeguard" tool on this bridge: `https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md`

Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL

client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

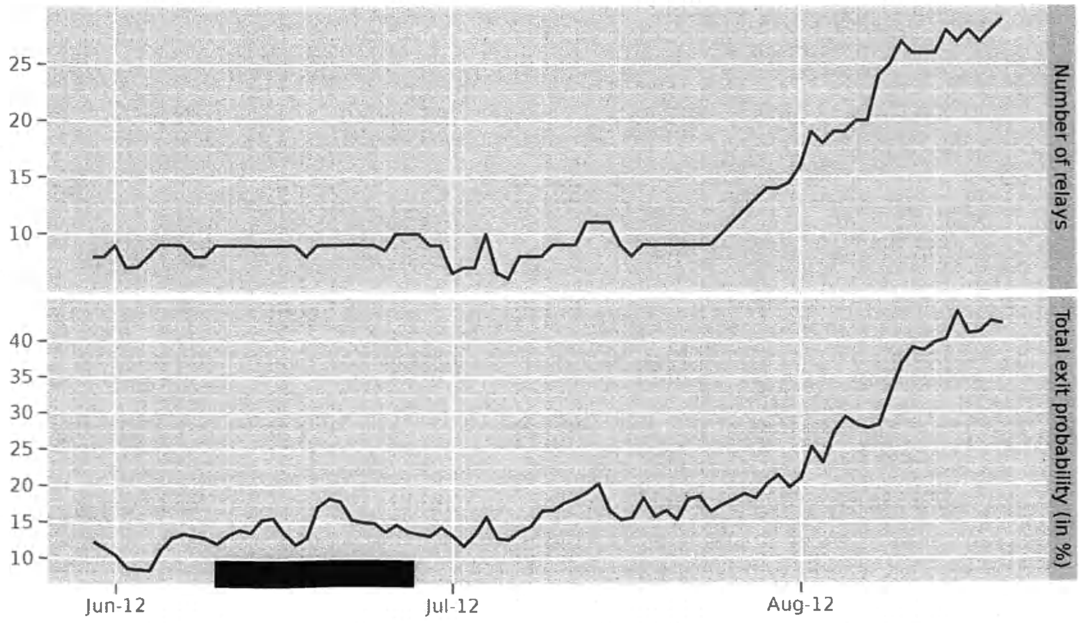
To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
`https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles` Lots of options as we go forward.

1.5 July 2012

The 'fast exit count' graphs are now updated daily at `https://metrics.torproject.org/fast-exits.html` We're up to 28 or so.

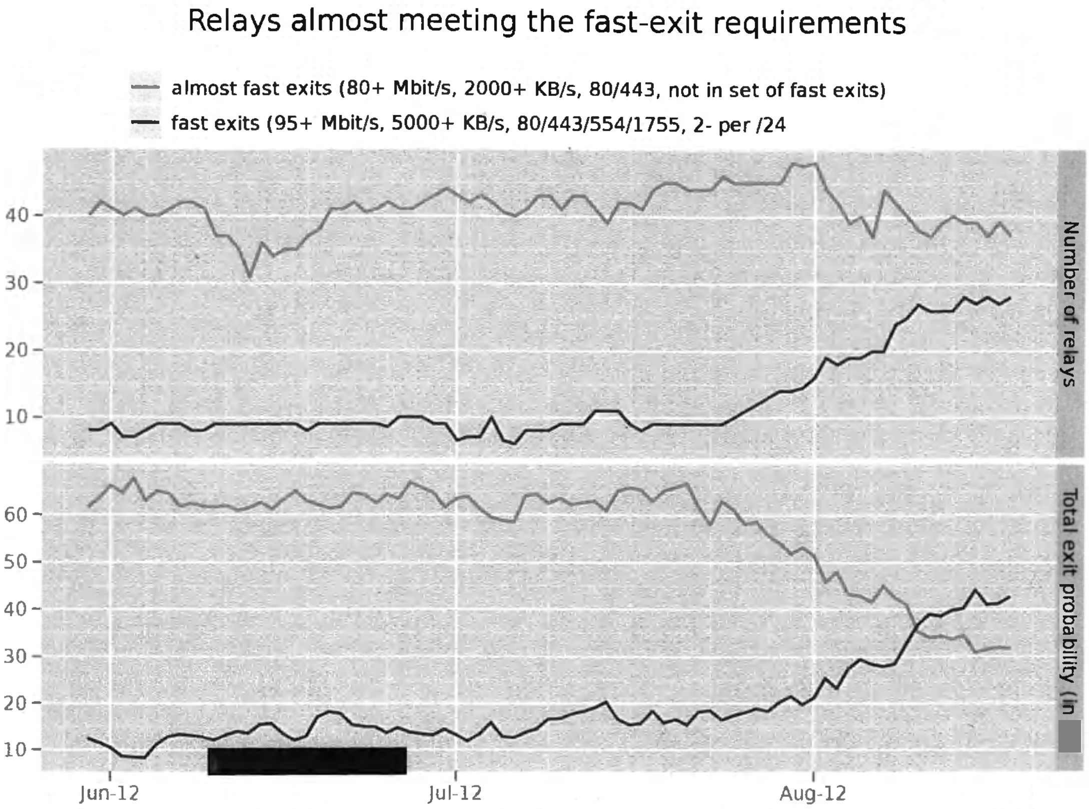
Fast exits (95+ Mbit/s configured bandwidth rate,
5000+ KB/s advertised bandwidth capacity,
exit to ports 80, 443, 554, and 1755,
at most 2 relays per /24 network)



[redacted]

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays

are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20% to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.6 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 November 2012

- We released a major new version of Tor Browser which is based on Tor 0.2.3-stable branch of Tor. The announcement is published.
- We released a test version of Tor Brwoser which is based on Tor 0.2.4-alpha branch of Tor. The alpha TBB announcement is published.
- Mike attended the W3C Do Not Track and Beyond workshop, and presented Tor Browser in an attempt to demonstrate that client-side Privacy by Design can solve the same problems as server-side opt-out. My paper is up at http://www.w3.org/2012/dnt-ws/agenda.html.
- Mike went further down the PathBias rabbit hole and found a few related bugs with respect to how we handle circuit timeouts for hidden services. Additionally, it appears that it's indeed possible to tag RELAY cells in such a way that failure to "untag" these cells results only in stream timeout conditions (which we also transparently retry on new circuits) rather than full circuit destruction. Thanks to Rob Jansen for bringing this up. Luckily, aside from the hidden service issues, CircuitStreamTimeouts and other post-construction failure modes appear almost non-existent in normal conditions once a circuit gets built successfully.
- Closed 4 tickets on the schedule for November TBB task list. The 4 tickets are:
    1. Client with low CBT can't establish any circuits
    2. Perform TBB version check async on new tab
    3. Image cache isolation causes assert crash in debug builds (and other cases?)
    4. Decide which tbb-usability tickets get addressed by a bounty program

2.2 October 2012

2.3 September 2012

We re-evaluated the inclusion of Firefox 15 favoring the Firefox ESR release series. The current ESR release is well-understood and patches are being applied with each release to improve functionality. We're beginning to work on the next ESR cycle which will be based upon Firefox 17.

In order to help make progress on this front, we've hired Pearl Crescent to help improve our Tor Browser.

2.4 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.5 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.6 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 November 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.2 October 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.3 September 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.4 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.5 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.6 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 November 2012

Updated Tor Browser Bundle with new Tor stable release. Announced and launched the testing branch of Tor Browser based on alpha Tor.

4.2 October 2012

4.3 September 2012

We updated the bridge-by-default bundles to include Tor 0.2.2.39-stable release. We also updated the Tor cloud images to fix a bug found in the unattended-upgrades configuration. The normal bridge images have also been updated to include obfsproxy, which attempts to help users circumvent censorship by transforming the Tor traffic between the client and the bridge.

4.4 August 2012

No new releases to report.

4.5 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.6 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 November 2012

Hired a flashproxy developer. Released flashproxy version 0.9 and version 0.10. These include binaries for the Microsoft Windows Operating System and improved documentation. Also Made the facilitator hand out more proxies by default, reducing a client's need to re-register.

5.2 October 2012

Released flashproxy version 0.8. Fixed a number of Microsoft Windows bugs. A big change is that flashproxy-client now operates as a managed proxy by default. This means that there is no longer a need to start flashproxy-client separately from Tor.

5.3 September 2012

Continued progress on flashproxy development. Released flashproxy version 0.4. This includes the ability to use HTTPS, easy instructions for getting it working in Debian Linux Operating System, fixed some command-line options, and updated the README directions.

5.4 August 2012

No progress to report.

5.5 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.6 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 November 2012

See C.2.7 above.

6.2 October 2012

See C.2.7 above.

6.3 September 2012

See C.2.7 above.

6.4 August 2012

See C.2.7 above.

6.5 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.6 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 November 2012

See C.2.9 above.

7.2 October 2012

See C.2.9 above.

7.3 September 2012

See C.2.9 above.

7.4 August 2012

No progress to report.

7.5 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.6 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

Tor Solutions
CORPORATION

October 18 - November 17 2012 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

1 C.2.1, C.2.2, C.2.3, C.2.4

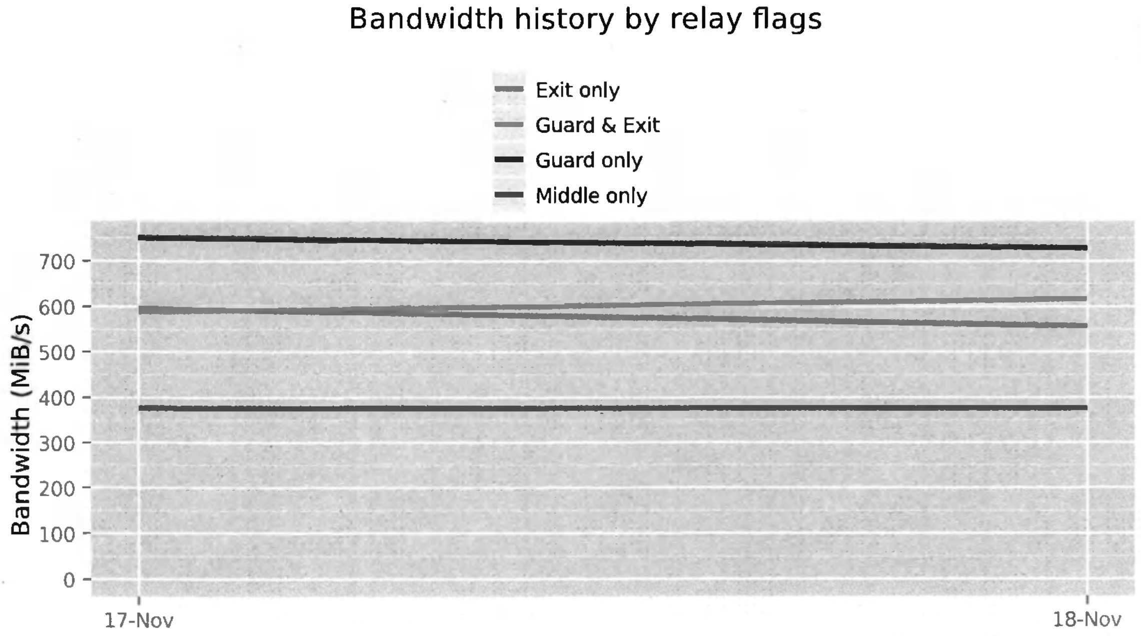
1.1 October 2012

We're up to 41 qualifying fast exits providing 22.9375% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 57 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

Discussions with lawyers continue. These discussions are blocking further progress on contracts and announcements of exit relay organizations.

Figure 1: Relay bandwidth by Exit and/or Guard flags



Bandwidth history by relay flags

The Tor Project - https://metrics.torproject.org/

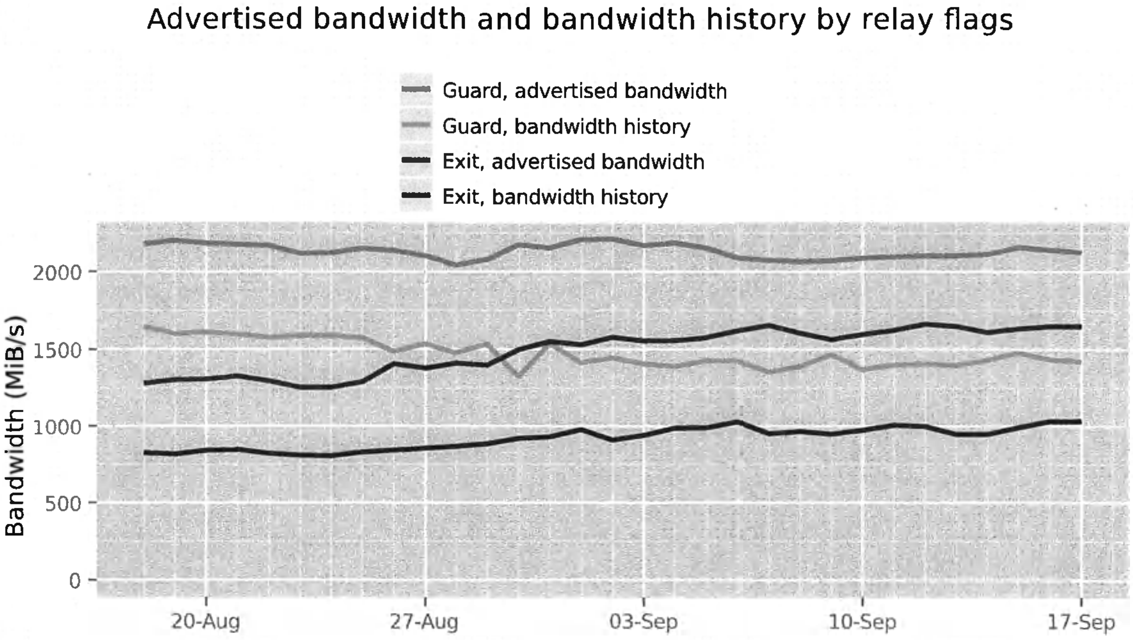
1.2 September 2012

1.2.1 Exit Relays

We're holding at 28 qualifying fast exits providing 16.667% of the bandwidth. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 37 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 57% of the exit probability.

Figure 2: Relay bandwidth by Exit and/or Guard flags



The Tor Project - https://metrics.torproject.org/

We are in negotiations with three organizations running a majority of the exit relay capacity. These three orgs will be publicly announced when contracts are signed.

We are in final discussions about the Tor network and legal aspects of running a funded relay under US laws. The main concern here is not falling under the definition of Internet Service Provider or telecommunications carrier which would subject Tor to CALEA compliance regulations.

1.3 August 2012

1.3.1 Exit Relays

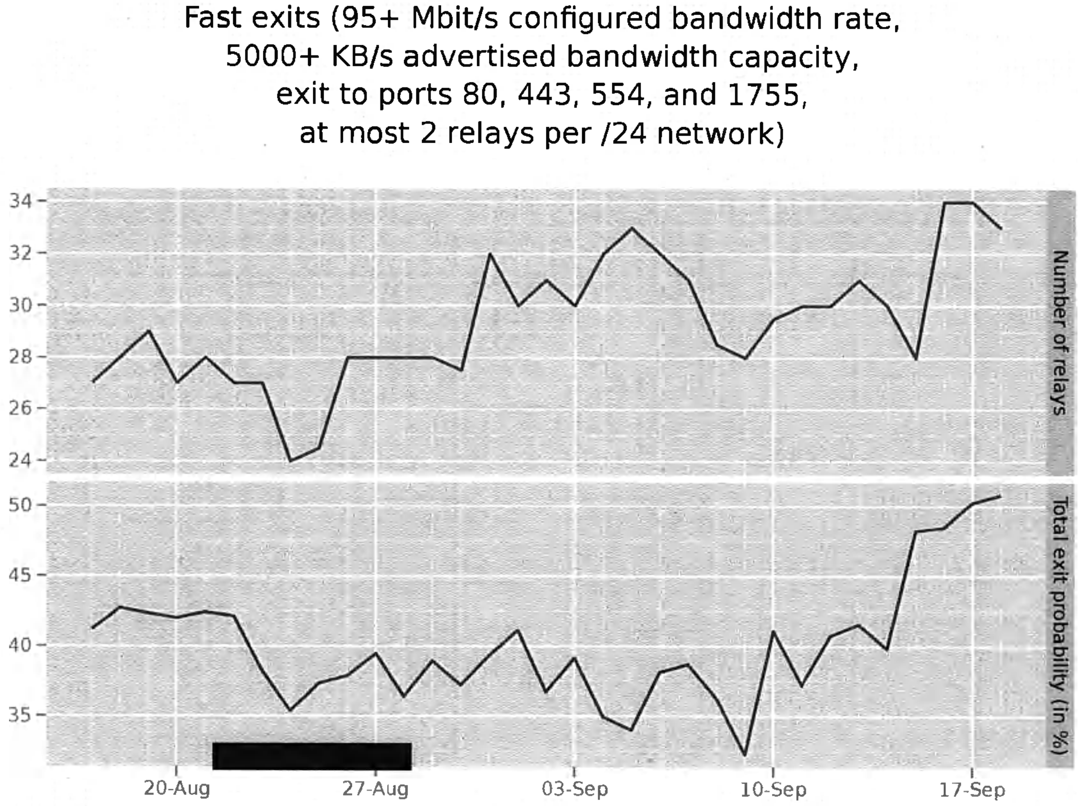
We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

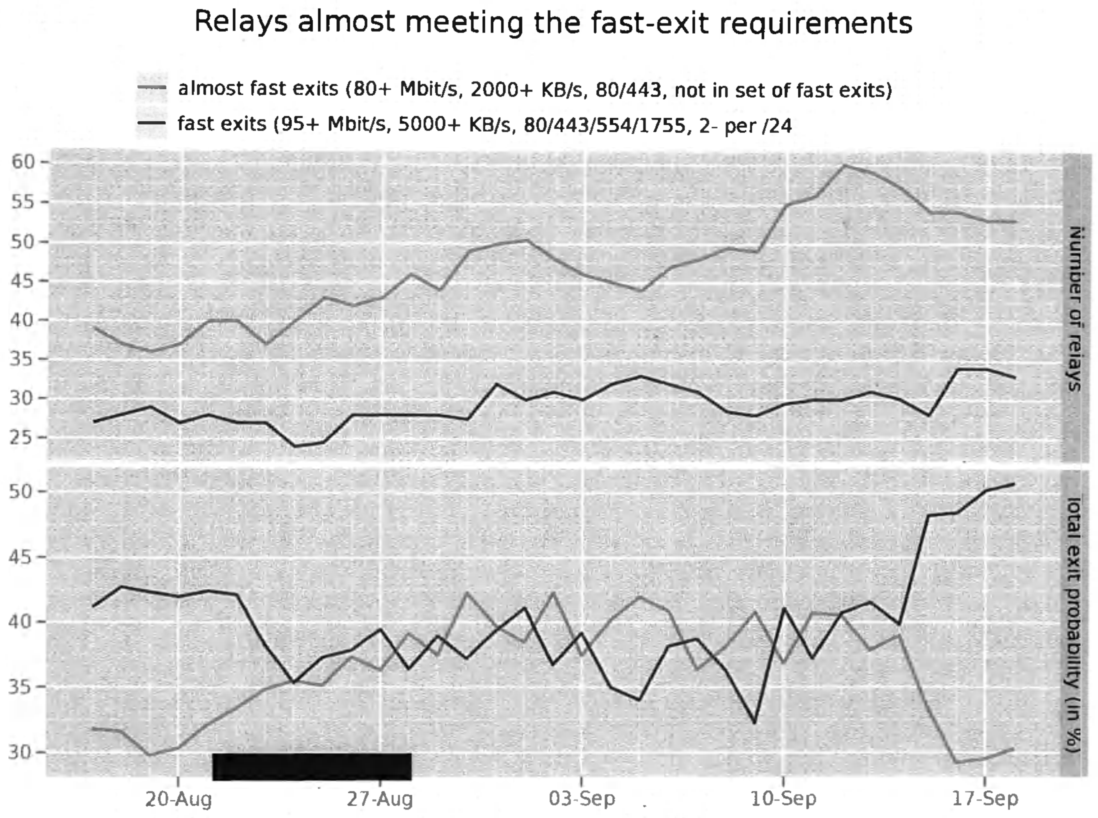
Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.



[redacted]



Karsten added `https://metrics.torproject.org/network.html#bandwidth-flags` for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: `https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags`.

1.3.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

We've set up our new "bridgeguard" tool on this bridge: `https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md`

Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL

client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

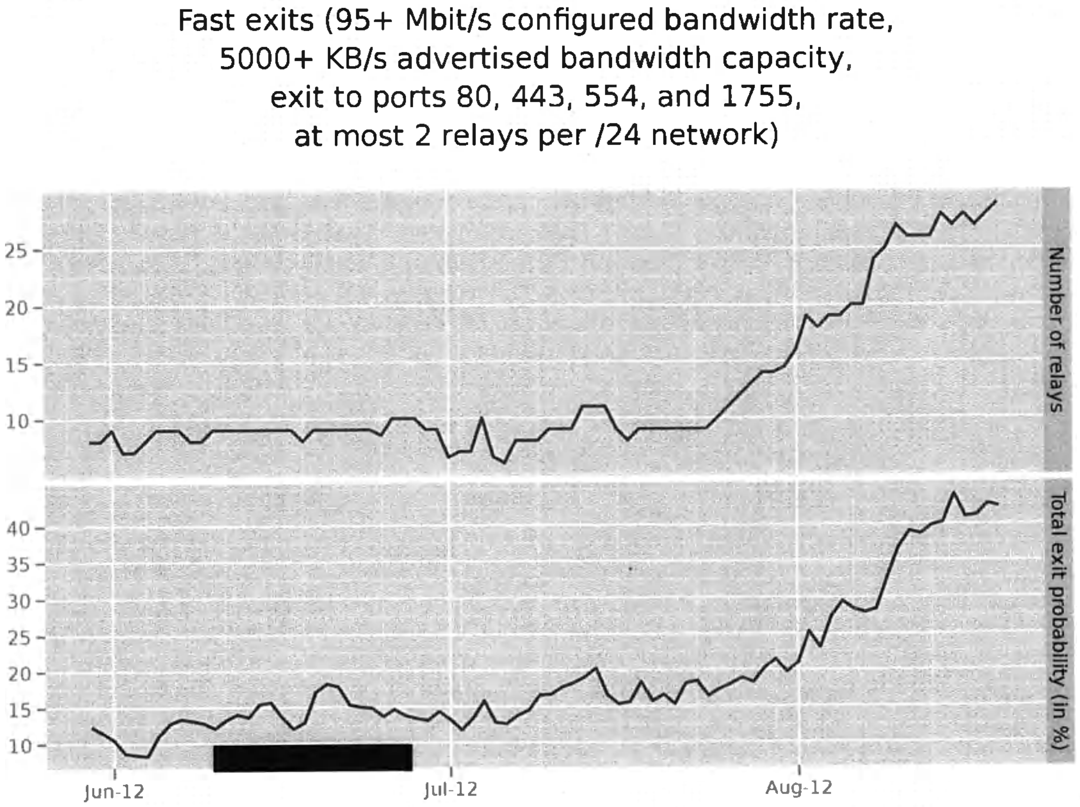
Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
`https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles` Lots of options as we go forward.

1.4 July 2012

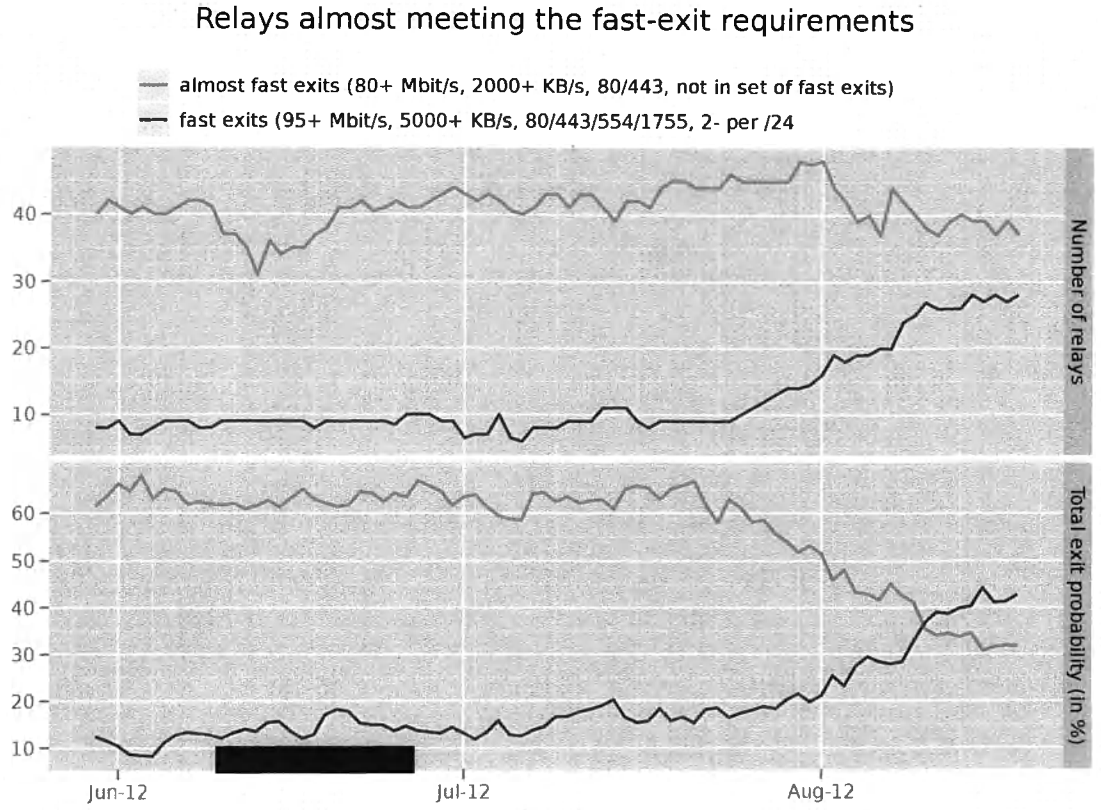
The 'fast exit count' graphs are now updated daily at `https://metrics.torproject.org/fast-exits.html` We're up to 28 or so.



[redacted]

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays

are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20% to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.5 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 October 2012

2.2 September 2012

We re-evaluated the inclusion of Firefox 15 favoring the Firefox ESR release series. The current ESR release is well-understood and patches are being applied with each release to improve functionality. We're beginning to work on the next ESR cycle which will be based upon Firefox 17.

In order to help make progress on this front, we've hired Pearl Crescent to help improve our Tor Browser.

2.3 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.4 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.5 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 October 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.2 September 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.3 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.4 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.5 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 October 2012

4.2 September 2012

We updated the bridge-by-default bundles to include Tor 0.2.2.39-stable release. We also updated the Tor cloud images to fix a bug found in the unattended-upgrades configuration. The normal bridge images have also been updated to include obfsproxy, which attempts to help users circumvent censorship by transforming the Tor traffic between the client and the bridge.

4.3 August 2012

No new releases to report.

4.4 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.5 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 October 2012

Released flashproxy version 0.8. Fixed a number of Microsoft Windows bugs. A big change is that flashproxy-client now operates as a managed proxy by default. This means that there is no longer a need to start flashproxy-client separately from Tor.

5.2 September 2012

Continued progress on flashproxy development. Released flashproxy version 0.4. This includes the ability to use HTTPS, easy instructions for getting it working in Debian Linux Operating System, fixed some command-line options, and updated the README directions.

5.3 August 2012

No progress to report.

5.4 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.5 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 October 2012

See C.2.7 above.

6.2 September 2012

See C.2.7 above.

6.3 August 2012

See C.2.7 above.

6.4 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.5 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 October 2012

See C.2.9 above.

7.2 September 2012

See C.2.9 above.

7.3 August 2012

No progress to report.

7.4 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.5 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

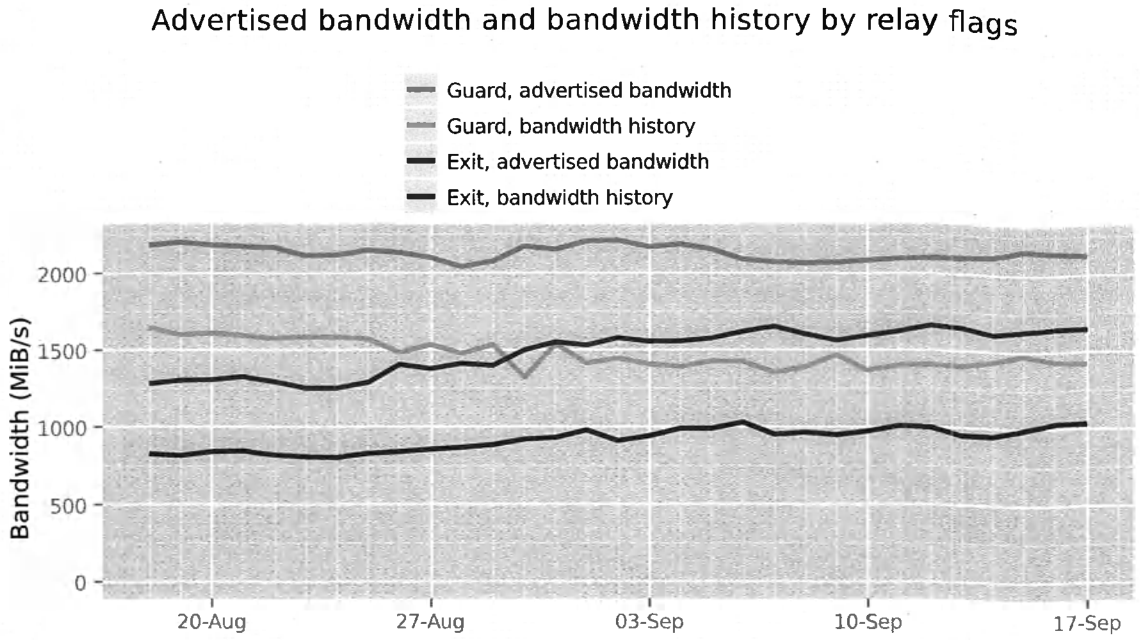
Tor Solutions
CORPORATION

September 2012 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

Figure 1: Relay bandwidth by Exit and/or Guard flags



The Tor Project - https://metrics.torproject.org/

1 C.2.1, C.2.2, C.2.3, C.2.4

1.1 September 2012

1.1.1 Exit Relays

We're holding at 28 qualifying fast exits providing 16.667% of the bandwidth. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 37 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 57% of the exit probability.

We are in negotiations with three organizations running a majority of the exit relay capacity. These three orgs will be publicly announced when contracts are signed.

We are in final discussions about the Tor network and legal aspects of running a funded relay under US laws. The main concern here is not falling under the definition of Internet Service Provider or telecommunications carrier which would subject Tor to CALEA compliance regulations.

1.2 August 2012

1.2.1 Exit Relays

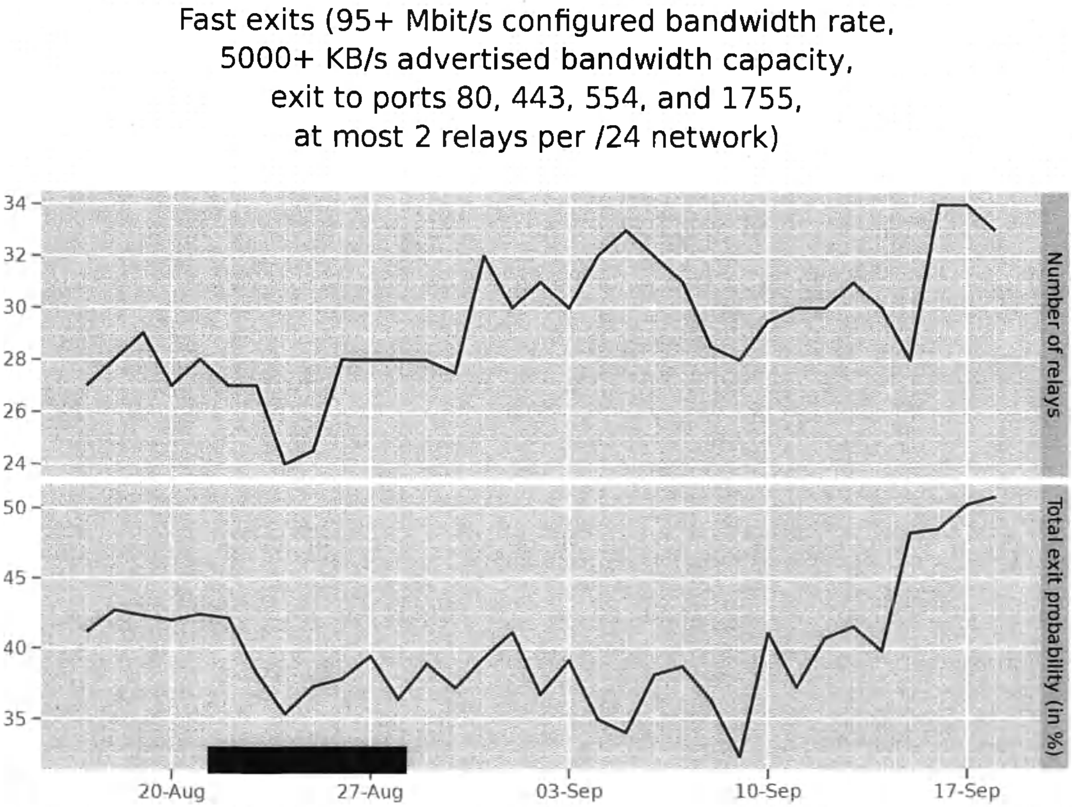
We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

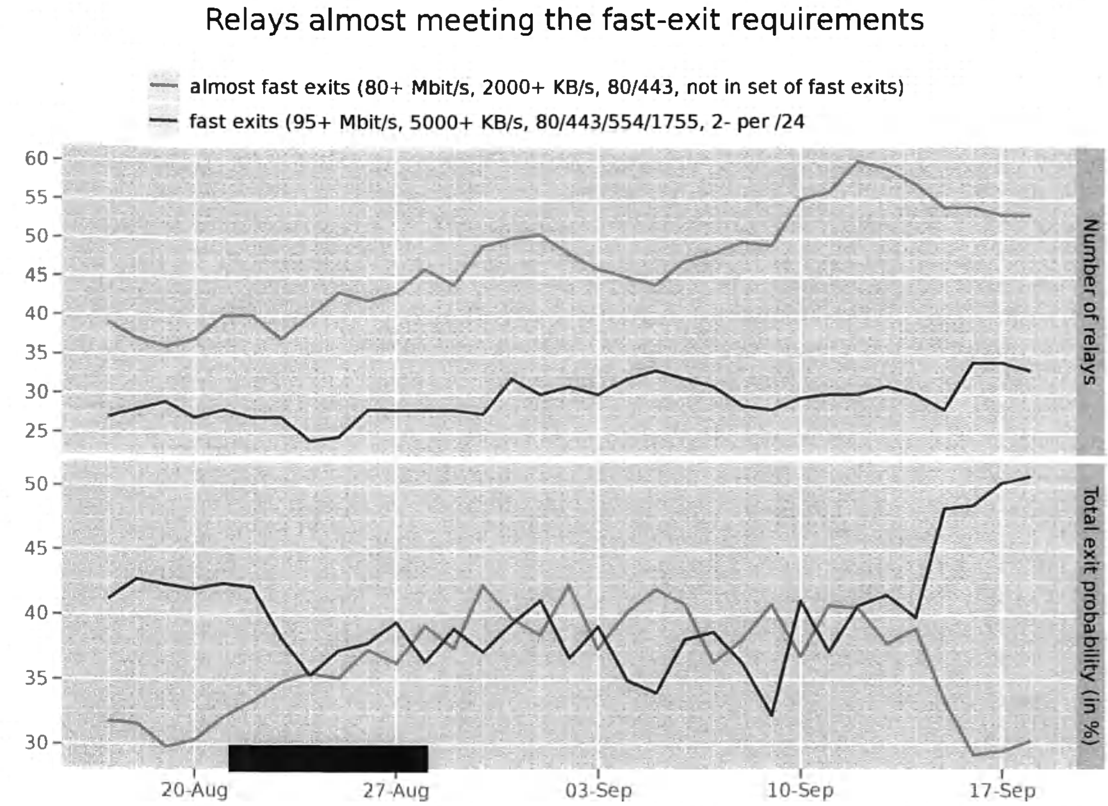
Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.



[redacted]



[redacted]

Karsten added https://metrics.torproject.org/network.html#bandwidth-flags for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags.

1.2.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

We've set up our new "bridgeguard" tool on this bridge: https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md

Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL

client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

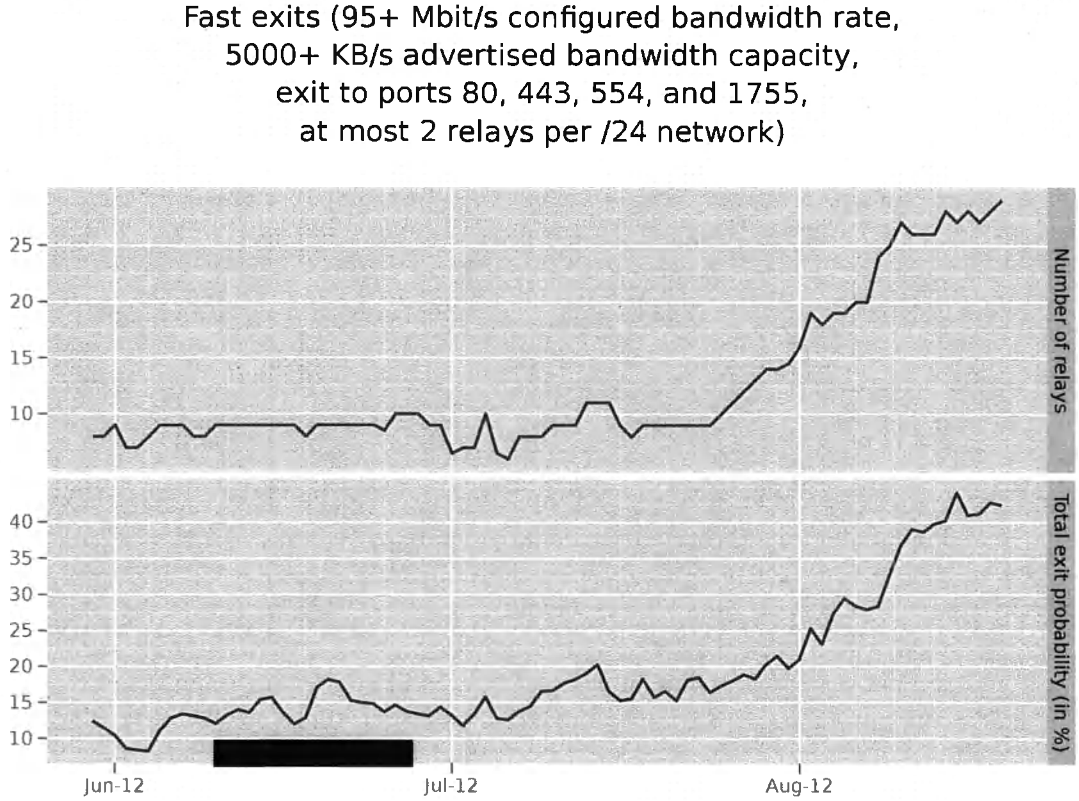
Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles Lots of options as we go forward.

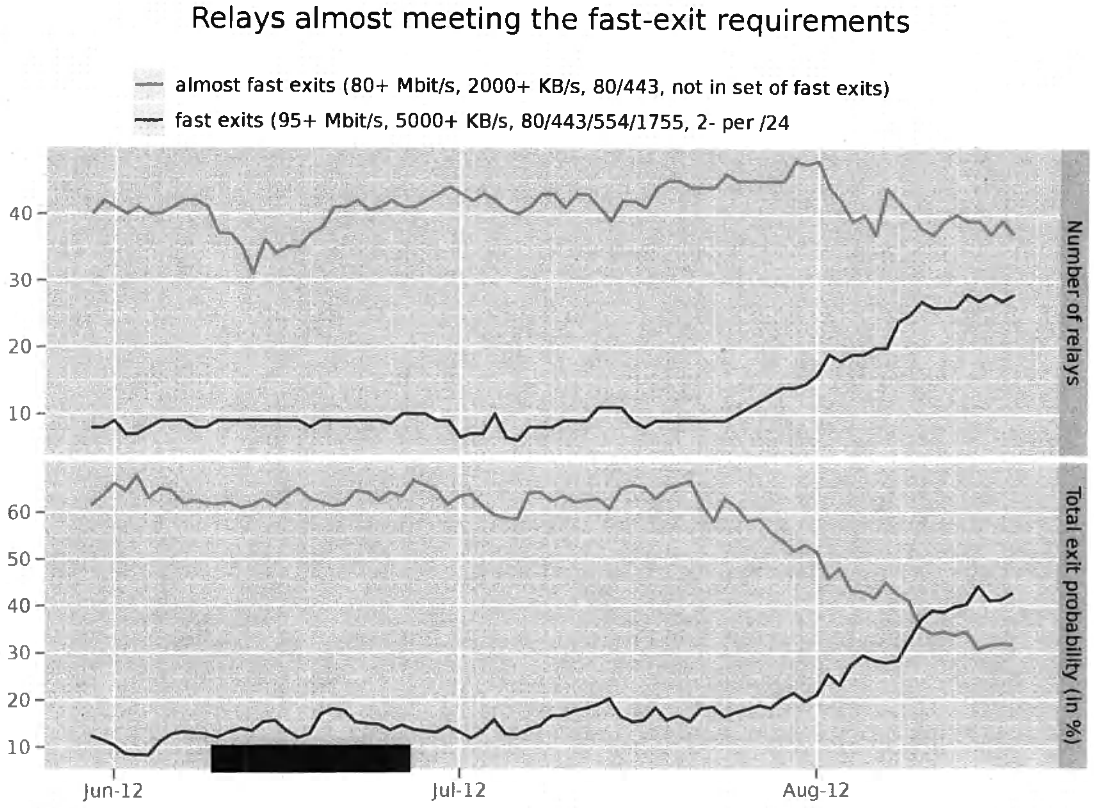
1.3 July 2012

The 'fast exit count' graphs are now updated daily at https://metrics.torproject.org/fast-exits.html We're up to 28 or so.



If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays

are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).



[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at `https://compass.torproject.org/`.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: `https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html` with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20% to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.4 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 September 2012

We re-evaluated the inclusion of Firefox 15 favoring the Firefox ESR release series. The current ESR release is well-understood and patches are being applied with each release to improve functionality. We're beginning to work on the next ESR cycle which will be based upon Firefox 17.

In order to help make progress on this front, we've hired Pearl Crescent to help improve our Tor Browser.

2.2 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.3 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.4 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 September 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.2 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.3 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.4 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 September 2012

We updated the bridge-by-default bundles to include Tor 0.2.2.39-stable release. We also updated the Tor cloud images to fix a bug found in the unattended-upgrades configuration. The normal bridge images have also been updated to include obfsproxy, which attempts to help users circumvent censorship by transforming the Tor traffic between the client and the bridge.

4.2 August 2012

No new releases to report.

4.3 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.4 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 September 2012

Continued progress on flashproxy development. Released flashproxy version 0.4. This includes the ability to use HTTPS, easy instructions for getting it working in Debian Linux Operating System, fixed some command-line options, and updated the README directions.

5.2 August 2012

No progress to report.

5.3 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.4 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 September 2012

See C.2.7 above.

6.2 August 2012

See C.2.7 above.

6.3 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.4 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 September 2012

See C.2.9 above.

7.2 August 2012

No progress to report.

7.3 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.4 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

Tor Solutions
CORPORATION

January 4, 2013

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #06:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 November 2012 - 17 December 2012	$25,000	$150,000
E013-12-IQ-00005-0	18 November 2012 - 17 December 2012	$39,633.35	$237,800.10
Total Invoice		$64,633.35	$387,800.10

Thank you.

TorProject Invoice #BBG20130104

Tor Solutions
CORPORATION

January 29, 2013

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #07:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 December 2012 - 17 January 2013	$25,000	$175,000
E013-12-IQ-00005-0	18 December 2012 - 17 January 2013	$39,633.35	$277,433.45
Total Invoice		$64,633.35	$452,433.45

Thank you.

TorProject Invoice #BBG20130128

March 3, 2013

Tor Solutions
CORPORATION

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #08:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 January 2013 - 17 February 2013	$25,000	$200,000
E013-12-IQ-00005-0	18 January 2013 - 17 February 2013	$39,633.35	$317,066.80
Total Invoice		$64,633.35	$517,066.80

Thank you.

TorProject Invoice #BBG20130303

April 11, 2013

Tor Solutions
CORPORATION

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #09:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 February 2013 - 17 March 2013	$25,000	$225,000
E013-12-IQ-00005-0	18 February 2013 - 17 March 2013	$39,633.35	$356,700.15
Total Invoice		$64,633.35	$581,700.15

Thank you.

TorProject Invoice #BBG20130411

May 13, 2013

Tor Solutions
CORPORATION

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #10:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 March 2013 - 17 April 2013	$25,000	$250,000
E013-12-IQ-00005-0	18 March 2013 - 17 April 2013	$39,633.35	$396,333.50
Total Invoice		$64,633.35	$646,333.50

Thank you.

TorProject Invoice #BBG20130513

Tor Solutions
CORPORATION

June 4, 2013

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #11:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 April 2013 - 17 May 2013	$25,000	$275,000
E013-12-IQ-00005-0	18 April 2013 - 17 May 2013	$39,633.35	$435,966.85
Total Invoice		$64,633.35	$710,966.85

Thank you.

TorProject Invoice #BBG20130604

Tor Solutions
CORPORATION

July 9, 2013

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
969 Main Street, Suite 206
Walpole, MA 02081-2972 USA

Invoice #12:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00038-0	18 May 2013 - 17 June 2013	$25,000	$300,000
E013-12-IQ-00005-0	18 May 2013 - 17 June 2013	$39,633.35	$475,600.20
Total Invoice		$64,633.35	$775,600.20

Thank you.

TorProject Invoice #BBG20130709

Tor Solutions
CORPORATION

September 30, 2013

BBG
Office of Engineering and Technical Services
330 Independence Ave SW
Washington, DC 20237

Please pay this invoice for Contract BBG50-D-11-0061-1. Services rendered are reflected in our monthly progress report emailed separately. Tor Solutions Corp is listed in USG Central Contractor Registration.

Please submit payment with Net30 terms to:

Tor Solutions Corp.
7 Temple Street, Suite A
Cambridge, MA 02139

Invoice #13:

Purchase Request Reference	Period	Current Amount	Total Amount
T013-12-IQ-00096-0, line 3	09/18/2012-09/17/2013	$126,000	$126,000
T013-12-IQ-00096-0, line 4	09/18/2012-09/17/2013	$100,800	$100,800
T013-12-IQ-00096-0, line 5	09/18/2012-09/17/2013	$189,000	$189,000
T013-12-IQ-00096-0, line 6	09/18/2012-09/17/2013	$50,000	$50,000
Total Invoice		$465,800	$465,800

Thank you.

TorProject Invoice #BBG20130815

Tor Solutions
CORPORATION

April 18 - May 17 2013 Progress Report for BBG Contract 50-D-11-0061

Tor Solutions Corp

Contents

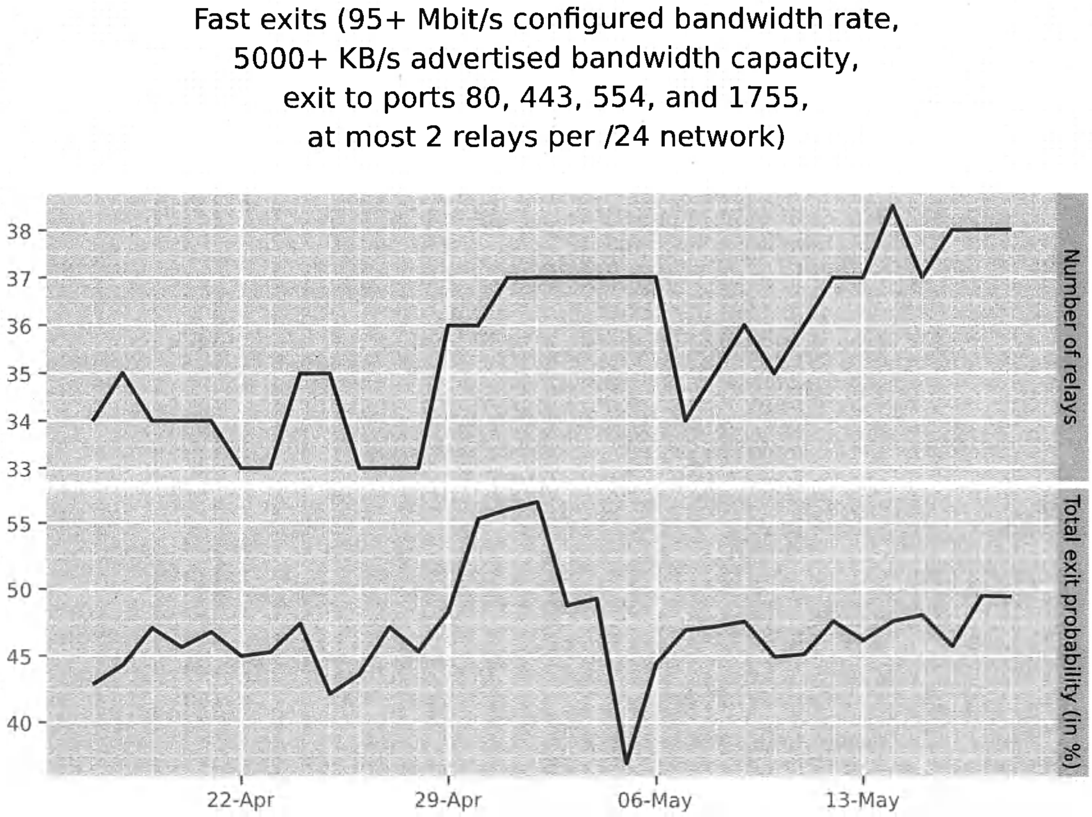
1 C.2.1, C.2.2, C.2.3, C.2.4

1.1 April 2013

We're at 39 qualifying fast exists providing 23.5131% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 49 qualifying fast exits providing 30.2807% of the bandwidth if we ignore the /24 diversity requirement.

Figure 1: Relays meeting the fast-exit requirements

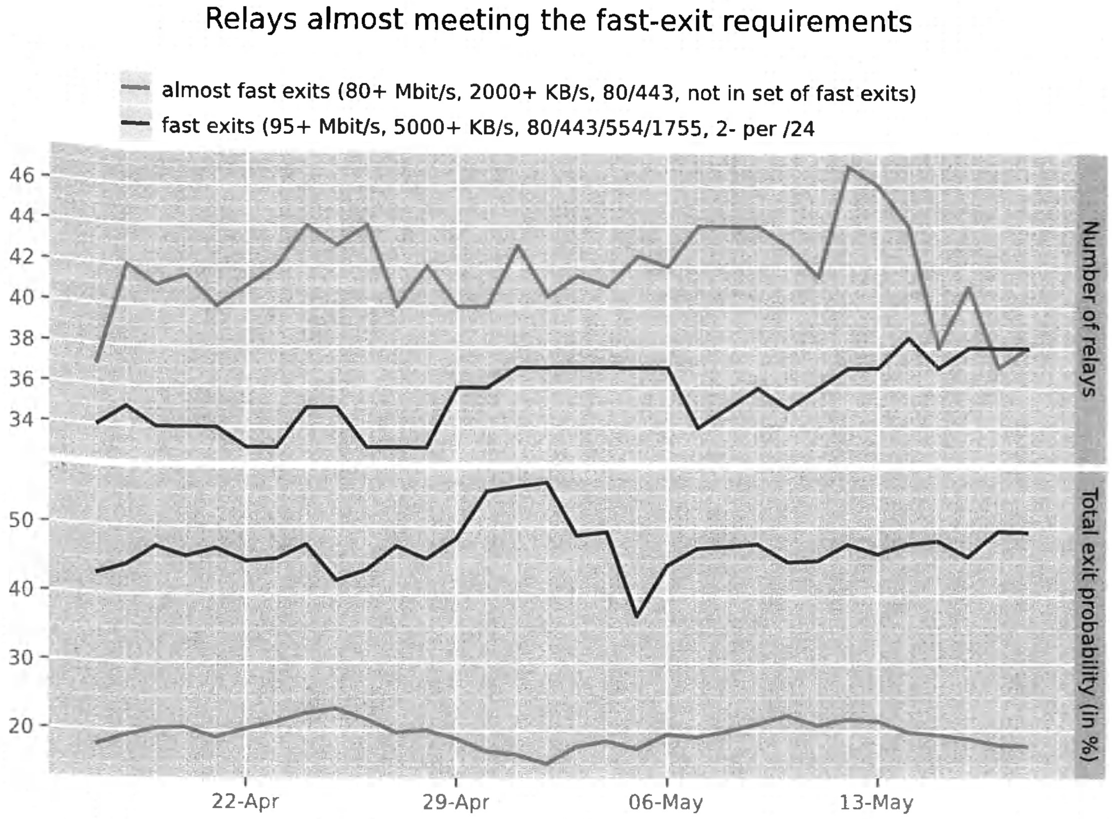


1.2 March 2013

We're at 35 qualifying fast exists providing 19.9959% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 47 qualifying fast exits providing 30.3162% of the bandwidth if we ignore the /24 diversity requirement.

Figure 2: Relays almost meeting the fast-exit requirements



1.3 February 2013

We're at 37 qualifying fast exists providing 19.6565% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 50 qualifying fast exits providing 24.7406% of the bandwidth if we ignore the /24 diversity requirement.

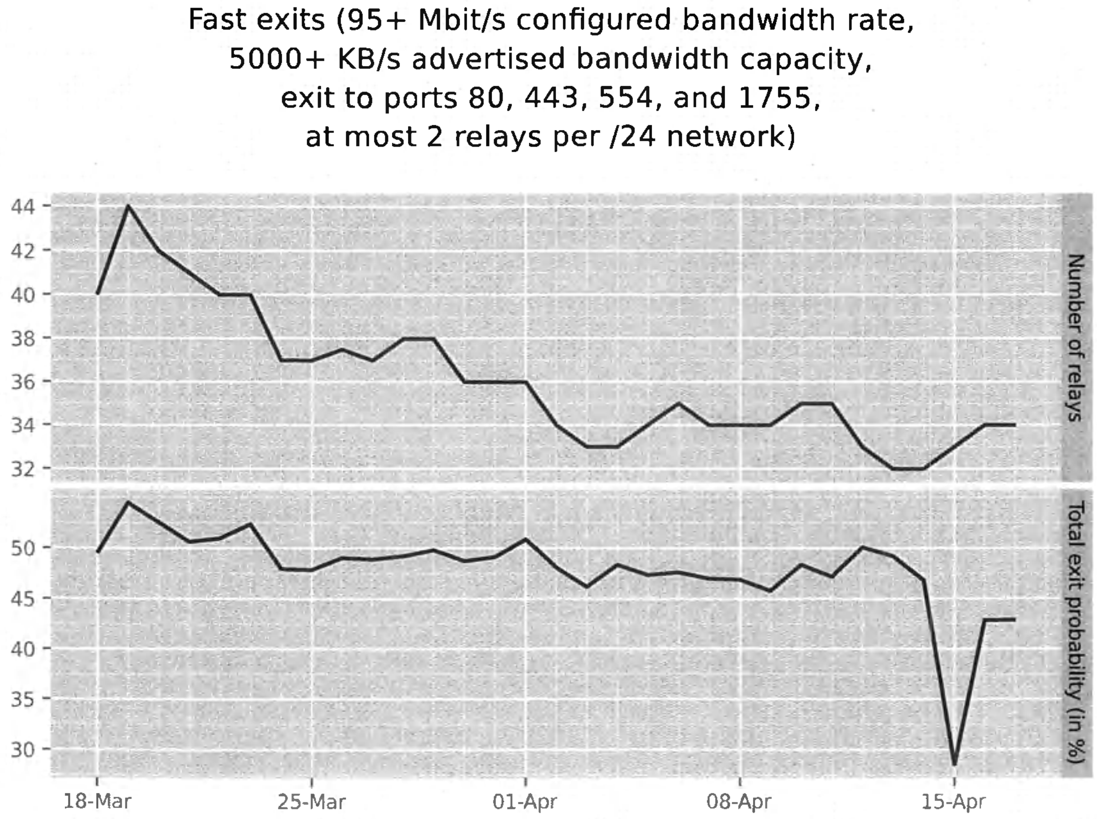
1.4 January 2013

We signed a Memorandum of Understanding with the Wau Holland Stiftung organization in Germany to reimburse exit relays located in the European Union.

We're at 34 qualifying fast exists providing 20.5026% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 47 qualifying fast exits providing 28.2256% of the bandwidth if we ignore the /24 diversity requirement.

Figure 3: Relays meeting the fast-exit requirements



1.5 December 2012

We've hired a dedicated relay community manager. Moritz Bartl of Torservers.net is now responsible for maintaining relationships with relay operators, finding new ISPs for hosting exit relays, and growing the Tor network.

We're at 42 qualifying fast exists providing 34.88% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

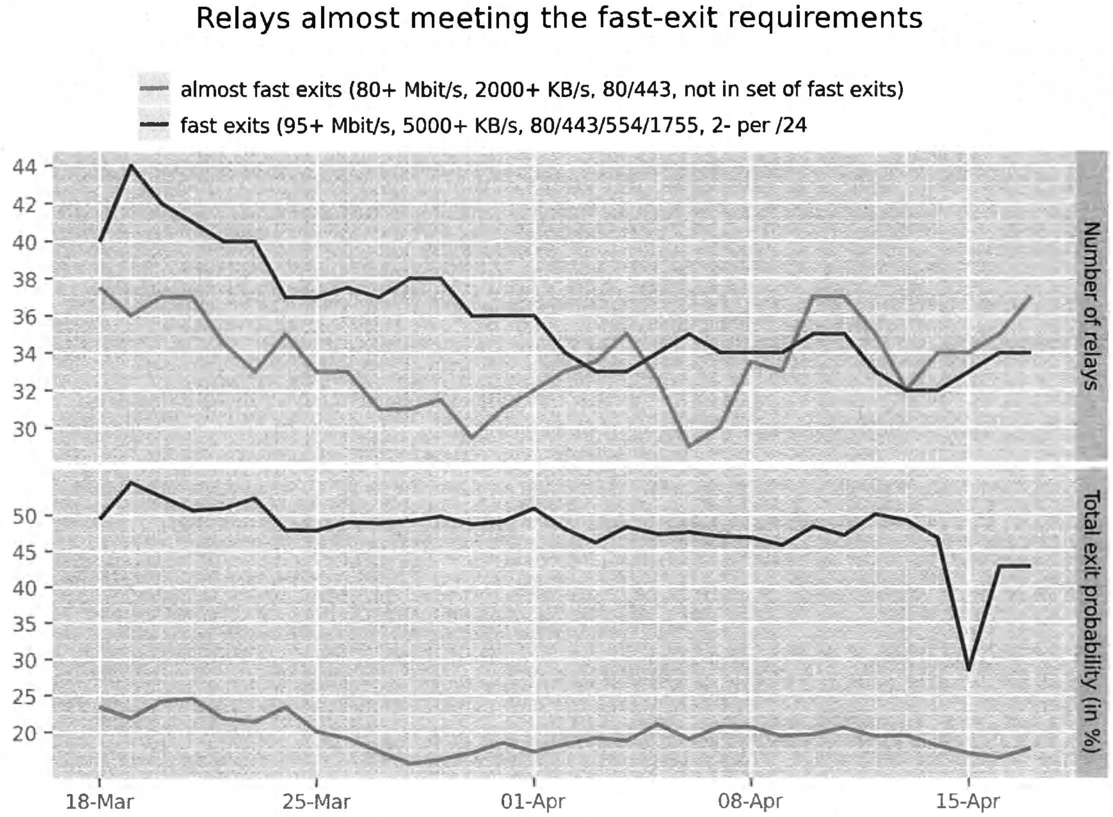
We're at 54 qualifying fast exits providing 44.4391% of the bandwidth if we ignore the /24 diversity requirement.

1.6 November 2012

We're at 38 qualifying fast exits providing 33.6749% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 51 qualifying fast exits providing 44.3442% of the bandwidth if we ignore the /24

Figure 4: Relays almost meeting the fast-exit requirements



diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

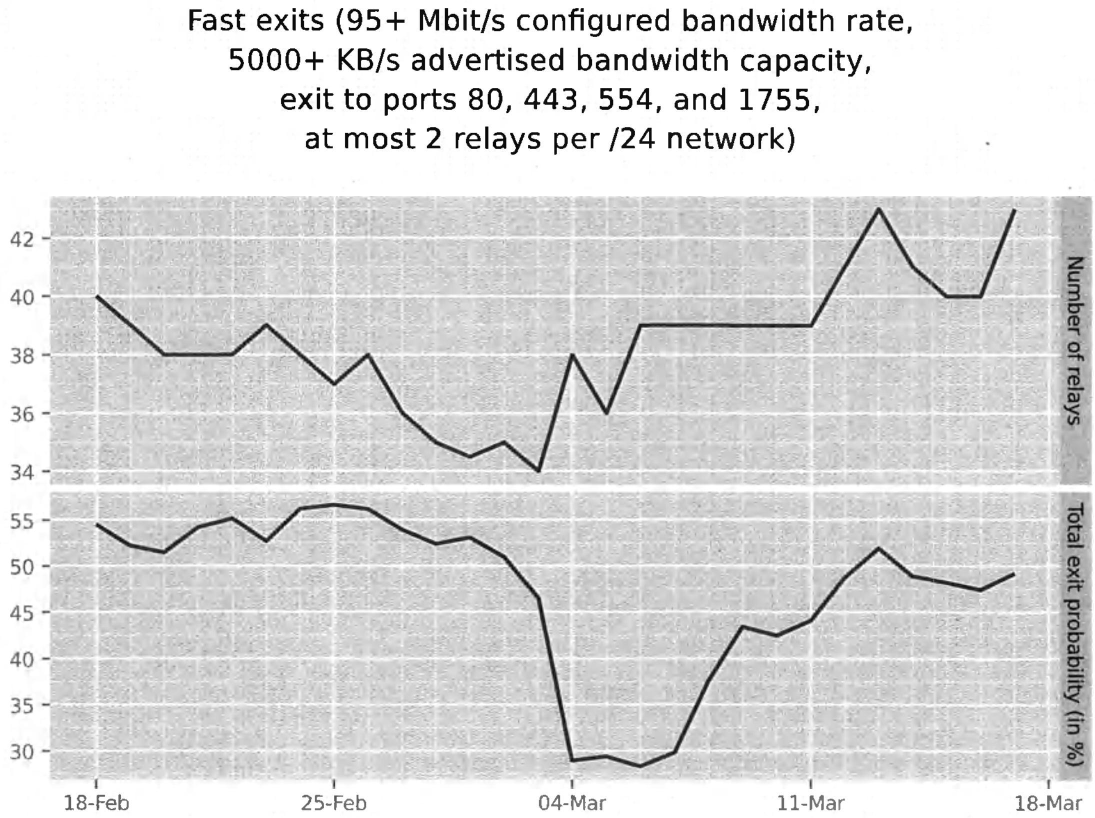
1.7 October 2012

We're up to 41 qualifying fast exits providing 22.9375% of the bandwidth in the Tor Network. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 57 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 49.3678% of the exit bandwidth available in the Tor network.

Discussions with lawyers continue. These discussions are blocking further progress on contracts and announcements of exit relay organizations.

Figure 5: Relays meeting the fast-exit requirements



1.8 September 2012

1.8.1 Exit Relays

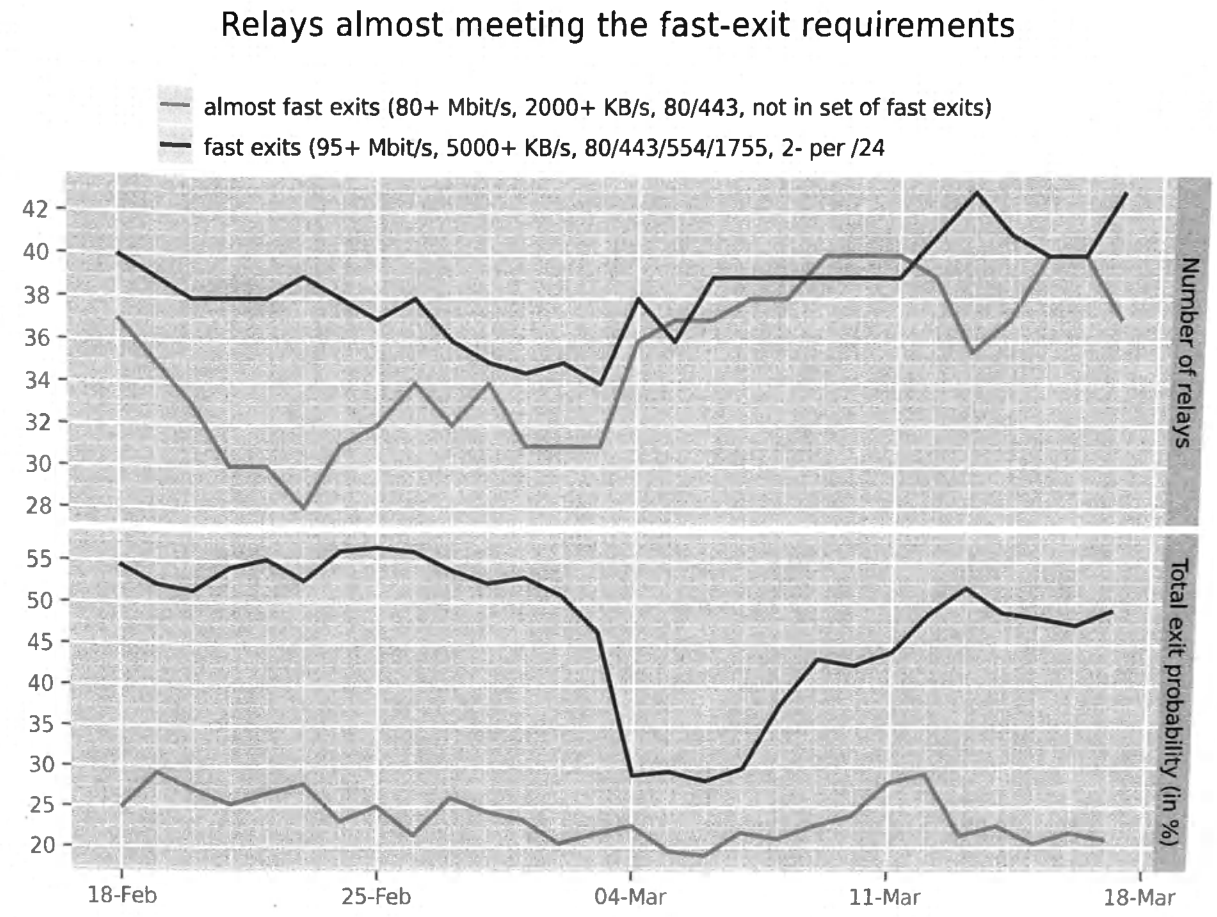
We're holding at 28 qualifying fast exits providing 16.667% of the bandwidth. These relays cover the US, Canada, and EU. We're working on finding partners in Africa and Asia for diversity.

We're at 37 qualifying fast exits providing 31.4027% of the bandwidth if we ignore the /24 diversity requirement. These exits cover 57% of the exit probability.

We are in negotiations with three organizations running a majority of the exit relay capacity. These three orgs will be publicly announced when contracts are signed.

We are in final discussions about the Tor network and legal aspects of running a funded relay under US laws. The main concern here is not falling under the definition of Internet Service Provider or telecommunications carrier which would subject Tor to CALEA compliance regulations.

Figure 6: Relays almost meeting the fast-exit requirements



1.9 August 2012

1.9.1 Exit Relays

We're working through the legal issues raised by our lawyers at the last step before full on exit relay reimbursements begin. The promise of funding, and raised profile has increased the exit count organically.

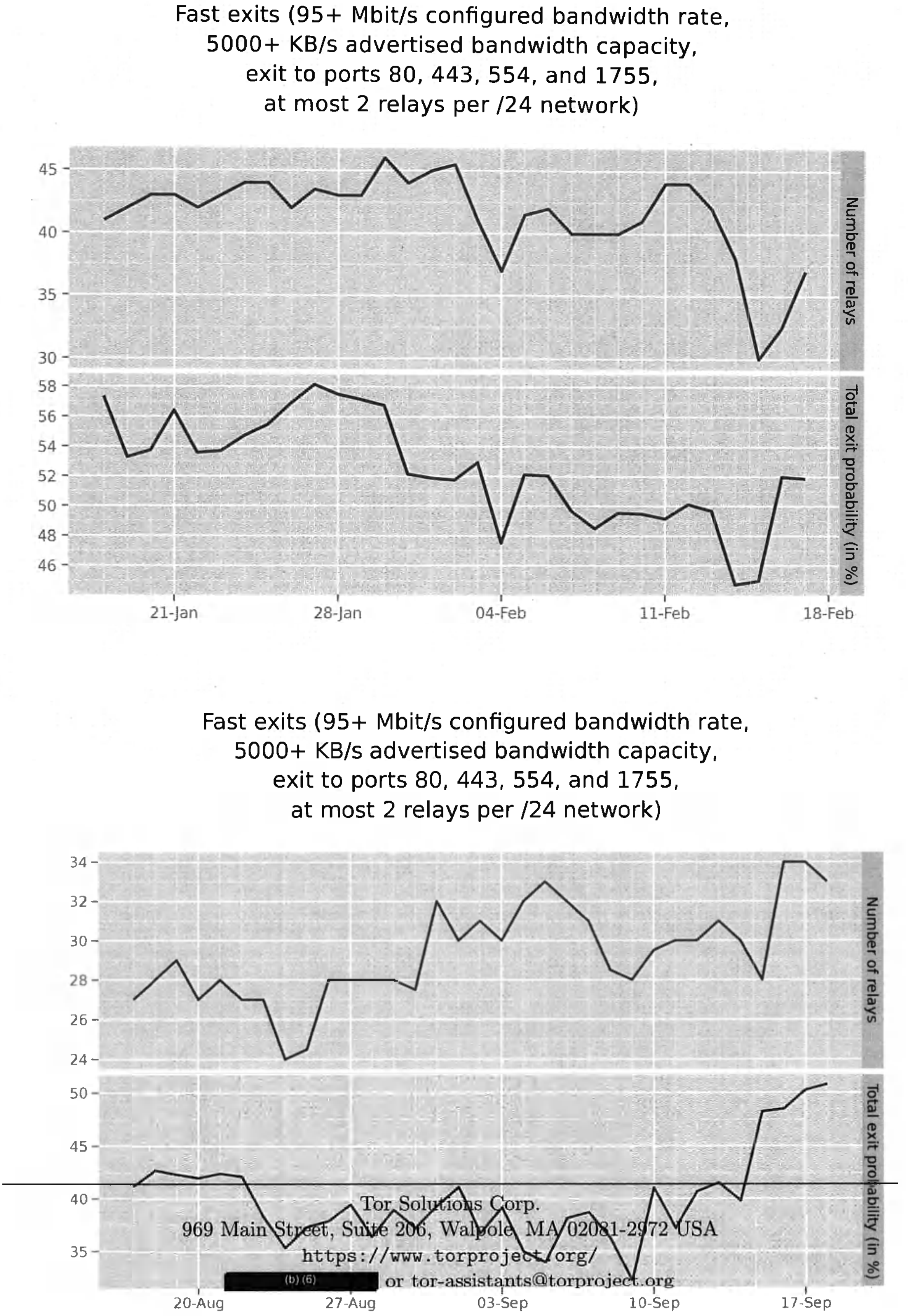
We're up to 34 qualifying fast exits: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only&top=-1` and the number is 55 if we ignore /24 diversity requirements: `https://compass.torproject.org/?family=&ases=&country=&exits=fast_exits_only_any_network&top=-1`

Then there are a further 32 that "almost" qualify, for example because they don't have the two extra ports in their exit policy, or their bandwidth is a bit under 100mbit.

Looked at it another way, these 34 exits are roughly 50% of the exit probabilities. The whole set of 87 relays I talk about above are nearly 80% of the exit probabilities.

Check out the "group by AS" and "group by country" options, as the beginning of our explorations into other diversity metrics.

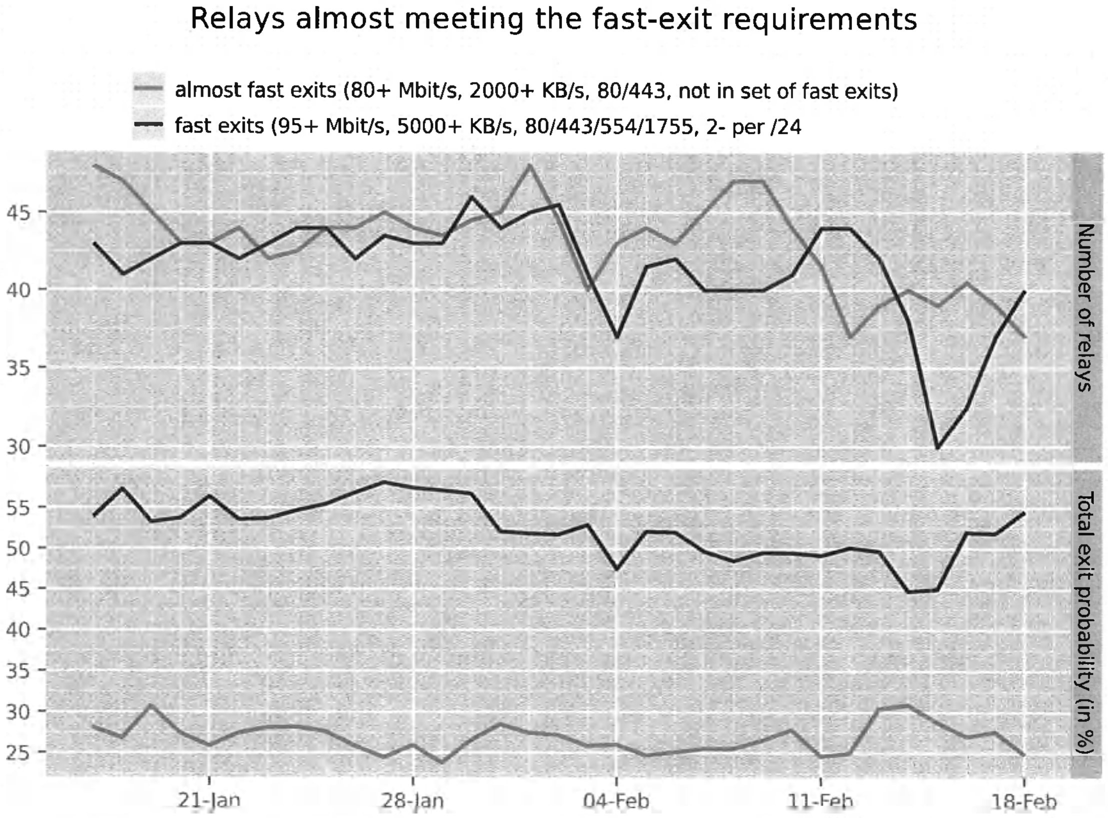
Figure 7: Relays meeting the fast-exit requirements



Fast exits (95+ Mbit/s configured bandwidth rate, 5000+ KB/s advertised bandwidth capacity, exit to ports 80, 443, 554, and 1755, at most 2 relays per /24 network)

Fast exits (95+ Mbit/s configured bandwidth rate, 5000+ KB/s advertised bandwidth capacity, exit to ports 80, 443, 554, and 1755, at most 2 relays per /24 network)

Figure 8: Relays almost meeting the fast-exit requirements



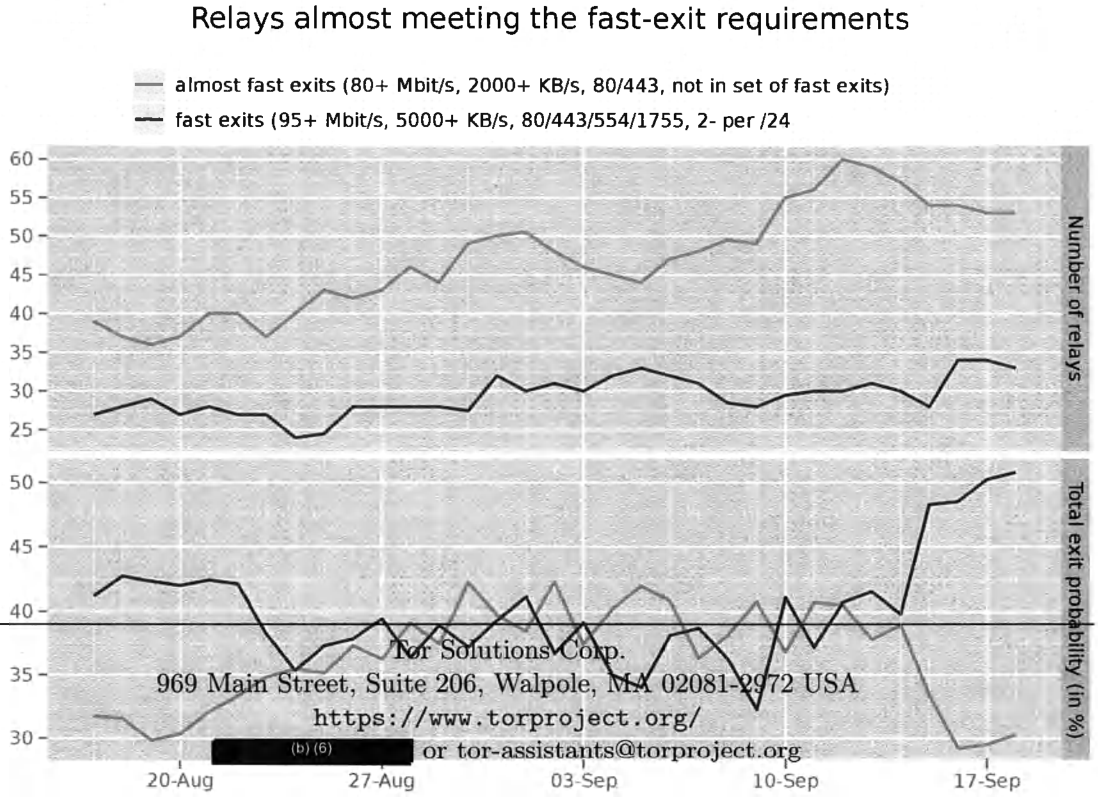
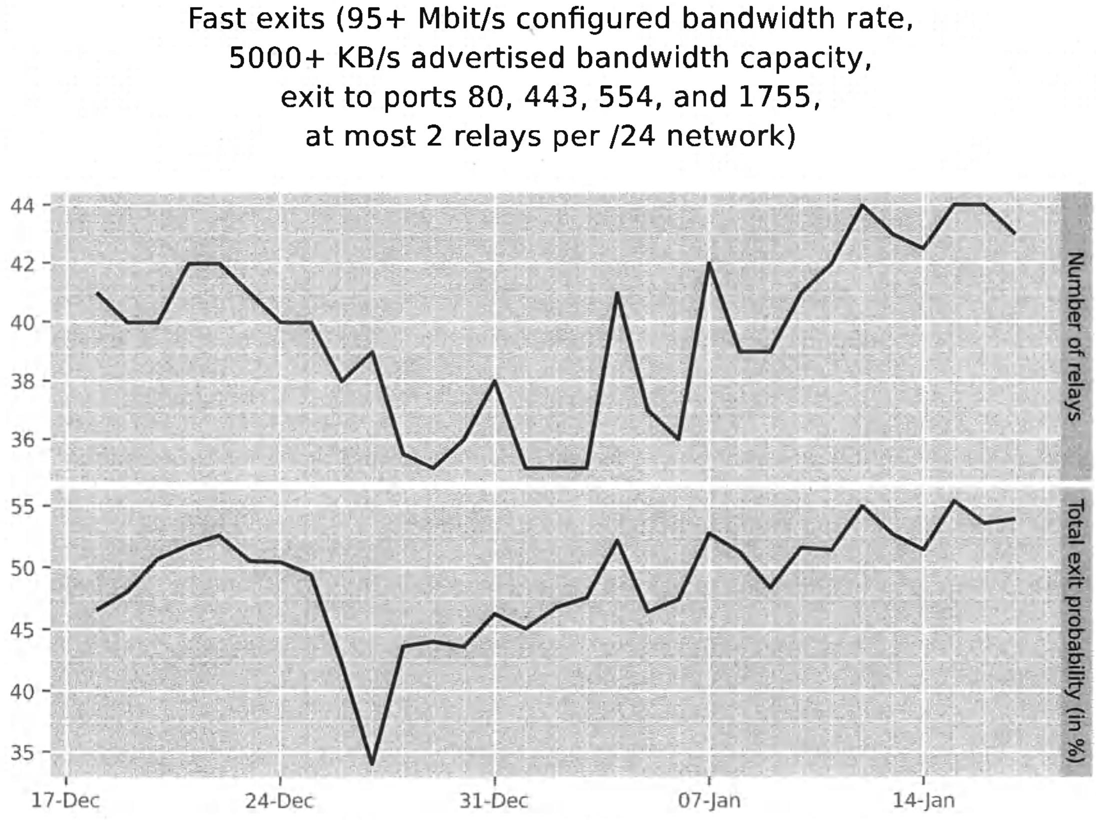


Figure 9: Relays meeting the fast-exit requirements



Karsten added `https://metrics.torproject.org/network.html#bandwidth-flags` for easier tracking of exit bandwidth capacity and history.

Advertised exit bandwidth is up 1700/1000 = 70% since start-of-project, and actual used bandwidth by exits is up 1000/625 = 60%: `https://metrics.torproject.org/network.html?graph=bandwidth-flags&start=2012-06-17&end=2012-09-17#bandwidth-flags`.

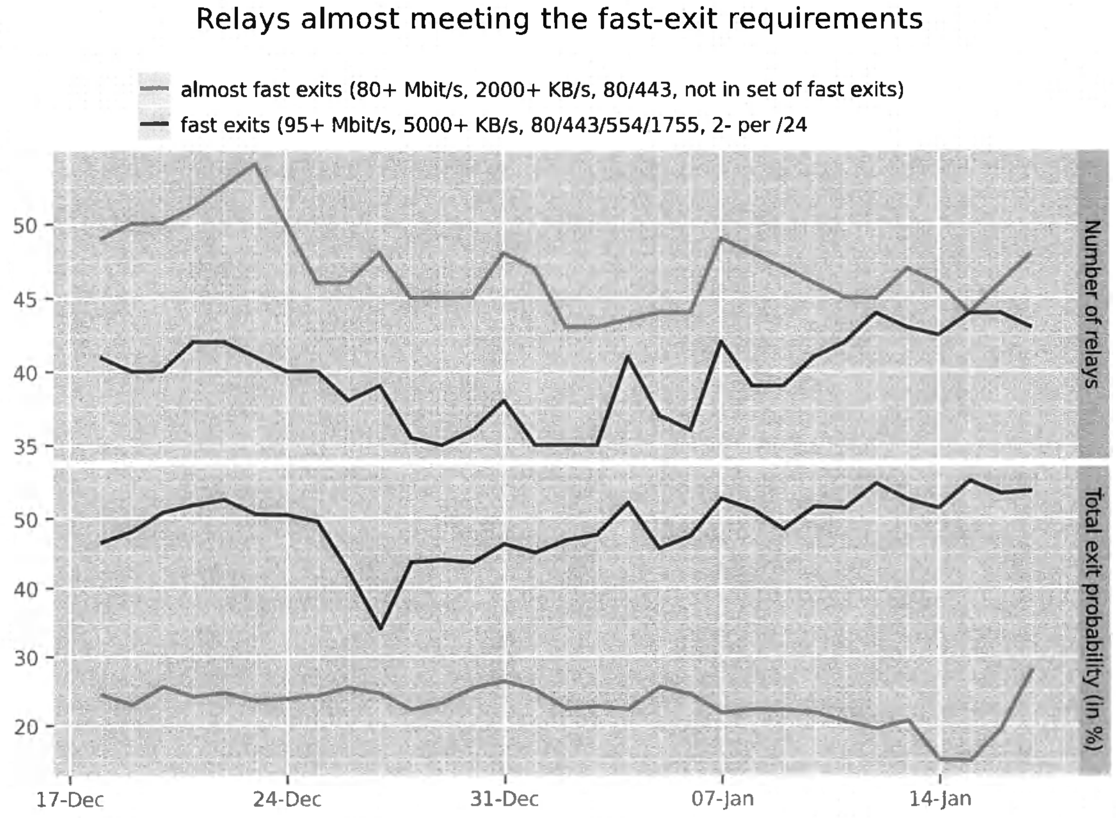
1.9.2 Bridge distribution

The custom BBG-only email responder is up and operational. We've had three requests since we set up the "count how many requests we get" metrics. We're guessing that means you haven't given the address out to a wide audience yet.

We've also realized that since these bridges don't publish to bridgedb, we don't get any usage stats from them. We've opened https://trac.torproject.org/projects/tor/ticket/6852 so by the time they start seeing more use, we should be ready to get usage stats from them manually.

It gives out only one bridge address for now, but that bridge should be stable and fast enough to handle basically whatever you throw at it. (Or at least, by the time it has enough users to fill it up, one of them is probably working for gfw.)

Figure 10: Relays almost meeting the fast-exit requirements



We've set up our new "bridgeguard" tool on this bridge: `https://gitweb.torproject.org/brdgrd.git/blob/HEAD:/README.md`

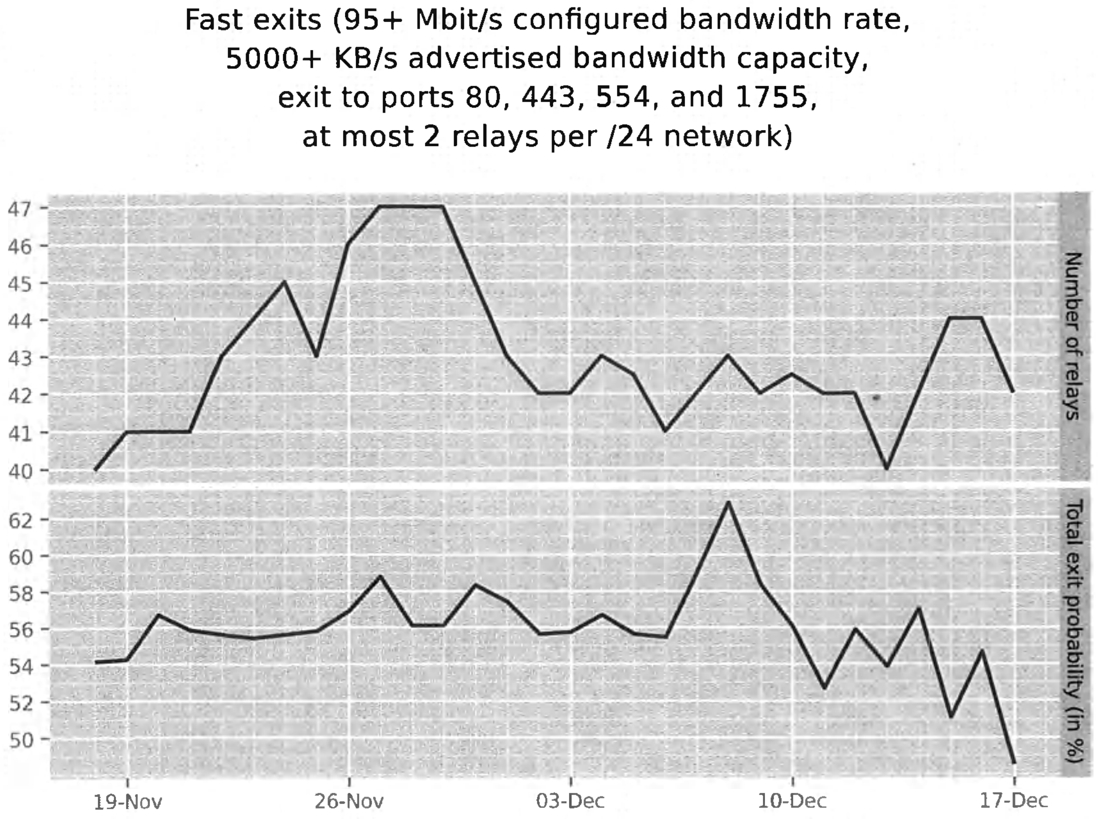
Bridgeguard is a bridge-side hack to manipulate the TCP window so clients will split their SSL client hello over multiple TCP packets – thus gfw won't notice the cipher list that the client offers, and even Tor 0.2.2 clients won't trigger a probe (and thus a block).

Remember that once a bad person learns about the email address, they can discover the bridge address and block it. When that happens (and potentially quite a bit later, when we notice and can confirm that it happened), we expect we'll change the text to explain that if you want a *working* bridge, you'll have to go back to wherever you found this email address and ask for a new one. Then we'll set up a second email alias with a new bridge address, and repeat.

To that end, we've avoided lining up all 75 bridge addresses quite yet – it would be a waste to set them up and not use them yet. We have our next few 100mbit private bridges up and running (and they're configuring Bridgeguard now), but hopefully we won't need to use them for a while.

In the future we might set up Obfsproxy bridges instead, now that we have the Tor Obfsproxy Browser Bundle building nicely again:
`https://blog.torproject.org/blog/new-tor-browser-and-obfsproxy-bundles` Lots of options

Figure 11: Relays meeting the fast-exit requirements

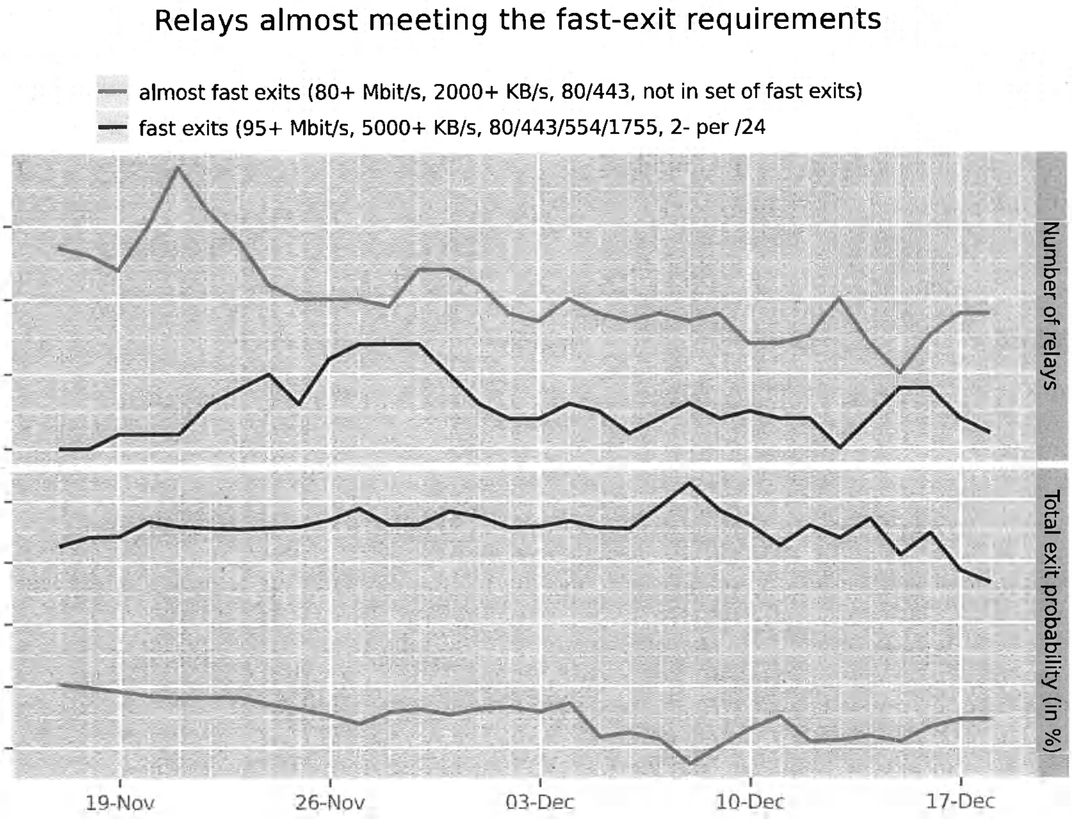


as we go forward.

1.10 July 2012

The 'fast exit count' graphs are now updated daily at `https://metrics.torproject.org/fast-exits.html` We're up to 28 or so.

Figure 12: Relays almost meeting the fast-exit requirements



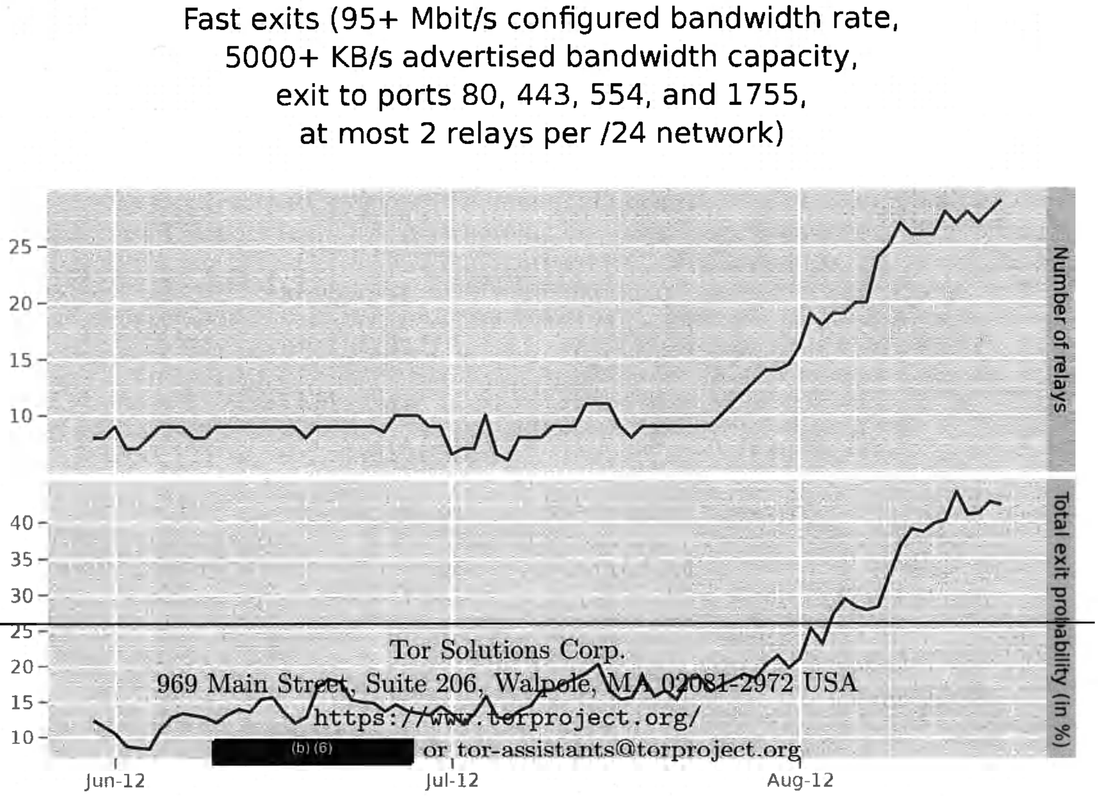
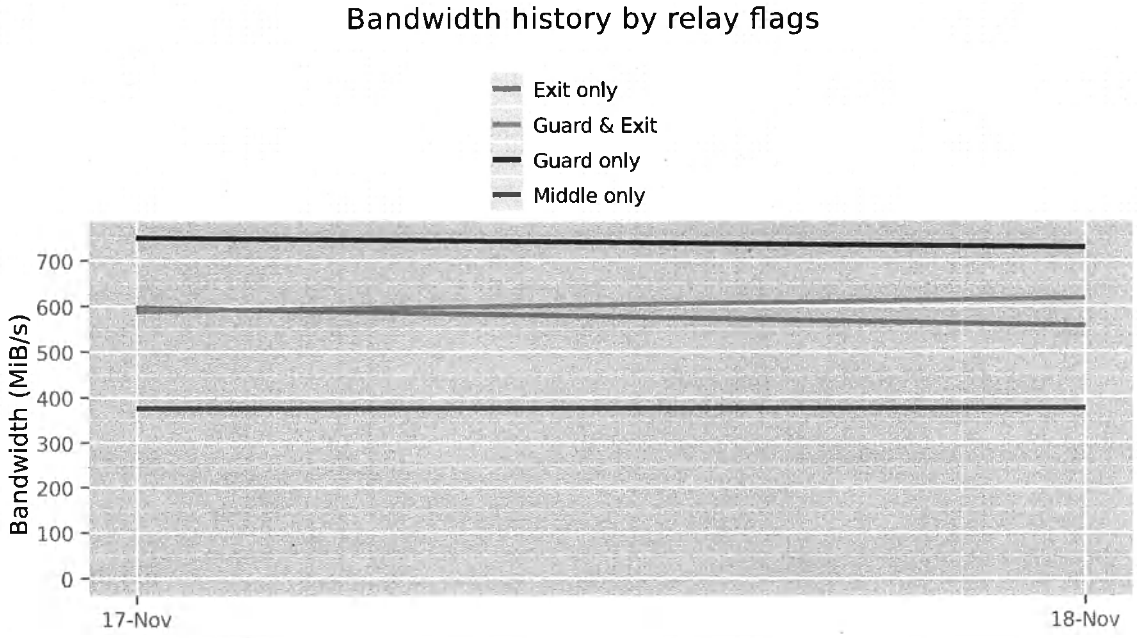


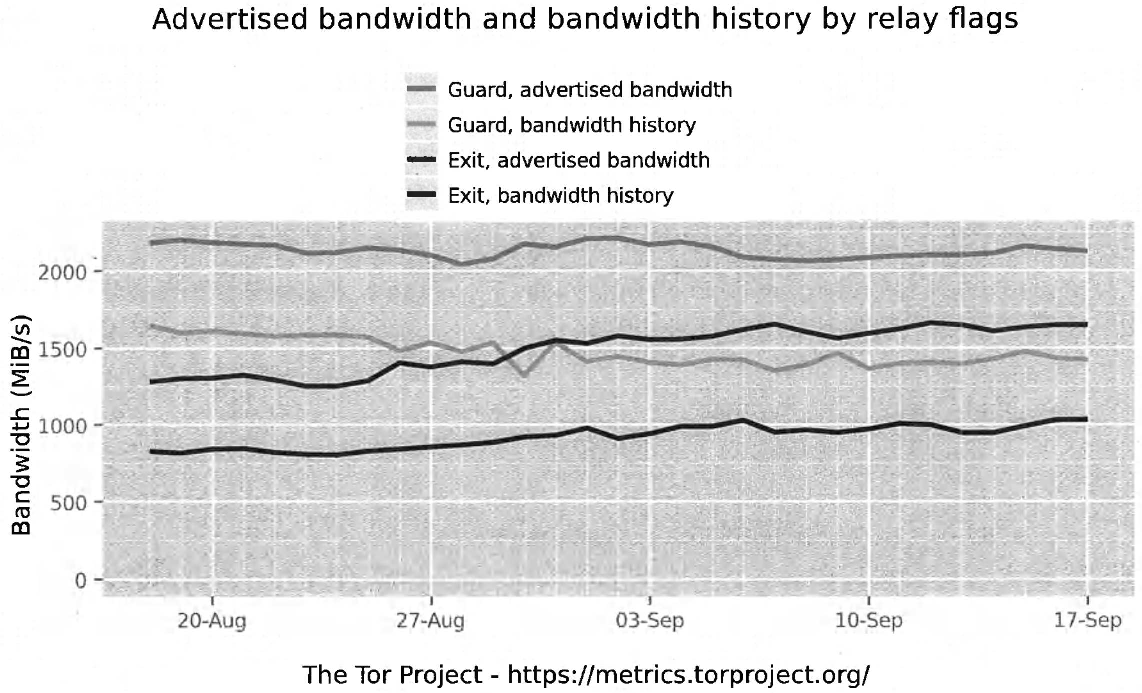
Figure 13: Relay bandwidth by Exit and/or Guard flags



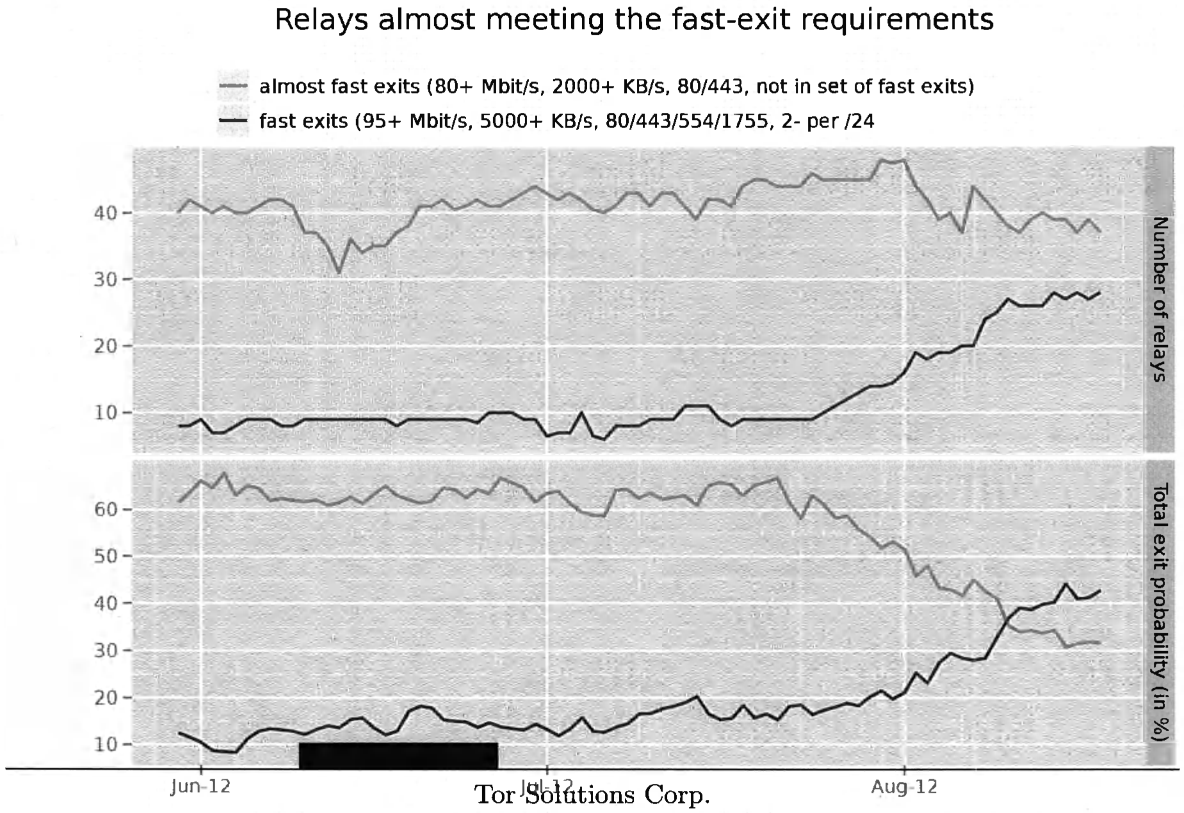
The Tor Project - https://metrics.torproject.org/

If we squint and allow more than 2 relays on a given /24 (since many of our current fast relays are actually 4-6 relays trying to fill a 1 gbps link), we're at 39 (and these 39 are 50-55% of our exit weights currently).

Figure 14: Relay bandwidth by Exit and/or Guard flags


Advertised bandwidth and bandwidth history by relay flags

The Tor Project - https://metrics.torproject.org/


Relays almost meeting the fast-exit requirements

[redacted]

Sathya has started working on automating the tracking and diversity measurements of fast exits at https://compass.torproject.org/.

And we're working on figuring out what diversity measurements are actually meaningful at ticket 6460.

We're in the process of funding Moritz Bartl, the torservers.net guy, to fill our new Tor Relay Coordinator position. His responsibilities will include 1) keep current relay operators happy; 2) find new relay operators, and new good hosting locations, so we grow our relay population, especially fast exit relays; and 3) make sure our statistics and metrics work provides good feedback to both our relay operators and our funders.

We've started talking to Wau Holland Foundation in Germany about having them be our European distributor-of-funds-to-exit-relay-operators, since many Europeans want to receive their money via European bank transfer rather than check. We're also moving forward at deciding how best to structure our (legal and contractual) relationship with the exit relay operators.

I've launched a campaign to get more US university-based fast exits – I have buy-in for 500mbit+ nodes at UPenn, UMich, CMU, and Georgia Tech: https://lists.torproject.org/pipermail/tor-relays/2012-August/001543.html with several more research groups looking into it too.

So that's the good news: if we squint enough, we're on track to meet our "30% of the exits running by the 60 day mark" goal, and we have more fast exits in the works.

The bad news is we probably can't (and probably shouldn't) keep up this pace of growth. We've added about 10% to the capacity of the network over the past two months, and added about 20% to the actual load handled by exits. Also, as I explained on the phone a few weeks back, we want to leave space to discover and fund great new hosting situations over the course of the year. And finally, at this growth pace we've started to see hints of the "second-order effects" I speculated about in my response to the original RFQ, where high-capacity relays draw traffic away from the current relays, and our algorithms for maximizing performance shift load so much that 10mbit-and-under relays see less use and we risk having them drop out. We must grow the available capacity in concert with increased network load.

1.11 June 2012

Started to develop a plan for implementation which includes how to distribute the funding, how to involve the community, and how to track the funded relays.

2 C.2.5, C.2.6

2.1 April 2013

We released updated Tor Browser alpha packages.

```
This release also includes a patch to enable optimistic data which should significantly speed ı

You can download the alpha Tor Browser Bundles here.

Tor Browser Bundle (2.4.12-alpha-1)

    Update Tor to 0.2.4.12-alpha
    Update Torbutton to 1.5.2
    Update libpng to 1.5.15
    Update NoScript to 2.6.6
    Update PDF.js to 0.8.1
    Firefox patch changes:
        Apply font limits to @font-face local() fonts and disable fallback
        rendering for @font-face. (closes: #8455)
        Use Optimistic Data SOCKS handshake (improves page load performance).
        (closes: #3875)
        Honor the Windows theme for inverse text colors (without leaking those
        colors to content). (closes: #7920)
        Increase pipeline randomization and try harder to batch pipelined
        requests together. (closes: #8470)
        Fix an image cache isolation domain key misusage. May fix several image
        cache related crash bugs with New Identity, exit, and certain websites.
        (closes: #8628)
    Torbutton changes:
        Allow session restore if the user allows disk actvity (closes: #8457)
        Remove the Display Settings panel and associated locales (closes: #8301)
        Fix "Transparent Torification" option. (closes: #6566)
        Fix a hang on New Identity. (closes: #8642)
    Build changes:
        Fetch our source deps from an https mirror (closes: #8286)
        Create watch scripts for syncing mirror sources and monitoring mirror
        integrity (closes: #8338)
```

We released updated Tor Browser stable packages.

```
Tor Browser Bundle (2.3.25-8)

    Update Firefox to 17.0.6esr
    Update HTTPS Everywhere to 3.2
    Update Torbutton to 1.5.2
    Update libpng to 1.5.15
    Update NoScript to 2.6.6.1
    Firefox patch changes:
        Apply font limits to @font-face local() fonts and disable fallback
        rendering for @font-face. (closes: #8455)
        Use Optimistic Data SOCKS handshake (improves page load performance).
        (closes: #3875)
        Honor the Windows theme for inverse text colors (without leaking those
        colors to content). (closes: #7920)
        Increase pipeline randomization and try harder to batch pipelined
        requests together. (closes: #8470)
        Fix an image cache isolation domain key misusage. May fix several image
        cache related crash bugs with New Identity, exit, and certain websites.
        (closes: #8628)
    Torbutton changes:
        Allow session restore if the user allows disk actvity (closes: #8457)
        Remove the Display Settings panel and associated locales (closes: #8301)
        Fix "Transparent Torification" option. (closes: #6566)
        Fix a hang on New Identity. (closes: #8642)
    Build changes:
        Fetch our source deps from an https mirror (closes: #8286)
        Create watch scripts for syncing mirror sources and monitoring mirror
        integrity (closes: #8338)

    Tor Browser Bundle (2.4.12-alpha-2)
        Update Firefox to 17.0.6esr
        Update NoScript to 2.6.6.1
```

2.2 March 2013

We released updated TorBrowser with a new version of Firefox with updates:

```
Tor Browser Bundle (2.3.25-6)

    Update Firefox to 17.0.5esr
    Update NoScript to 2.6.59

Tor Browser Bundle (2.4.11-alpha-2)

    Update Firefox to 17.0.5esr
    Update NoScript to 2.6.59
```

2.3 February 2013

- We released updated TorBrowser with a new version of Firefox and many, many updates:

```
We've updated all of the bundles with Firefox 17.0.3esr. This includes
significant changes to Torbutton and its interaction with Firefox,
in addition to many new patches being added to Firefox, which are
outlined below.

Very important: if you've been using the Tor Browser Bundles with Firefox
10.0.x, you must not attempt to overwrite it with the new bundle. Open
these into their own directory and do not copy any profile material from
older TBB versions.

Tor Browser Bundle (2.3.25-4)
```

```
    Update Firefox to 17.0.3esr
    Downgrade OpenSSL to 1.0.0k
    Update libpng to 1.5.14
    Update NoScript to 2.6.5.7
    Firefox patch changes:
        Exempt remote @font-face fonts from font limits (and prefer them).
        (closes: #8270)
            Remote fonts (aka "User Fonts") are not a fingerprinting threat, so
            they should not count towards our CSS font count limits. Moreover,
            if a CSS font-family rule lists any remote fonts, those fonts are
            preferred over the local fonts, so we do not reduce the font count
            for that rule.
            This vastly improves rendering and typography for many websites.
        Disable WebRTC in Firefox build options. (closes: #8178)
            WebRTC isn't slated to be enabled until Firefox 18, but the code
            was getting compiled in already and is capable of creating UDP Sockets
            and bypassing Tor. We disable it from build as a safety measure.
        Move prefs.js into omni.ja and extension-overrides. (closes: #3944)
            This causes our browser pref changes to appear as defaults. It also
            means that future updates of TBB should preserve user pref settings.
        Fix a use-after-free that caused crashing on MacOS (closes: #8234)
        Eliminate several redundant, useless, and deprecated Firefox pref settings
        Report Firefox 17.0 as the Tor Browser user agent
        Use Firefox's click-to-play barrier for plugins instead of NoScript
        Set the Tor SOCKS+Control ports to 9150, 9151 respectively on all platforms
            This fixes a SOCKS race condition with our SOCKS autoport configuration
            and HTTPS-Everywhere's Tor test. Firefox 17 appears to cache proxy
            settings per URL now, which resulted in a proxy error for
            check.torproject.org if we lost the race.
    Torbutton was updated to 1.5.0. The following issues were fixed:
        Remove old toggle observers and related code (closes: #5279)
        Simplify Security Preference UI and associated pref updates (closes: #3100)
        Eliminate redundancy in our Flash/plugin disabling code (closes: #1305)
        Leave most preferences under Tor Browser's control (closes: #3944)
        Disable toggle-on-startup and crash detection logic (closes: #7974)
        Disable/remove toggle-mode code and related observers (closes: #5279)
        Add menu hint to Torbutton icon (closes: #6431)
        Make Torbutton icon flash a warning symbol if TBB is out of date (closes: #7495)
        Perform version check every time there's a new tab. (closes: #6096)
        Rate limit version check queries to once every 1.5hrs max. (closes: #6156)
        misc: Allow WebGL and DOM storage.
        misc: Disable independent Torbutton updates
        misc: Change the recommended SOCKSPort to 9150 (to match TBB)

The following Firefox patch changes are also included in this release:
    Isolate image cache to url bar domain (closes: #5742 and #6539)
    Enable DOM storage and isolate it to url bar domain (closes: #6564)
    Include nsIHttpChannel.redirectTo API for HTTPS-Everywhere (closes: #5477)
    Misc preference changes:
        Disable DOM performance timers (dom.enable_performance) (closes: #6204)
        Disable HTTP connection retry timeout (network.http.connection-retry-timeout) (cl
        Disable full path information for plugins (plugin.expose_full_path) (closes: #621
        Disable NoScript's block of remote WebFonts (noscript.forbidFonts) (closes: #7937

Tor Browser Bundle (2.4.10-alpha-2)

    Update Firefox to 17.0.3esr
    Downgrade OpenSSL to 1.0.0k
    Update libpng to 1.5.14
    Update NoScript to 2.6.5.7
    Firefox patch changes:
        Exempt remote @font-face fonts from font limits (and prefer them).
        (closes: #8270)
            Remote fonts (aka "User Fonts") are not a fingerprinting threat, so
            they should not count towards our CSS font count limits. Moreover,
            if a CSS font-family rule lists any remote fonts, those fonts are
            preferred over the local fonts, so we do not reduce the font count
            for that rule.
            This vastly improves rendering and typography for many websites.
        Disable WebRTC in Firefox build options. (closes: #8178)
            WebRTC isn't slated to be enabled until Firefox 18, but the code
            was getting compiled in already and is capable of creating UDP Sockets
            and bypassing Tor. We disable it from build as a safety measure.
        Move prefs.js into omni.ja and extension-overrides. (closes: #3944)
            This causes our browser pref changes to appear as defaults. It also
            means that future updates of TBB should preserve user pref settings.
        Fix a use-after-free that caused crashing on MacOS (closes: #8234)
        Eliminate several redundant, useless, and deprecated Firefox pref settings
        Report Firefox 17.0 as the Tor Browser user agent
        Use Firefox's click-to-play barrier for plugins instead of NoScript
        Set the Tor SOCKS+Control ports to 9150, 9151 respectively on all platforms
            This fixes a SOCKS race condition with our SOCKS autoport configuration
            and HTTPS-Everywhere's Tor test. Firefox 17 appears to cache proxy
            settings per URL now, which resulted in a proxy error for
            check.torproject.org if we lost the race.
    Torbutton was updated to 1.5.0. The following issues were fixed:
        Remove old toggle observers and related code (closes: #5279)
        Simplify Security Preference UI and associated pref updates (closes: #3100)
        Eliminate redundancy in our Flash/plugin disabling code (closes: #1305)
        Leave most preferences under Tor Browser's control (closes: #3944)
        Disable toggle-on-startup and crash detection logic (closes: #7974)
        Disable/remove toggle-mode code and related observers (closes: #5279)
        Add menu hint to Torbutton icon (closes: #6431)
        Make Torbutton icon flash a warning symbol if TBB is out of date (closes: #7495)
        Perform version check every time there's a new tab. (closes: #6096)
        Rate limit version check queries to once every 1.5hrs max. (closes: #6156)
        misc: Allow WebGL and DOM storage.
        misc: Disable independent Torbutton updates
        misc: Change the recommended SOCKSPort to 9150 (to match TBB)
```

- We published a talk about flash proxy.
- We released updated Tor Browser bundles with new firefox and another huge set of patches:

```
We've updated the stable and alpha Tor Browser Bundles with Firefox
17.0.4esr and Tor 0.2.4.11-alpha. These releases have numerous bug fixes
and a new Torbutton as well.

Tor Browser Bundle (2.3.25-5)

    Update Firefox to 17.0.4esr
    Update NoScript to 2.6.5.8
    Update HTTPS Everywhere to 3.1.4
    Fix non-English language bundles to have the correct branding (closes: #8302)
    Firefox patch changes:
        Remove "This plugin is disabled" barrier
            This improves the user experience for HTML5 Youtube videos:
            They "silently" attempt to load flash first, which was not so silent
            with this barrier in place. (closes: #8312)
        Disable NoScript's HTML5 media click-to-play barrier (closes: #8386)
        Fix a New Identity hang and/or crash condition (closes: #6386)
        Fix crash with Drag + Drop on Windows (closes: #8324)
    Torbutton changes:
        Fix Drag+Drop crash by using a new TBB drag observer (closes: #8324)
        Fix XML/E4X errors with Cookie Protections (closes: #6202)
        Don't clear cookies at shutdown if user wants disk history (closes: #8423)
        Leave IndexedDB and Offline Storage disabled. (closes: #8382)
        Clear DOM localStorage on New Identity. (closes: #8422)
        Don't strip "third party" HTTP auth from favicons (closes: #8335)
        Localize the "Spoof english" button strings (closes: #5183)
        Ask user for confirmation before enabling plugins (closes: #8313)
        Emit private browsing session clearing event on "New Identity"

Tor Browser Bundle (2.4.11-alpha-1)
```

```
Update Firefox to 17.0.4esr
Update Tor to 0.2.4.11-alpha
Update NoScript to 2.6.5.8
Update HTTPS Everywhere to 4.0development.6
Update PDF.js to 0.7.236
Fix non-English language bundles to have the correct branding (closes: #8302)
Firefox patch changes:
    Remove "This plugin is disabled" barrier
        This improves the user experience for HTML5 Youtube videos:
        They "silently" attempt to load flash first, which was not so silent
        with this barrier in place. (closes: #8312)
    Disable NoScript's HTML5 media click-to-play barrier (closes: #8386)
    Fix a New Identity hang and/or crash condition (closes: #6386)
    Fix crash with Drag + Drop on Windows (closes: #8324)
Torbutton changes:
    Fix Drag+Drop crash by using a new TBB drag observer (closes: #8324)
    Fix XML/E4X errors with Cookie Protections (closes: #6202)
    Don't clear cookies at shutdown if user wants disk history (closes: #8423)
    Leave IndexedDB and Offline Storage disabled. (closes: #8382)
    Clear DOM localStorage on New Identity. (closes: #8422)
    Don't strip "third party" HTTP auth from favicons (closes: #8335)
    Localize the "Spoof english" button strings (closes: #5183)
    Ask user for confirmation before enabling plugins (closes: #8313)
    Emit private browsing session clearing event on "New Identity"
```

2.4 January 2013

- We released new Tor Browser Bundles highlighting updates to Firefox 17.03 ESR. We also released updated -alpha Tor Browser Bundle testing bundles. These testing bundles include Tor 0.2.4.10-alpha.

- We released and then reverted new Tor Browser Bundles which contained an unsafe version of OpenSSL.

2.5 December 2012

- We released updated Tor Browser Bundles to fix a certificate authority problem with Turk-Trust and to update the testing branch of Tor Browser with Tor 0.2.4.7-alpha.

- We've contracted two additional Firefox/TorBrowser developers to help address the backlog of bug fixes and enhancements. The current list of Tor Browser tickets is always available.

  We've recently closed the following tickets:

  - Ticket 6096 Perform TBB version check async on new tab
  - Ticket 6156 Rate limit of check.tpo
  - Ticket 6431 Torbutton should have a downward arrow menu

```
/var/log/daemon.log, /var/log/syslog, /var/log/kern.log,
/var/log/messages: contains information about attached devices. I had an
external drive attached to the virtual machine, so these files contain
lines such as \Mounted /dev/sdb1 (Read-Write, label \THA", NTFS
3.1)" and \Initializing USB Mass Storage driver...".
```

3.3 February 2013

No progress to report.

3.4 January 2013

We have a contractor who has started to work on this project. We're tracking progress on this deliverable with tickets 6845, 6846, 7032, 7033, and 8166.

3.5 November 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.6 October 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.7 September 2012

No progress to report. We've scheduled this work to start in Q1 2013 due to resource contention.

3.8 August 2012

Andrew started with a baseline Windows 7 system and tracked all changes made by downloading, running, and using Tor Browser. Analysis is slow, but ongoing. The Windows 7 analysis is being tracked in ticket 6845.

3.9 July 2012

Starting to investigate automated tools to get a baseline footprint of Tor Browser on Windows and OSX.

3.10 June 2012

Developing a plan to run the forensic analysis of Tor Browser on various systems.

4 C.2.8

4.1 April 2013

See Section C.2.5 and C.2.6 for status.

4.2 March 2013

See Section C.2.5 and C.2.6 for status.

4.3 February 2013

See Section C.2.5 and C.2.6 for status.

4.4 January 2013

- We released new Tor Browser Bundles highlighting updates to Firefox 17.03 ESR. We also released updated -alpha Tor Browser Bundle testing bundles. These testing bundles include Tor 0.2.4.10-alpha.
- We released and then reverted new Tor Browser Bundles which contained an unsafe version of OpenSSL.

4.5 December 2012

Updated Tor Browser bundle with new Firefox release. Updated the testing branch of TBB with Tor 0.2.4.7-alpha. The bridge-by-default bundles were updated to include Tor 0.2.4.7-alpha release. Tor 0.2.4.8-alpha) was released. (Tor 0.2.4.9 was quickly released to address a bug and will soon make it into packages.

4.6 November 2012

Updated Tor Browser Bundle with new Tor stable release. Announced and launched the testing branch of Tor Browser based on alpha Tor.

4.7 October 2012

4.8 September 2012

We updated the bridge-by-default bundles to include Tor 0.2.2.39-stable release. We also updated the Tor cloud images to fix a bug found in the unattended-upgrades configuration. The normal bridge images have also been updated to include obfsproxy, which attempts to help users circumvent censorship by transforming the Tor traffic between the client and the bridge.

4.9 August 2012

No new releases to report.

4.10 July 2012

Bridge-by-default bundles were updated on August 14th which include the latest stable version of Tor, 0.2.2.38.

4.11 June 2012

Bridge-by-default bundles exist.

5 C.2.9

5.1 April 2013

5.2 March 2013

5.3 February 2013

We released new pluggable transports bundles.

We've updated the Pluggable Transports Tor Browser Bundles with Firefox 17.0.4esr and Tor 0.2.4.11-alpha. These releases have numerous bug fixes and a new Torbutton as well.

There is a bug that prevents the bundled Obfsproxy from working on Mac OS X 10.6. We are working on fixing it. See ticket #8549 for progress.

Like the previous bundles, these contain Flashproxy and the Python version of Obfsproxy.

Flash proxy is a transport that uses proxies running in web browsers as access points into Tor. Obfsproxy is a pluggable transport that makes network traffic look unlike normal Tor traffic. Both of these technologies make it harder to block access to Tor. If you previously used the obfsproxy bundle, please upgrade to this bundle, which in addition to flash proxy has new obfsproxy bridges.

Flash proxy works differently from other pluggable transports, and you need to take extra steps to make it work. In particular, you will probably need to configure port forwarding in order to receive connections from browser proxies. There are instructions and hints on how to do that at this page: flash proxy howto.

These bundles contain the same hardcoded obfs2 bridge addresses as the previous bundles which may work for some jurisdictions but you are strongly advised to get new bridge addresses from BridgeDB: https://bridges.torproject.org/?transport=obfs2.

Furthermore, we are looking for feedback on how the bundles work. Please leave comments on the flash proxy usability wiki page or ticket #7824 with your experience, good or bad.

There are other ways you can help beyond testing the bundles. One is to run a bridge with pyobfsproxy. Another is to put the flash proxy badge on your web site or blog, or add it to your Wikipedia profile. If you want your browser to continue to be a proxy after a switch to an opt-in model, click the \Yes" button on the options page.

5.4 January 2013

Released more experimental combined flashproxy and obfsproxy bundles for testing. Flash proxy is a transport that uses proxies running in web browsers as access points into Tor. pyobfsproxy is a Python implementation of the obfsproxy modular transport that makes network traffic look unlike normal Tor traffic. Both of these technologies make it harder to block access to Tor. If you previously used the obfsproxy bundle, please upgrade to this bundle, which in addition to flash proxy has new obfsproxy bridges.

Flash proxy works differently than other pluggable transports, and you need to take extra steps to make it work. In particular, you will probably need to configure port forwarding in order to receive connections from browser proxies. There are instructions and hints on how to do that at this page: flash proxy howto.

These bundles contain fresh obfs2 bridge addresses, which may work for you if the bridges in the obfsproxy bundle are blocked. The bundles also includes an experimental obfs3 bridge—obfs3 is a new protocol designed to be harder to identify than the previous obfs2. If even these new bridges become blocked, you can find your own obfs2 bridges.

We are looking for feedback on how the bundles work. Please leave comments on the flash proxy usability wiki page or ticket 7824 with your experience, good or bad.

There are other ways you can help beyond testing the bundles. One is to run a bridge with pyobfsproxy. Another is to put the flash proxy badge on your web site or blog, or add it to your Wikipedia profile. If you want your browser to continue to be a proxy after a switch to an opt-in model, click the "Yes" button on the options page.

5.5 December 2012

We released new combined flashproxy and pyobfsproxy bundles for users who need them. The bundles also includes an experimental obfs3 bridge—obfs3 is a new protocol designed to be harder to identify than the previous obfs2.

5.6 November 2012

Hired a flashproxy developer. Released flashproxy version 0.9 and version 0.10. These include binaries for the Microsoft Windows Operating System and improved documentation. Also Made the facilitator hand out more proxies by default, reducing a client's need to re-register.

5.7 October 2012

Released flashproxy version 0.8. Fixed a number of Microsoft Windows bugs. A big change is that flashproxy-client now operates as a managed proxy by default. This means that there is no longer a need to start flashproxy-client separately from Tor.

5.8 September 2012

Continued progress on flashproxy development. Released flashproxy version 0.4. This includes the ability to use HTTPS, easy instructions for getting it working in Debian Linux Operating System, fixed some command-line options, and updated the README directions.

5.9 August 2012

No progress to report.

5.10 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

5.11 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

6 C.3.3

6.1 April 2013

6.2 March 2013

See C.2.7 above.

6.3 February 2013

See C.2.7 above.

6.4 January 2013

See C.2.7 above.

6.5 December 2012

See C.2.7 above.

6.6 November 2012

See C.2.7 above.

6.7 October 2012

See C.2.7 above.

6.8 September 2012

See C.2.7 above.

6.9 August 2012

See C.2.7 above.

6.10 July 2012

The US State Dept is also interested in a forensic analysis of Tor Browser. They may match BBG funding to make this item happen faster. Determination of their match will happen in September.

In the meanwhile, we've start writing up a specification of the work to be performed for this forensic analysis.

6.11 June 2012

Started work to find a forensics person to analyze the traces left behind by current Tor Browser.

7 C.3.4

7.1 April 2013

See C.2.9 above.

7.2 March 2013

See C.2.9 above.

7.3 February 2013

See C.2.9 above.

7.4 January 2013

See C.2.9 above.

7.5 December 2012

See C.2.9 above.

7.6 November 2012

See C.2.9 above.

7.7 October 2012

See C.2.9 above.

7.8 September 2012

See C.2.9 above.

7.9 August 2012

No progress to report.

7.10 July 2012

Continuing discussion of how to integrate Flashproxy into the tor product line and how to make them easy to deploy.

7.11 June 2012

Started a discussion with the developer of Flashproxy about stability, deployment, and testing with users.

  - Ticket 6539 Image cache isolation causes assert crash
  - Ticket 7494 Create local homepage for TBB
  - Ticket 7495 Browser-based update notification mechanism (was 4238)
  - Ticket 4234 Firefox update process
  - Ticket 6564 Enable DOM Storage and isolate it to url bar domain
  - Re-base the following patches for compatibility with Firefox ESR 17:
    * Ticket 6786 0010-Limit-device-and-system-specific-CSS-Media-Queries.patch
    * Ticket 6253 0020-Add-mozIThirdPartyUtil.getFirstPartyURI-API.patch
    * Ticket 6253 0021-Add-canvas-image-extraction-prompt.patch
    * Ticket 5856 0022-Return-client-window-coordinates-for-mouse-event-scr.patch
    * Ticket 5856 0023-Do-not-expose-physical-screen-info.-via-window-and-w.patch
    * Ticket 6786 0024-Do-not-expose-system-colors-to-CSS-or-canvas.patch

2.6 November 2012

- We released a major new version of Tor Browser which is based on Tor 0.2.3-stable branch of Tor. The announcement is published.
- We released a test version of Tor Brwoser which is based on Tor 0.2.4-alpha branch of Tor. The alpha TBB announcement is published.
- Mike attended the W3C Do Not Track and Beyond workshop, and presented Tor Browser in an attempt to demonstrate that client-side Privacy by Design can solve the same problems as server-side opt-out. My paper is up at http://www.w3.org/2012/dnt-ws/agenda.html.
- Mike went further down the PathBias rabbit hole and found a few related bugs with respect to how we handle circuit timeouts for hidden services. Additionally, it appears that it's indeed possible to tag RELAY cells in such a way that failure to "untag" these cells results only in stream timeout conditions (which we also transparently retry on new circuits) rather than full circuit destruction. Thanks to Rob Jansen for bringing this up. Luckily, aside from the hidden service issues, CircuitStreamTimeouts and other post-construction failure modes appear almost non-existent in normal conditions once a circuit gets built successfully.
- Closed 4 tickets on the schedule for November TBB task list. The 4 tickets are:
  1. Client with low CBT can't establish any circuits
  2. Perform TBB version check async on new tab
  3. Image cache isolation causes assert crash in debug builds (and other cases?)
  4. Decide which tbb-usability tickets get addressed by a bounty program

2.7 October 2012

No progress to report.

2.8 September 2012

We re-evaluated the inclusion of Firefox 15 favoring the Firefox ESR release series. The current ESR release is well-understood and patches are being applied with each release to improve functionality. We're beginning to work on the next ESR cycle which will be based upon Firefox 17.

In order to help make progress on this front, we've hired Pearl Crescent to help improve our Tor Browser.

2.9 August 2012

Firefox 15 integration has been painful and broken some of the functionality we rely upon for user protection. We're re-evaluating the move to FF15 so quickly.

2.10 July 2012

Continuing to develop a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser. TBB builds are mostly automated now and next steps are to engineer custom TBB parameters and to be able to allow for at-build-time integration of bookmarks, landing pages, and look and feel.

2.11 June 2012

Developing a plan to implement the build infrastructure changes to deliver the 12 customized versions of Tor Browser.

3 C.2.7

3.1 April 2013

Made progress on Ticket 6845 for Windows forensics. Five new bugs were opened to address the data detritus left behind.

Defined the steps for OSX analysis in Ticket 6846.

3.2 March 2013

Initial results from the forensic analysis were published on our blog. Blog post is copied below:

As part of a deliverable for two of our sponsors (Sponsor J, Sponsor L), I have been working on a forensic analysis of the Tor Browser Bundle. In this three part series, I will summarize the most interesting or significant traces left behind after using the bundle. This post will cover Debian Linux (#8166), part two will cover Windows 7, and part three will cover OS X 10.8.

Process

I set up a virtual machine with a fresh install of Debian 6.0 Squeeze, logged in once and shut it down cleanly. I then connected the virtual drive to another virtual machine and used dd to create an image of the drive. I also used hashdeep to compute hashes for every file on the drive, and rsync to copy all the files over to an external drive.

After having secured a copy of the clean virtual machine, I rebooted the system, connected an external drive, and copied the Tor Browser Bundle (version 2.3.25-6, 64-bit) from the external drive to my Debian home directory. I extracted the package archive and started the Tor Browser Bundle by running ./start-tor-browser inside the Tor Browser directory.

Once the Tor Browser was up and running, I browsed to a few pages, read a few paragraphs here and there, clicked on a few links, and then shut it down by closing the Tor Browser and clicking on the Exit-button in Vidalia. The Tor Browser did not crash and I did not see any error messages. I deleted the Tor Browser directory and the tarball using rm -rf.

I repeated the steps with dd, hashdeep, and rsync to create a copy of the tainted virtual machine.

Results

Using hashdeep, I compared the hashes from the tainted virtual machine against the hashes from the clean virtual machine: 68 files had a hash that did not match any of the hashes in the clean set. The most interesting files are:

~/.local/share/gvfs-metadata/home: contains the filename of the Tor Browser Bundle tarball: tor-browser-gnu-linux-x86_64-2.3.25-5-dev-en-US.tar.gz. GVFS is the virtual filesystem for the GNOME desktop, so this result will probably vary depending on the window manager used. I have created #8695 for this issue.

~/.xsession-errors: contains the following string: \Window manager warning: Buggy client sent a _NET_ACTIVE_WINDOW message with a timestamp of 0 for 0x3800089 (Tor Browse)". It is worth noting that a file named .xsession-errors.old could also exist. I have created #8696 for this issue.

~/.bash_history: contains a record of commands typed into the terminal. I started the Tor Browser Bundle from the command line, so this file contains lines such as ./start-tor-browser. I have created #8697 for this issue.