

Trawling for Tor Hidden Services: Detection, Measurement, Deanononymization

A. Biryukov, I. Pustogarov, R.P. Weinmann
University of Luxembourg
Ivan.pustogarov@uni.lu

May 20, 2013

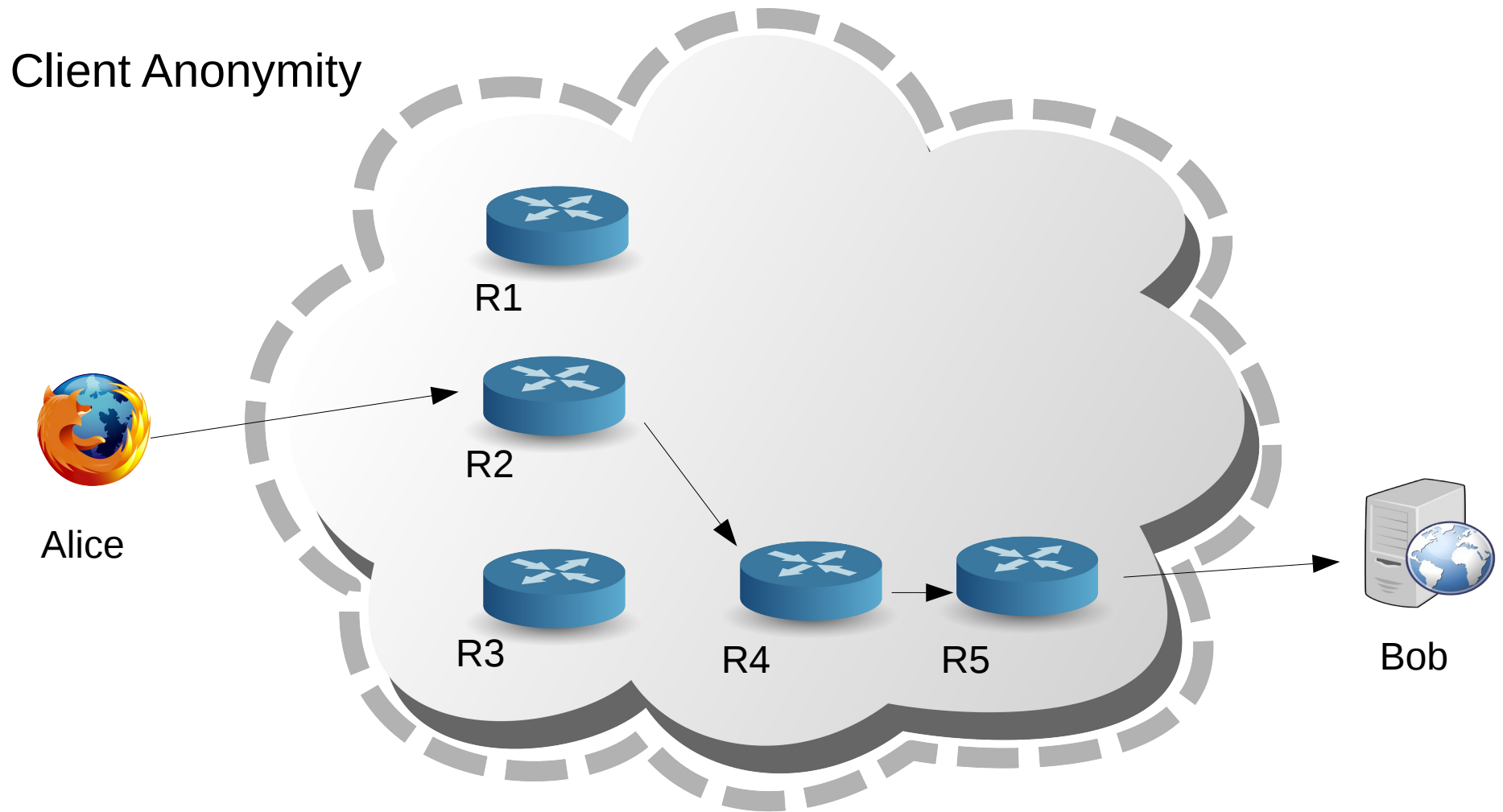
Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.

Overview

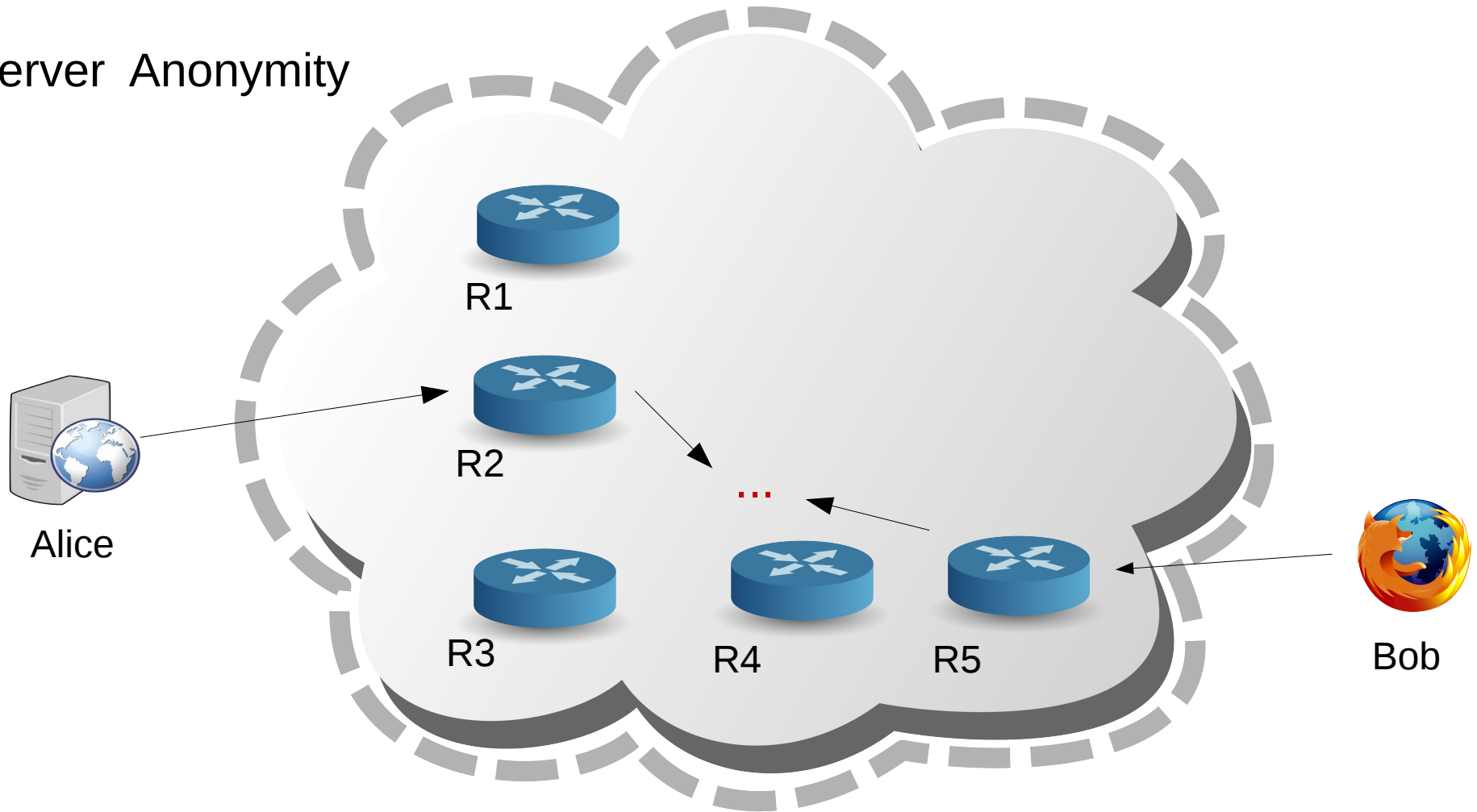
- **Background**
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.

Tor anonymity network



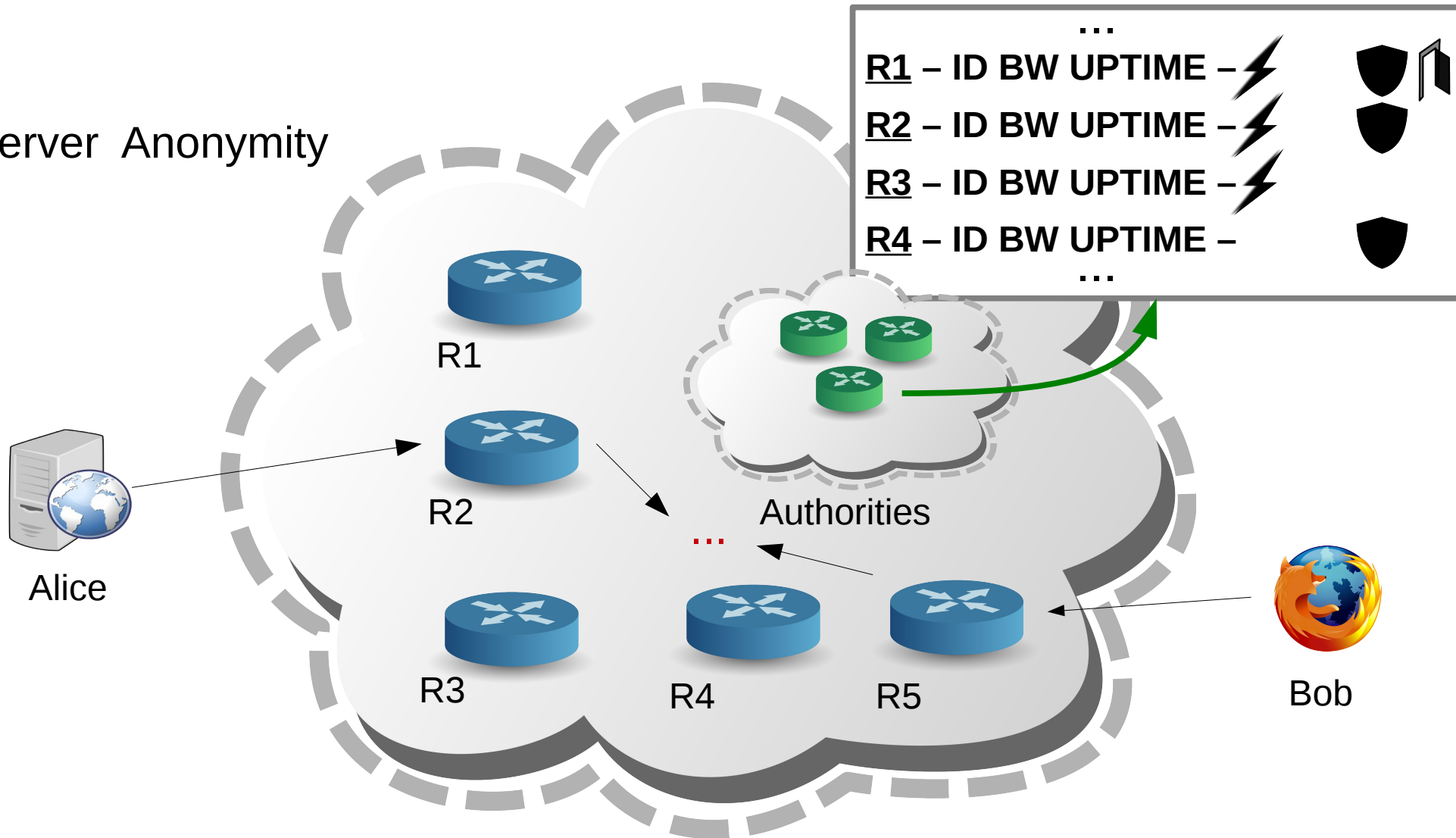
Tor anonymity network

Server Anonymity























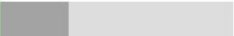













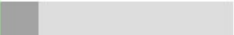






























































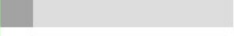














Tor anonymity network

Server Anonymity

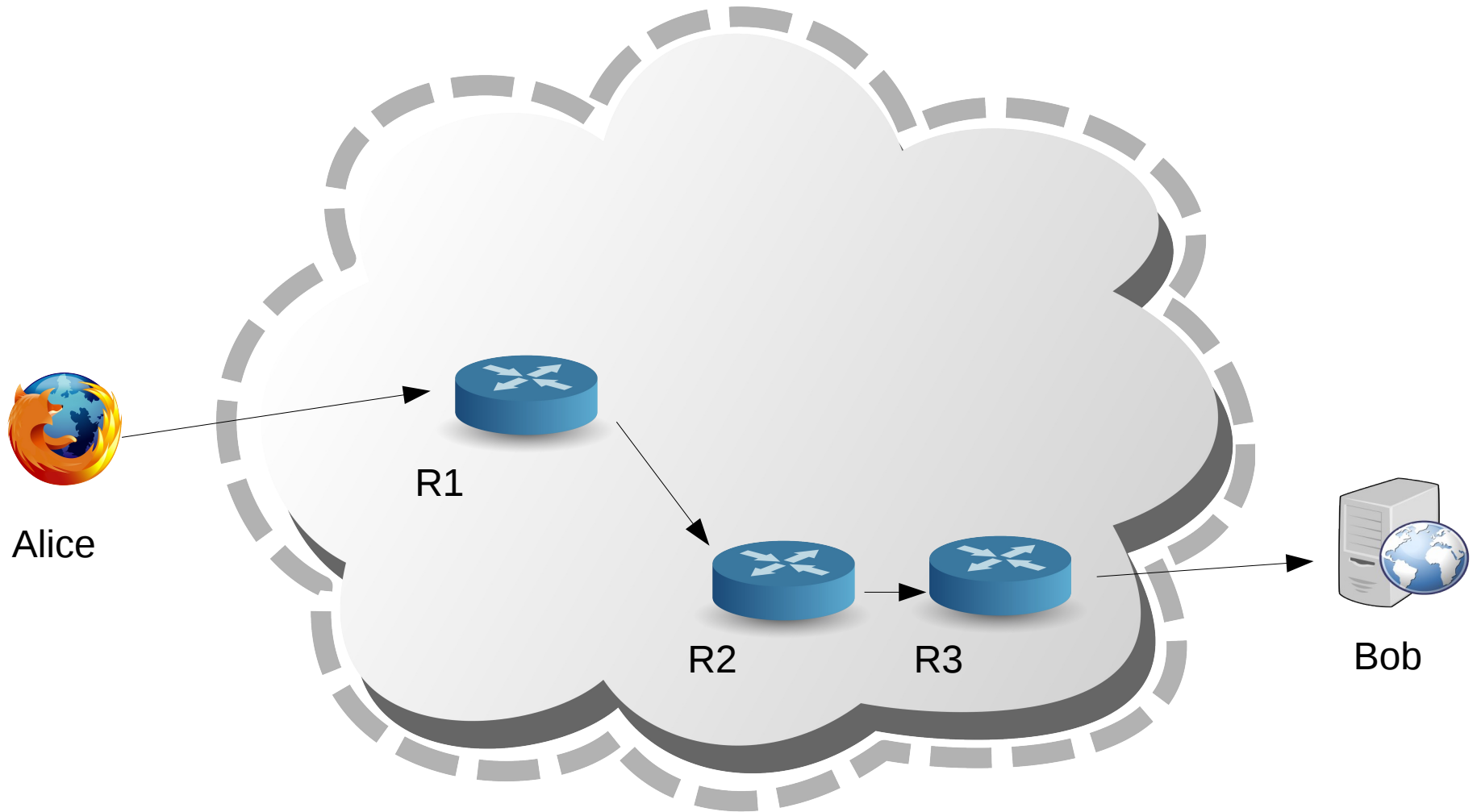


Consensus

 menTor		1737	67 d	55863896.cust.multi.fi [85.134.56.150]	    
 microshaft		2820	66 d	tor-exit.microshaft.org [208.201.249.3]	    
 minisausage		3348	35 d	50.7.184.58 [50.7.184.58]	    
 morphium		298	51 d	this.is.a.Tor.server.please.see.tor.morphium.info [91.143.90.25]	    
 NetromAc		2115	47 d	1385160742.business.dbnet.dk [82.143.224.38]	    
 Nitr0x		175	78 d	50.97.1.36-static.reverse.softlayer.com [50.97.1.36]	    
 OhCanada		419	51 d	van1.zworg.com [209.17.191.117]	    
 onconnex80		392	213 d	tor01.onconnex.com [184.105.231.11]	    
 PasToutAFaitNet1		261	176 d	91.229.20.159 [91.229.20.159]	    
 PasToutAFaitNet2		763	196 d	tor2.pastoutafait.net [95.130.11.247]	    
 plebia		3599	79 d	tor-exit.plebia.org [37.59.162.218]	    
 pps		9	59 d	184-22-164-107.static.hostnoc.net [184.22.164.107]	    
 PrivaTOReu		4229	100 d	torexit.privator.eu [88.208.90.1]	    
 programmercpp		149	36 d	proxy [213.171.220.40]	    
 PsyNetNP		155	52 d	broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]	    
 Qwerty		91	157 d	93.167.245.178 [93.167.245.178]	    

<http://torstatus.blutmagie.de/>

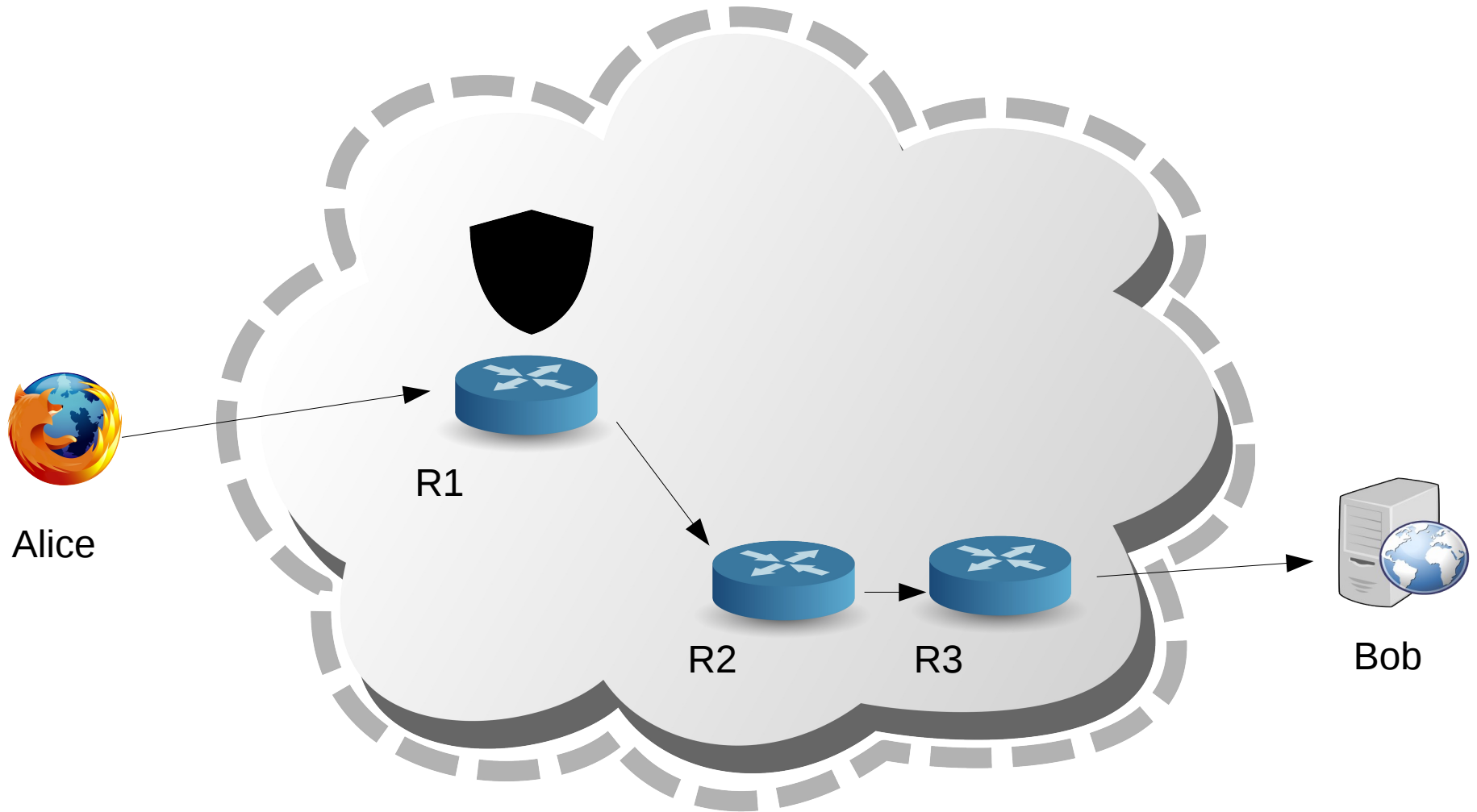
Guards



Guard = high uptime + high bandwidth

Every client has 3 Guard nodes

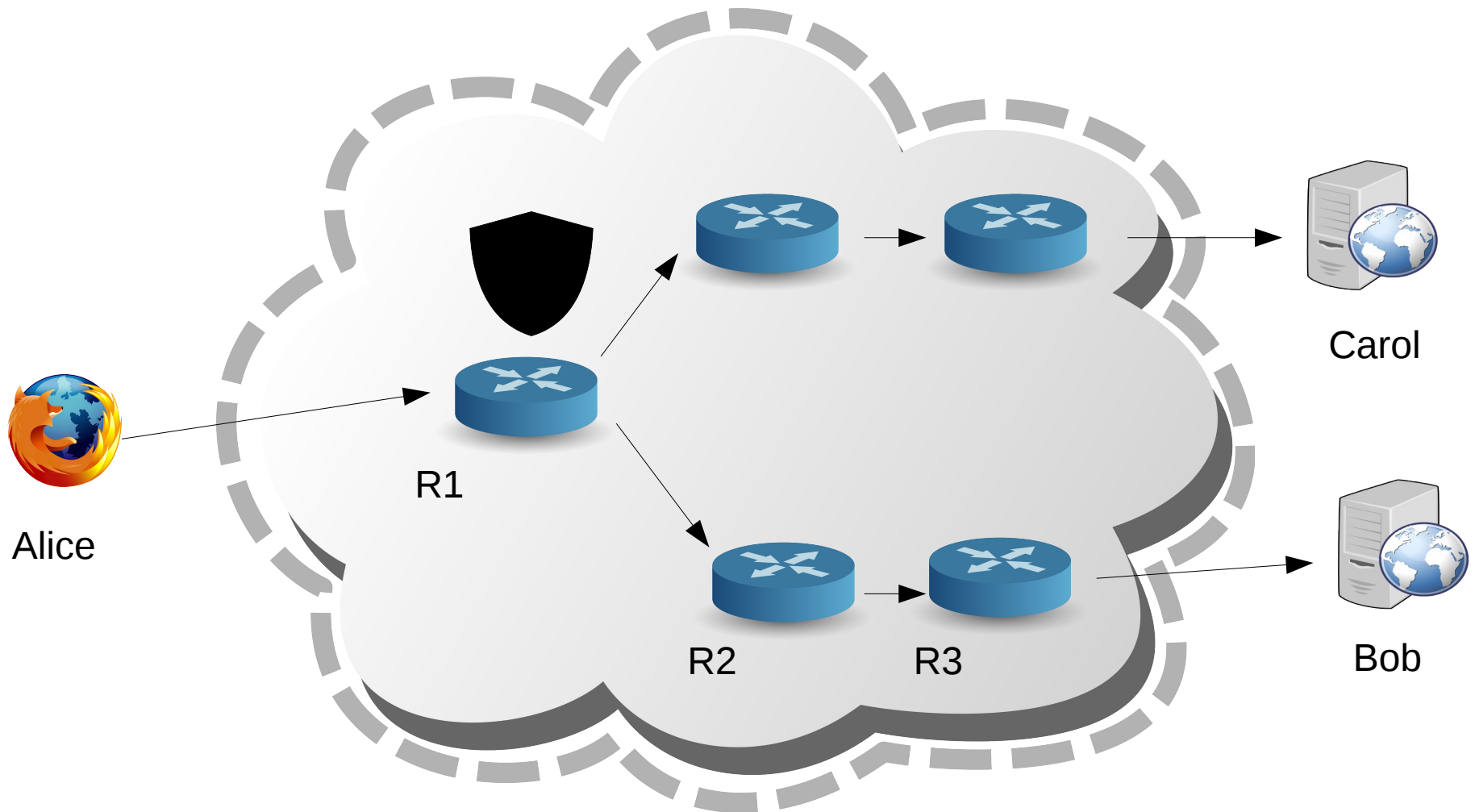
Guards



Guard = high uptime + high bandwidth

Every client has 3 Guard nodes

Guards



Guard = high uptime + high bandwidth

Every client has 3 Guard nodes

Examples of Tor HS



Public Library of US Diplomacy: Kissinger Cables

2013-04-08

The Kissinger Cables are part of today's launch of the WikiLeaks Public Library of US Diplomacy (PlusD), which holds the world's largest searchable collection of United States confidential, or formerly confidential, diplomatic communications. As of its launch on April 8, 2013 it holds 2 million records comprising approximately 1 billion words.

Detainee Policies

2012-10-24

WikiLeaks has begun releasing the 'Detainee Policies': more than 100 classified or otherwise restricted files from the United States Department of Defense covering the rules and procedures for detainees in U.S. military custody. Over the next month, WikiLeaks will release in chronological order the United States' military detention policies followed for more than a

In Wikile

U.K. (2008) contacts li

WikiLeaks
individuals
whose men
number of c
details of al
individuals
fascists" wh

China (200

Examples of Tor HS



Public Library of US Diplomacy: Kissinger Cables

duckduckgo

Duck Duck Go

Duck Duck Go is a search engine based in Valley Forge, Pennsylvania that uses information from crowd-sourced sites (like Wikipedia) with the aim of augmenting traditional results and improving relevance.

[More at Wikipedia](#) | Official site: duckduckgo.com

[Internet search engines](#)

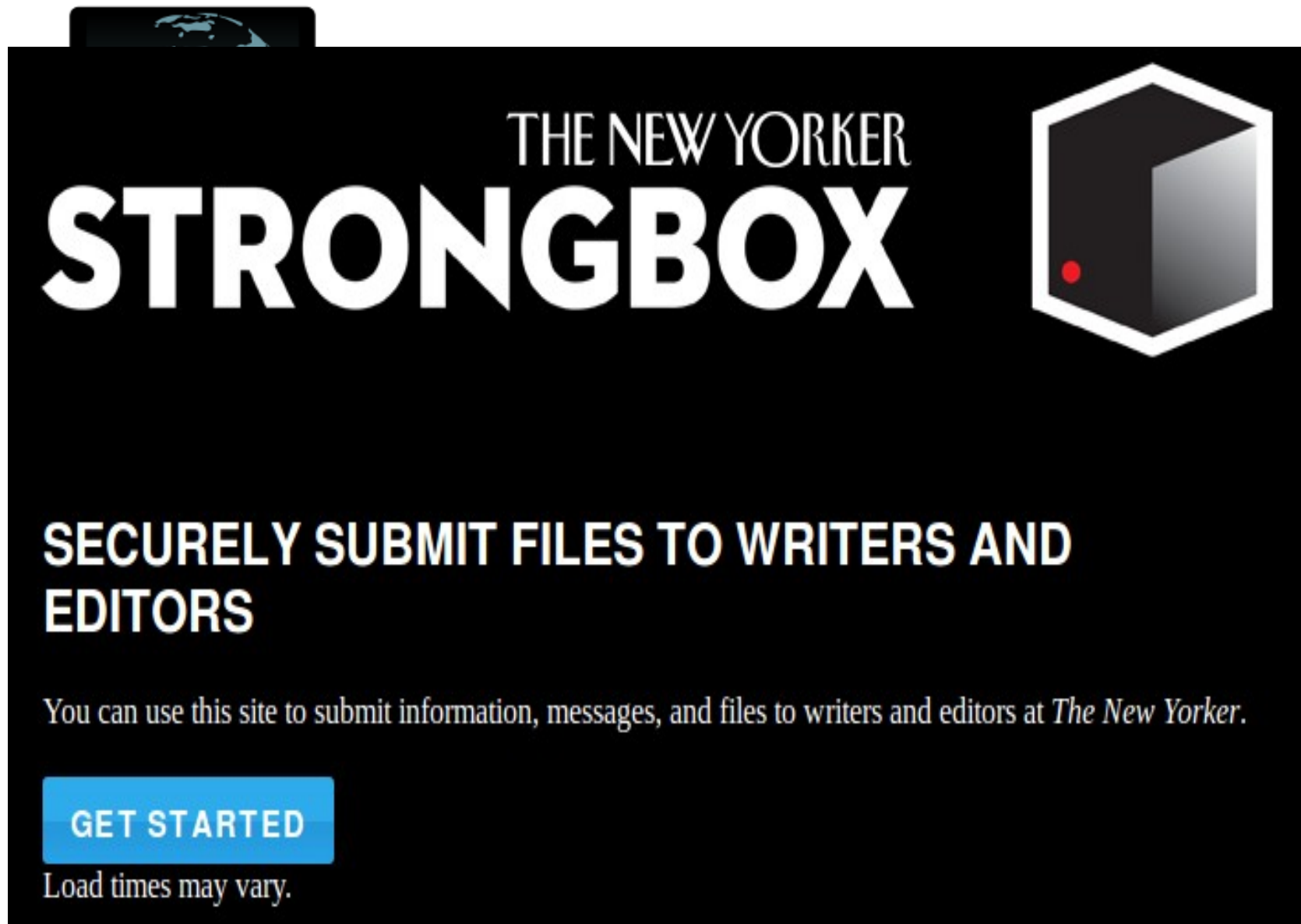
[Duckduckgo | BEGIN-DOWNLOAD.com](#)
Free Download flv app Fast & Simple.
begin-download.com Sponsored link

[Duck Duck Go](#) Official site
duckduckgo.com [More from duckduckgo.com](#)

[DuckDuckGo | CrunchBase Profile](#)
DuckDuckGo is a search engine, like Google. Use it to get more Zero-click Info, more privacy, less spam, lbang syntax and lots of other goodies.
crunchbase.com/company/duck-duck-go [More from crunchbase.com](#)

[DuckDuckGo Challenges Google on Privacy \(With a Billboard\) | Wired Business...](#)
DuckDuckGo, a one-man-band search engine based out of Valley Forge, Pennsylvania, is aiming at Google's privacy practices with an unusual tactic: a billboard.
wired.com/business/2011/01/duckduckgo-google-privacy/ [More from wired.com](#)

Examples of Tor HS



The screenshot shows a web browser window displaying the 'The New Yorker Strongbox' website. The website has a black background with white text. At the top, it says 'THE NEW YORKER' in a smaller font, followed by 'STRONGBOX' in a large, bold font. To the right of the text is a logo consisting of a white hexagon with a black cube inside, and a small red dot on the left side of the cube. Below the main title, the text 'SECURELY SUBMIT FILES TO WRITERS AND EDITORS' is displayed in a bold, white font. Underneath this, a paragraph states: 'You can use this site to submit information, messages, and files to writers and editors at *The New Yorker*.' At the bottom left, there is a blue button with the text 'GET STARTED' in white. Below the button, it says 'Load times may vary.' The browser's address bar at the bottom shows a URL starting with 'wired.com/business/2017/07/duckduckgo-google-privacy/'.

THE NEW YORKER
STRONGBOX

SECURELY SUBMIT FILES TO WRITERS AND EDITORS

You can use this site to submit information, messages, and files to writers and editors at *The New Yorker*.

GET STARTED

Load times may vary.

wired.com/business/2017/07/duckduckgo-google-privacy/ more from wired.com

Examples of Tor HS

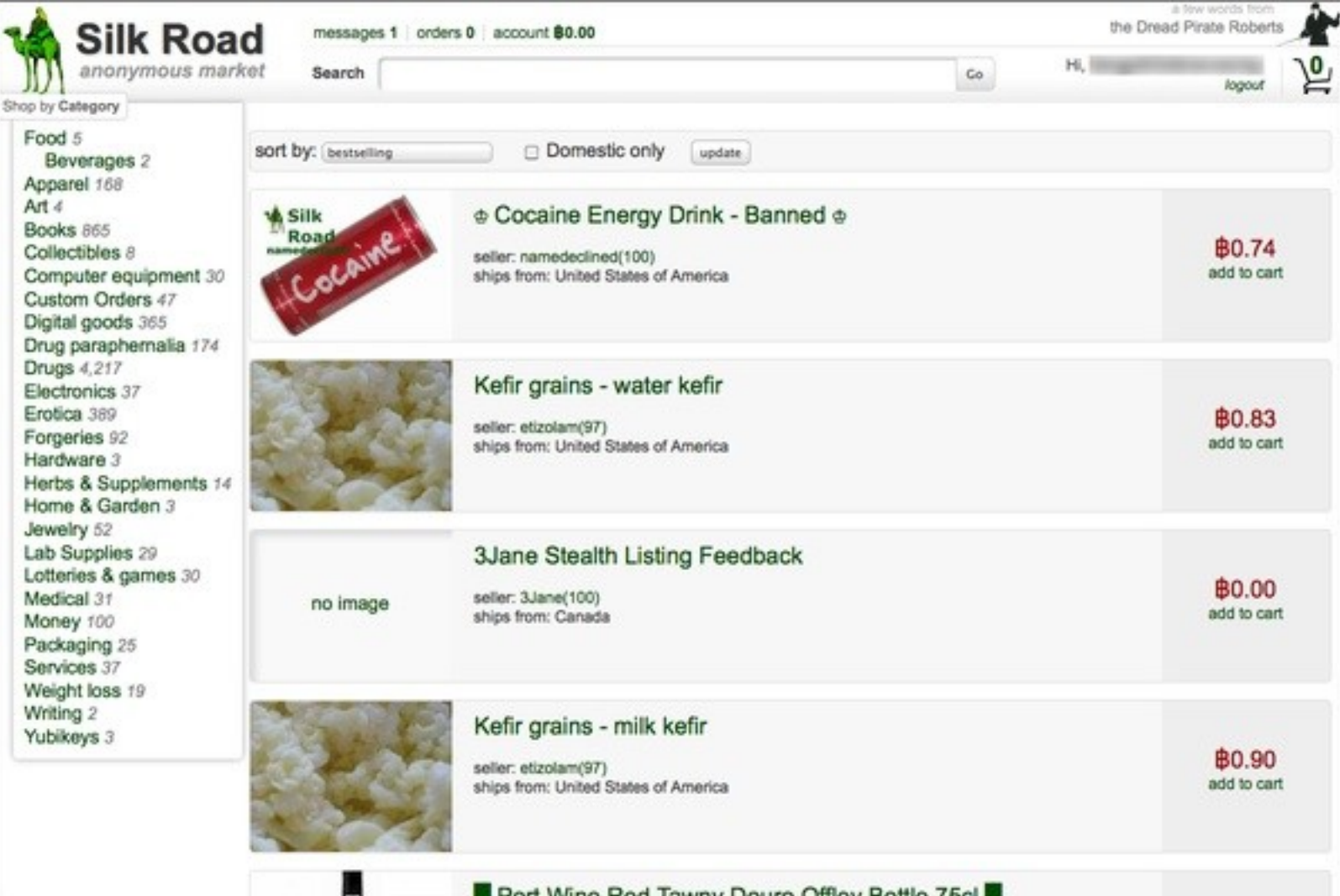
ST

SECURE
EDITOR

You can use this

GET STARTED

Load times may vary.



The image shows a screenshot of the Silk Road anonymous market interface. The header includes the Silk Road logo, navigation links for messages, orders, and account, a search bar, and a user profile section. A sidebar on the left lists various categories for sale, such as Food, Beverages, Apparel, Art, Books, Collectibles, Computer equipment, Custom Orders, Digital goods, Drug paraphernalia, Drugs, Electronics, Erotica, Forgeries, Hardware, Herbs & Supplements, Home & Garden, Jewelry, Lab Supplies, Lotteries & games, Medical, Money, Packaging, Services, Weight loss, Writing, and Yubikkeys. The main content area displays a list of items for sale, including Cocaine Energy Drink - Banned, Kefir grains - water kefir, 3Jane Stealth Listing Feedback, and Kefir grains - milk kefir. Each item listing includes a price, an 'add to cart' button, and a seller name.

Item	Price	Action
Cocaine Energy Drink - Banned	\$0.74	add to cart
Kefir grains - water kefir	\$0.83	add to cart
3Jane Stealth Listing Feedback	\$0.00	add to cart
Kefir grains - milk kefir	\$0.90	add to cart

Examples of Tor HS

The image shows a screenshot of the Silk Road anonymous market interface. The header includes the Silk Road logo, navigation links for messages, orders, and account, a search bar, and a user profile for 'the Dread Pirate Roberts'. The main content area displays a list of items for sale, each with a price and an 'add to cart' button. Overlaid on this is a screenshot of a Reddit post titled 'Skynet, a Tor-powered botnet straight from Reddit' by Claudio Guarnieri. The post discusses a malware artifact found on the Internet, its origin, and its capabilities. The article text is partially obscured by the market interface elements.

Silk Road
anonymous market

messages 1 | orders 0 | account \$0.00

Search [] Go

Hi, [] logout

Shop by Category

Food 5
Beverages 2

sort by: bestselling ☐ Domestic only update

Skynet, a Tor-powered botnet straight from Reddit

Posted by [Claudio Guarnieri](#) in [Information Security](#) on Dec 6, 2012 2:51:13 PM

...ndering through the dark alleys of the Internet we encountered an unusual malware artifact, something that w...e night.

...we spent time looking at it, the more it started to look unusually familiar. As a matter of fact it turned out be...origin named "throwaway236236" described in a very popular *I Am A* thread you can read [here](#).

...is an overview of this malware labelled by the creator as **Skynet**: a Tor-powered trojan with DDoS, Bitcoin m...Usenet.

are the warez

You c...

...ople download software from Usenet and install it in the offices or at friends pretty often. Also Usenet isn't th...k hoster. Most Providers have their own Usenet client for idiot proof downloads"

...a distributed discussion platform established around 1980 and still very popular worldwide.

\$0.74
add to cart

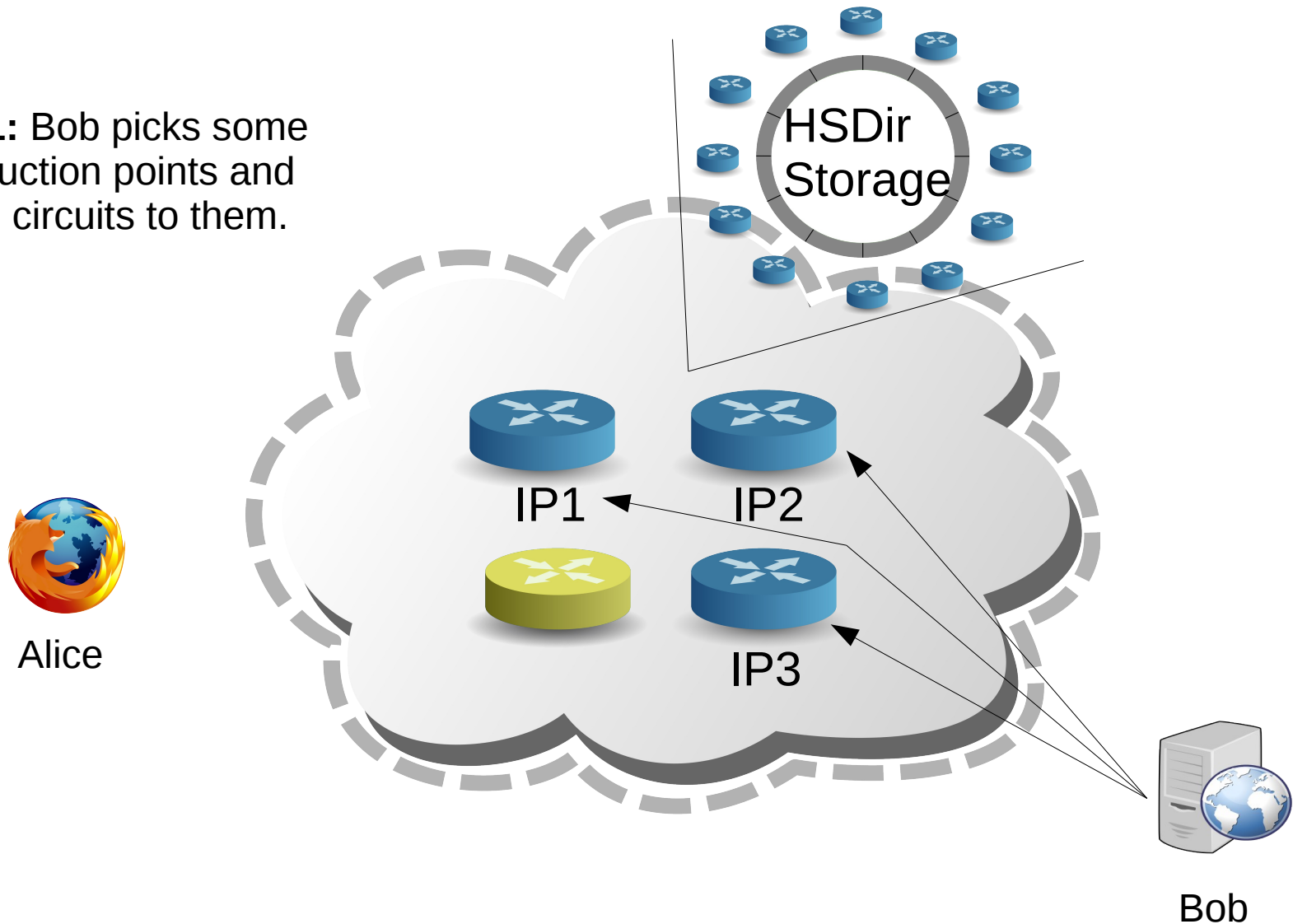
\$0.83
add to cart

\$0.00
add to cart

\$0.90
add to cart

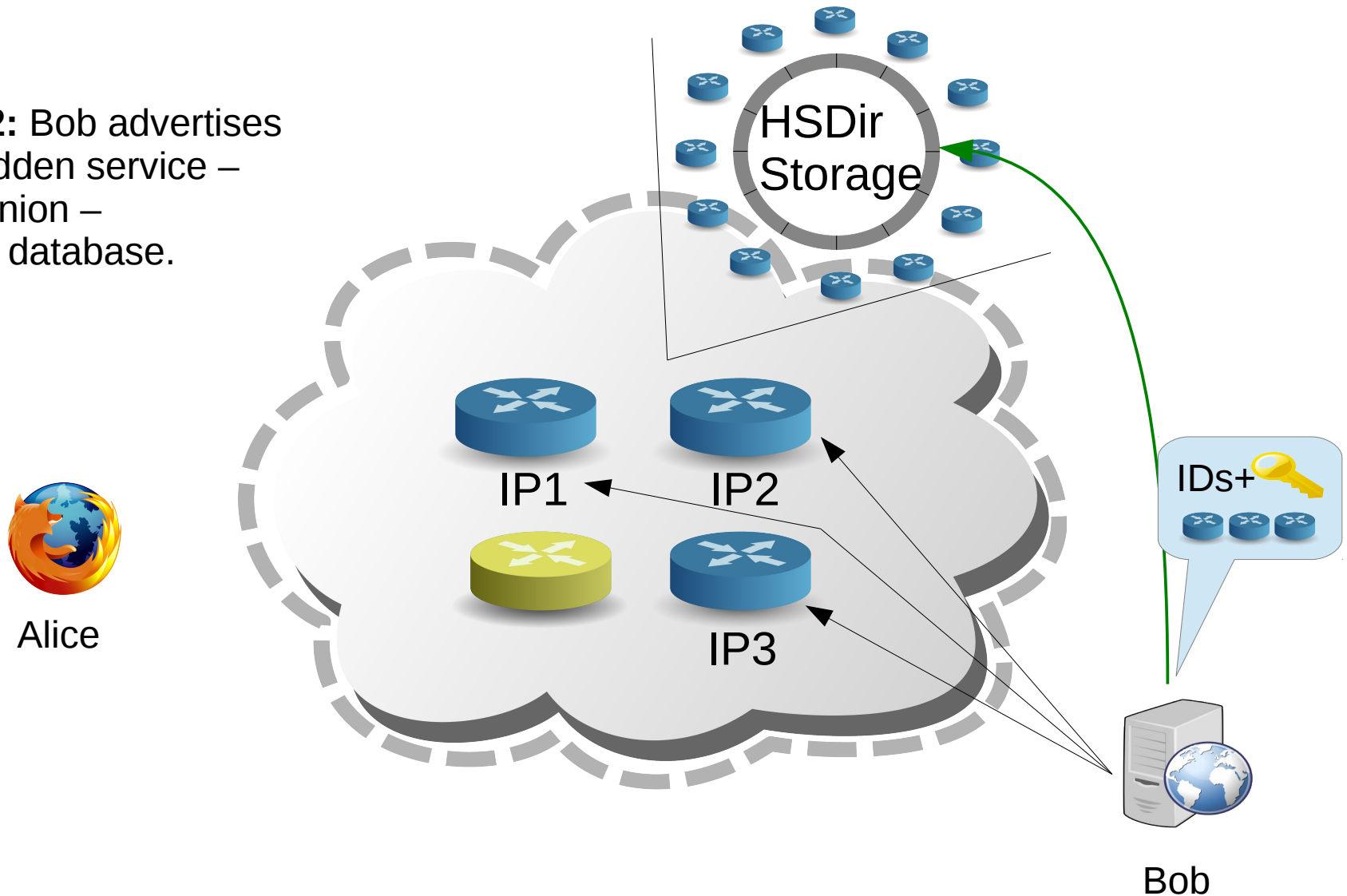
Tor rendezvous protocol

Step1: Bob picks some introduction points and builds circuits to them.



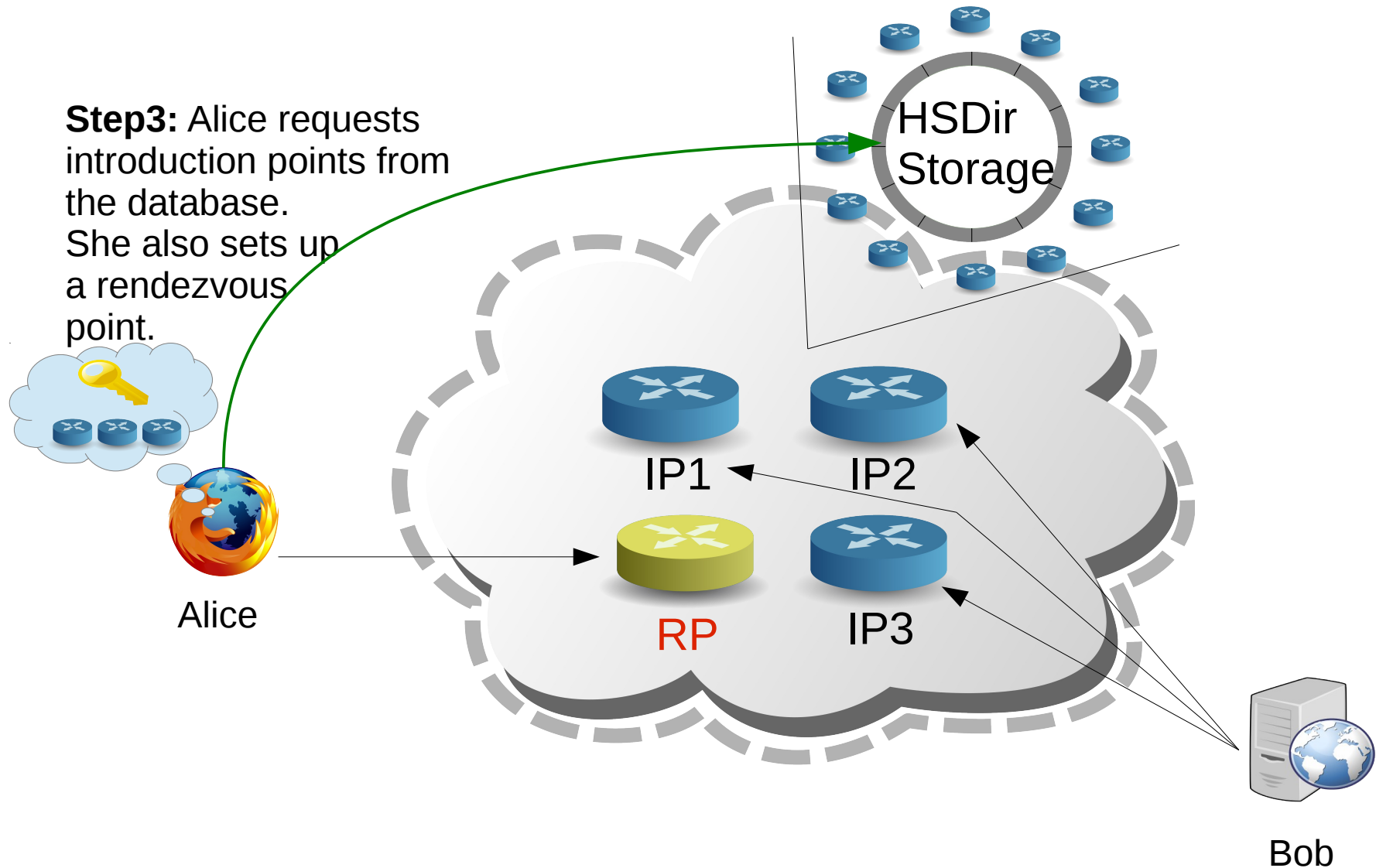
Tor rendezvous protocol

Step2: Bob advertises his hidden service – `<z>.onion` – at the database.



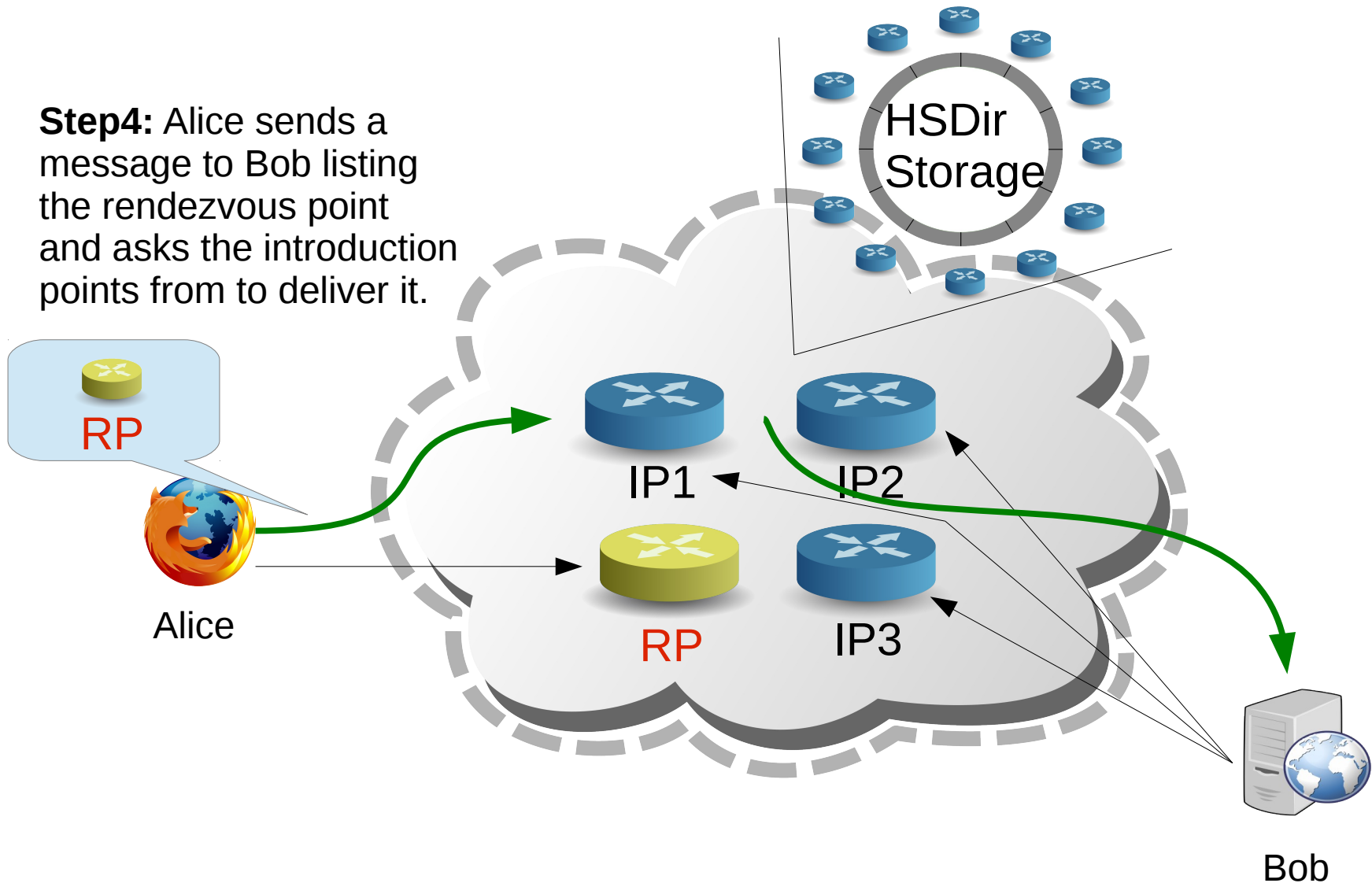
Tor rendezvous protocol

Step3: Alice requests introduction points from the database. She also sets up a rendezvous point.



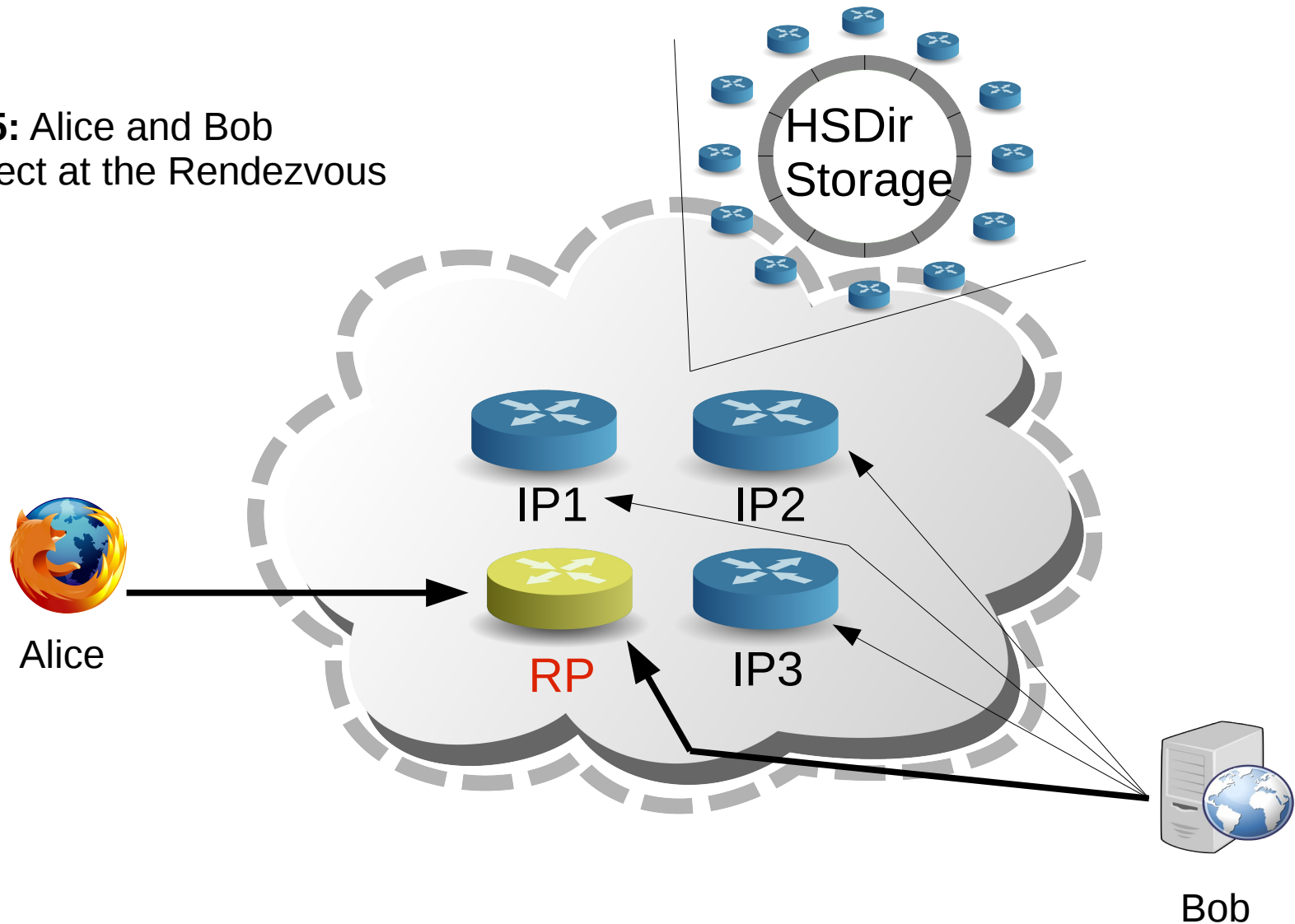
Tor rendezvous protocol

Step4: Alice sends a message to Bob listing the rendezvous point and asks the introduction points from to deliver it.

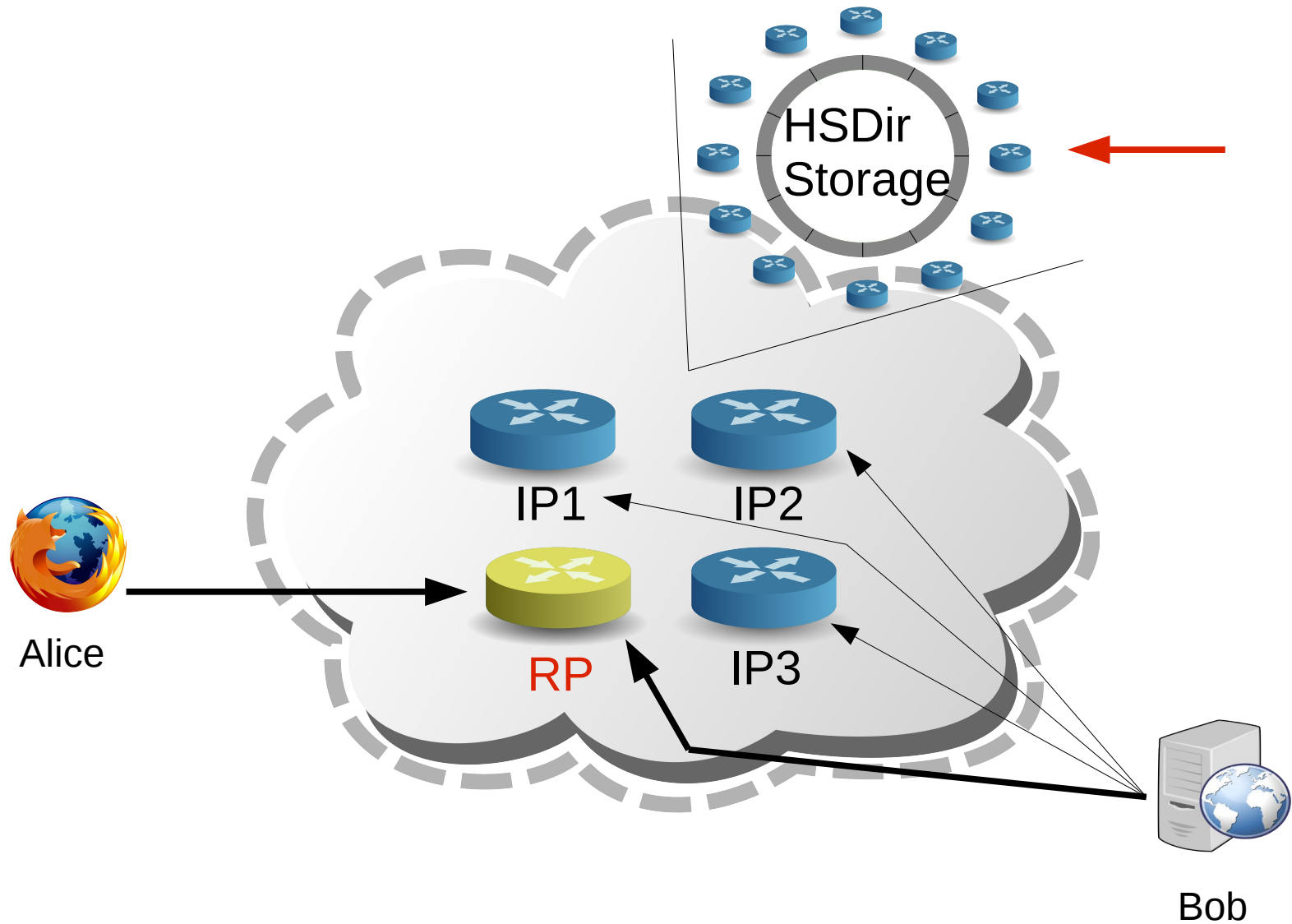


Tor rendezvous protocol

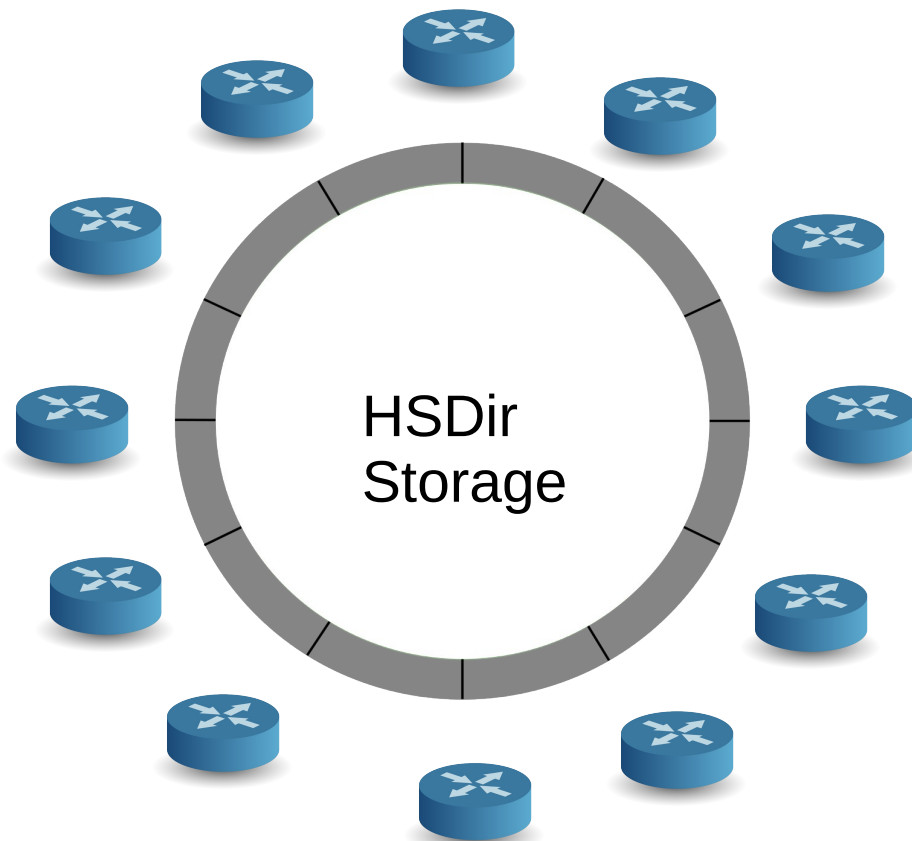
Step5: Alice and Bob
Connect at the Rendezvous
point




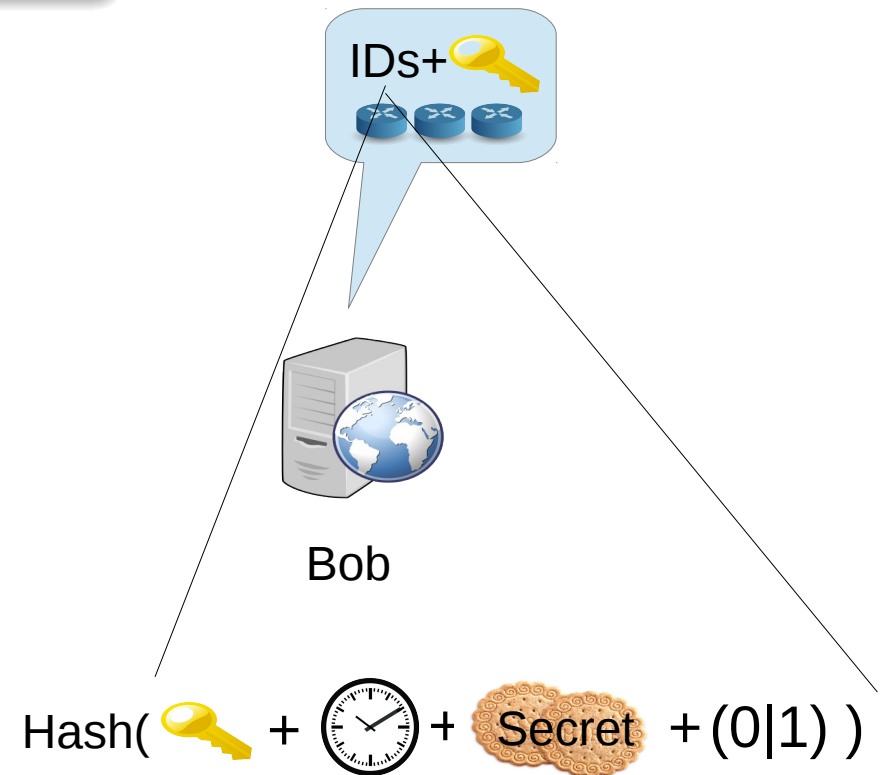
Tor rendezvous protocol



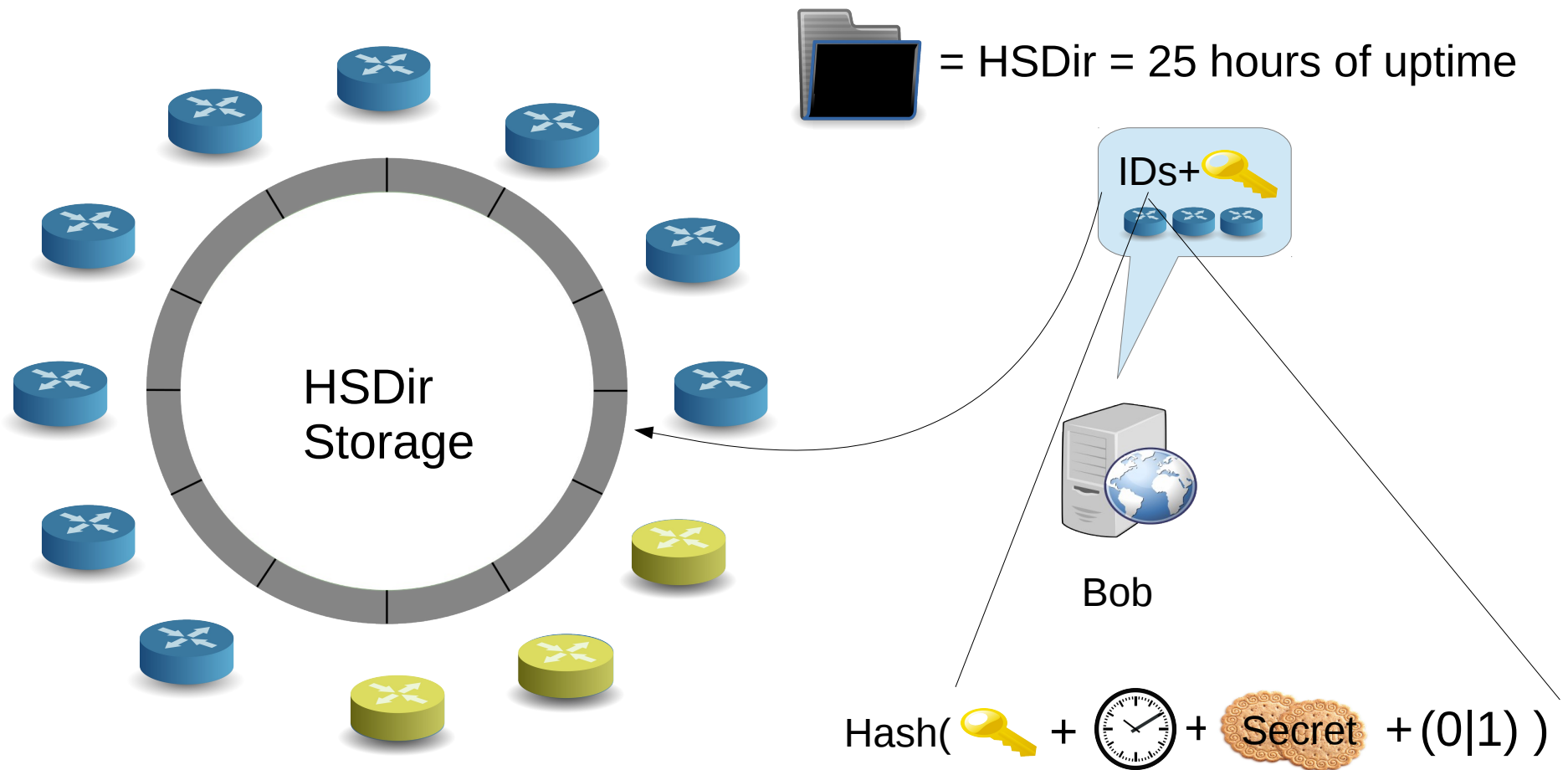
Responsible hidden service directories



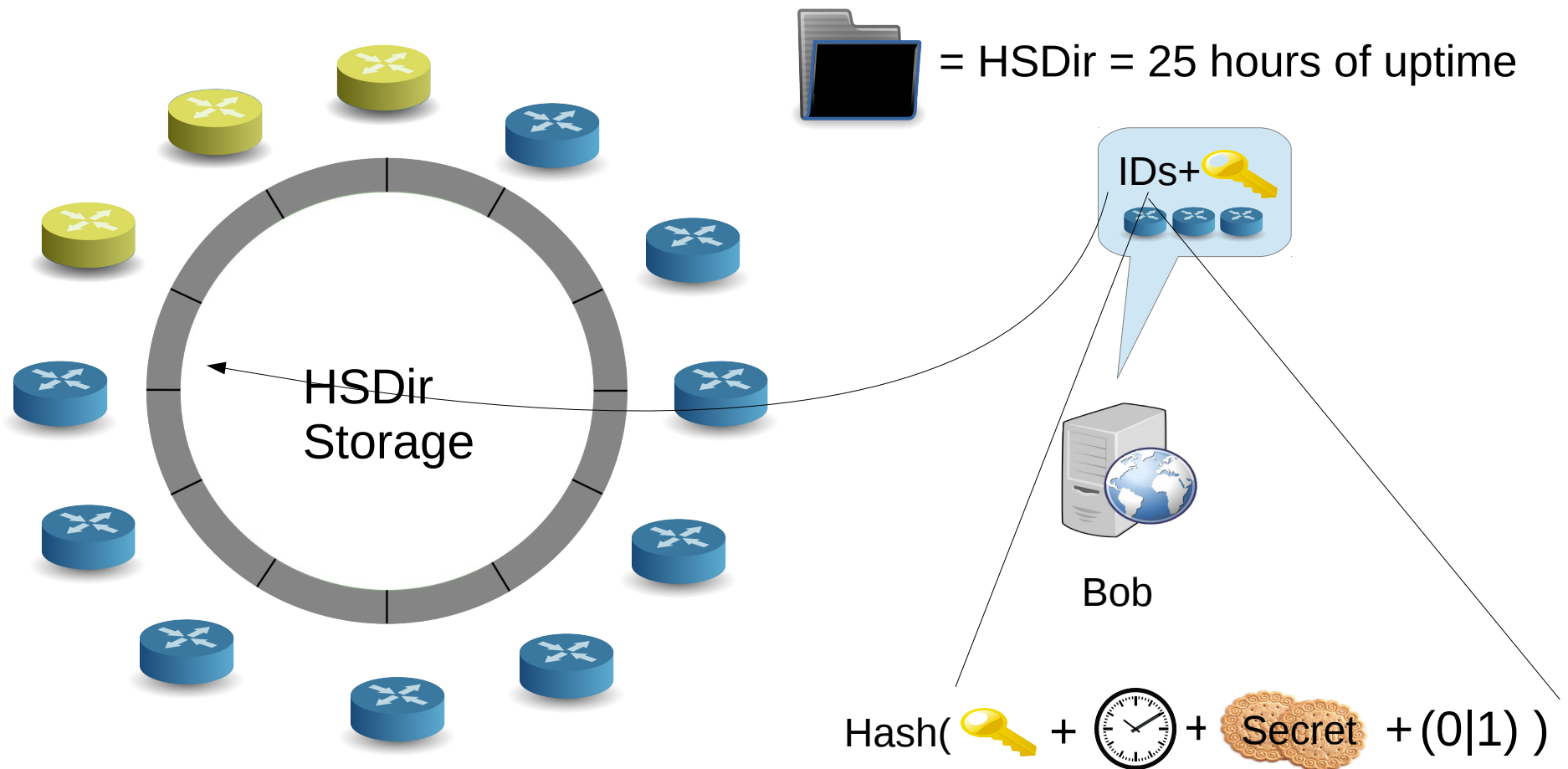
 = HSDir = 25 hours of uptime



Responsible hidden service directories



Responsible hidden service directories

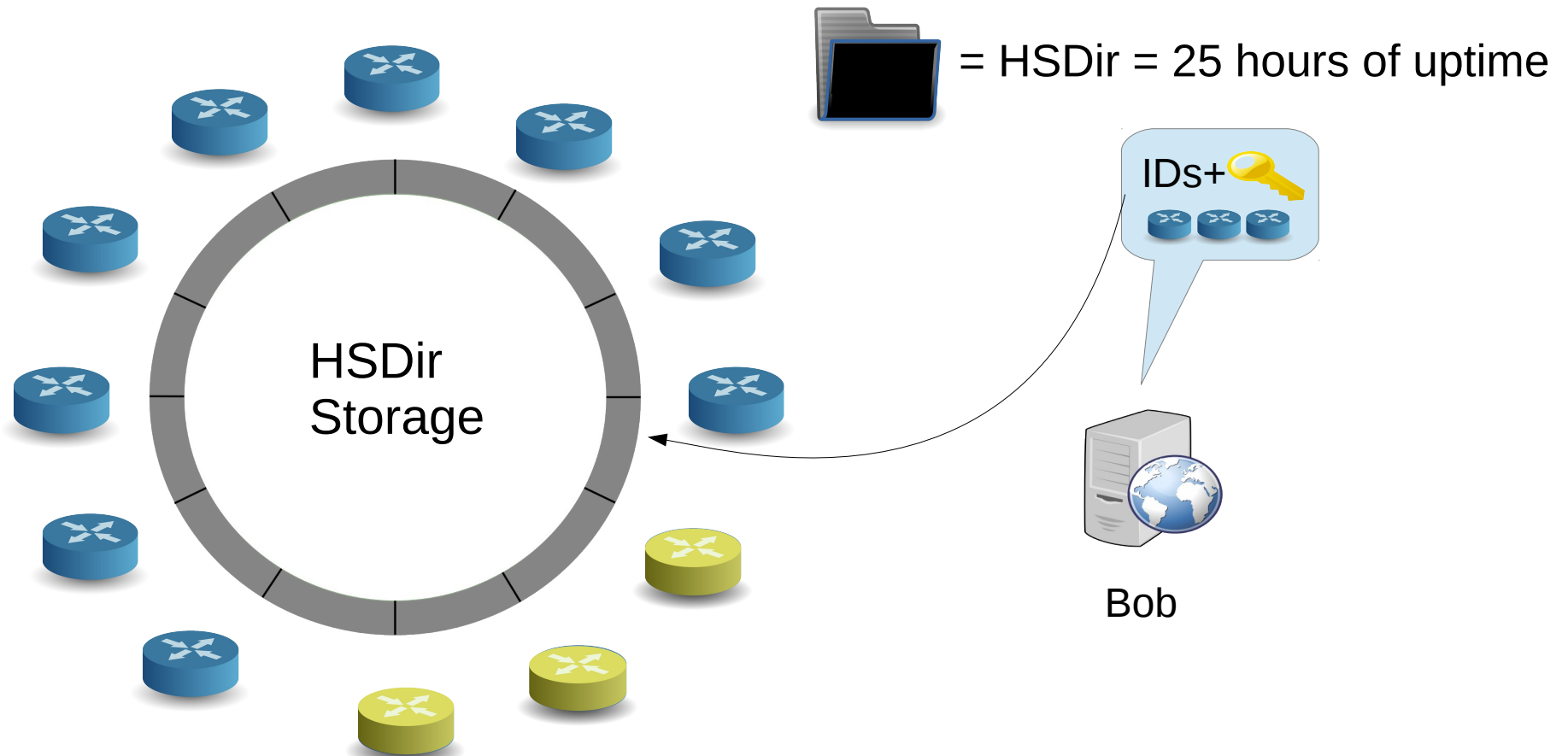


- IDs change every 24 hours at some time during the day
- Re-upload every hour

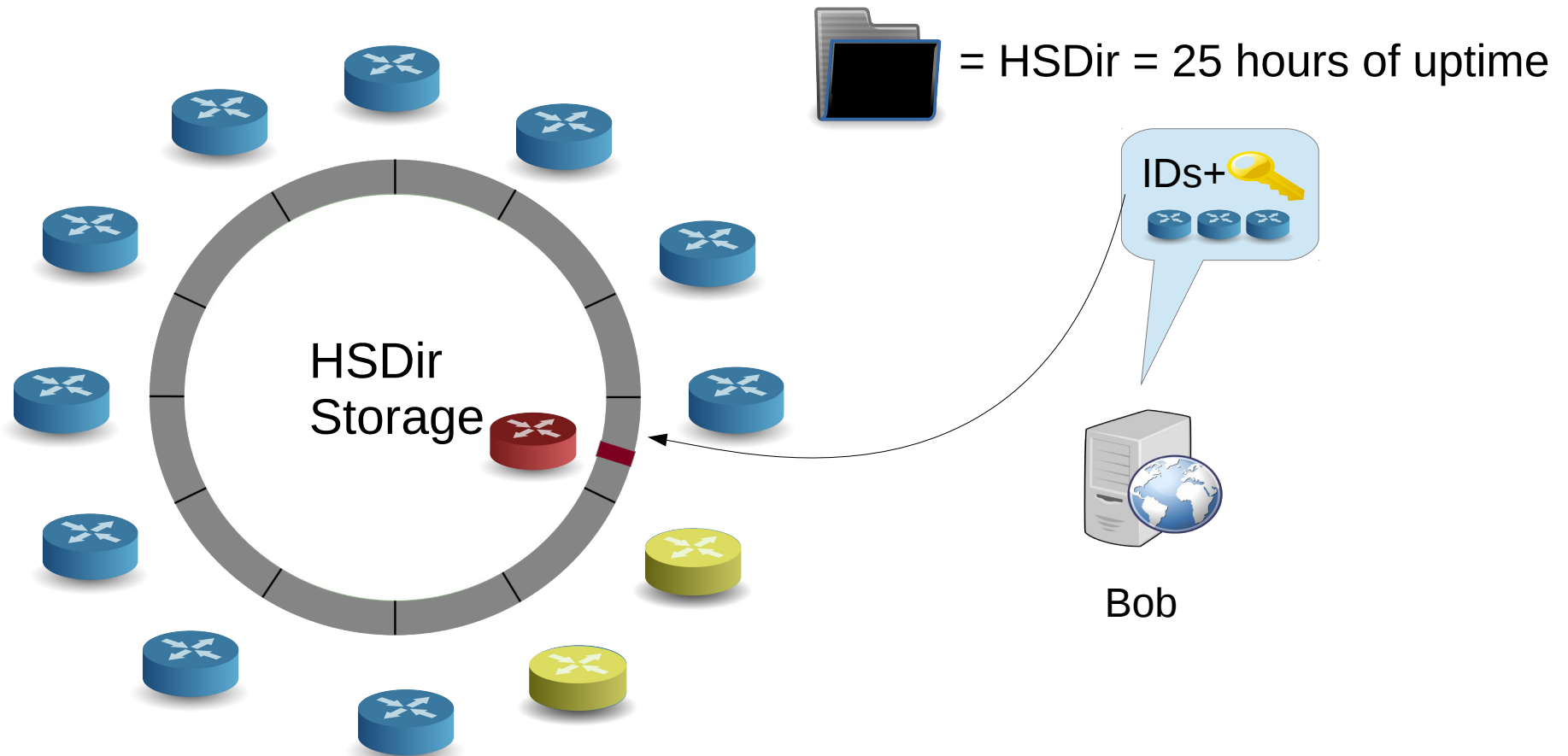
Overview

- Background
- **Measuring the popularity of hidden services**
- **DoSing hidden services.**
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.

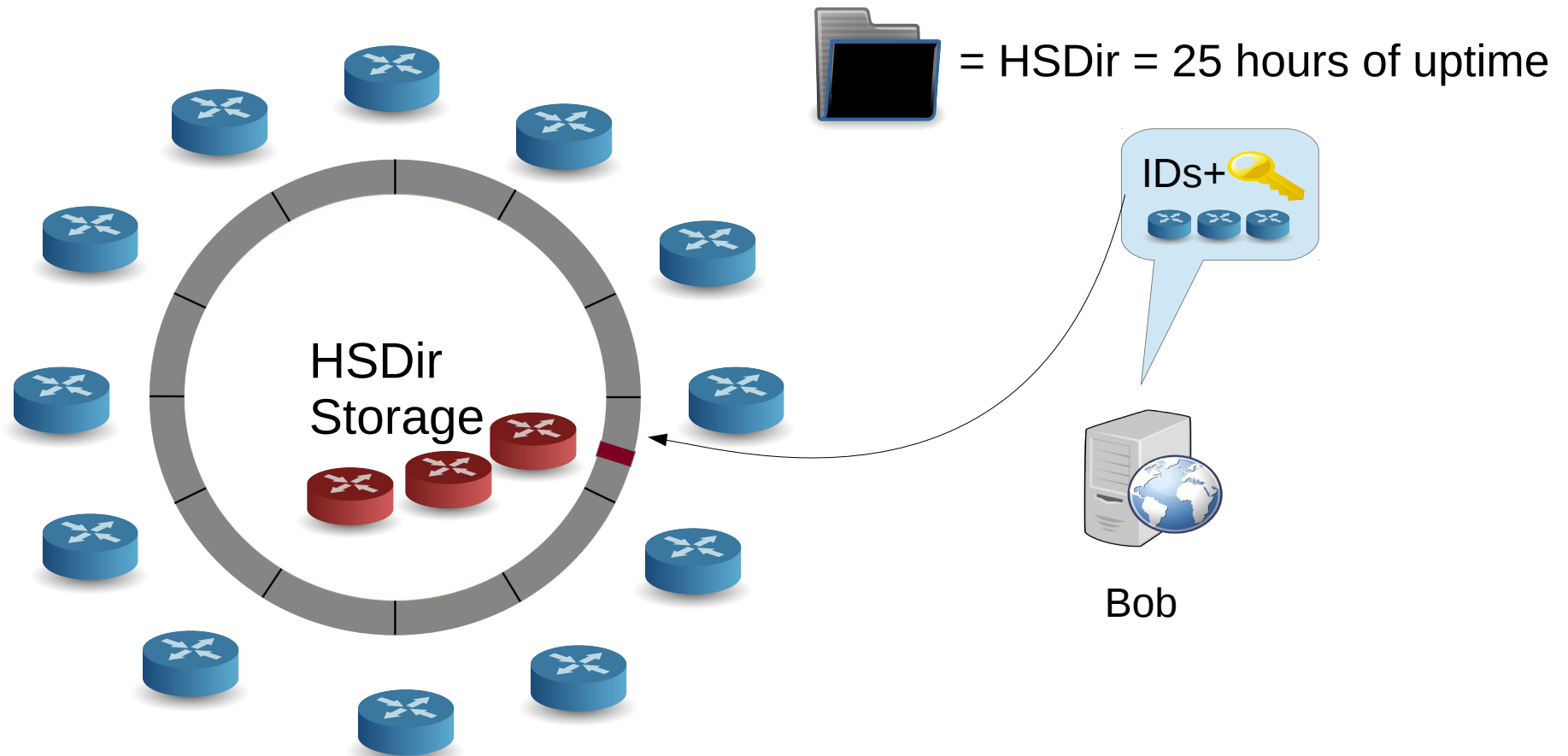
Impersonating Hidden service directory



Impersonating Hidden service directory

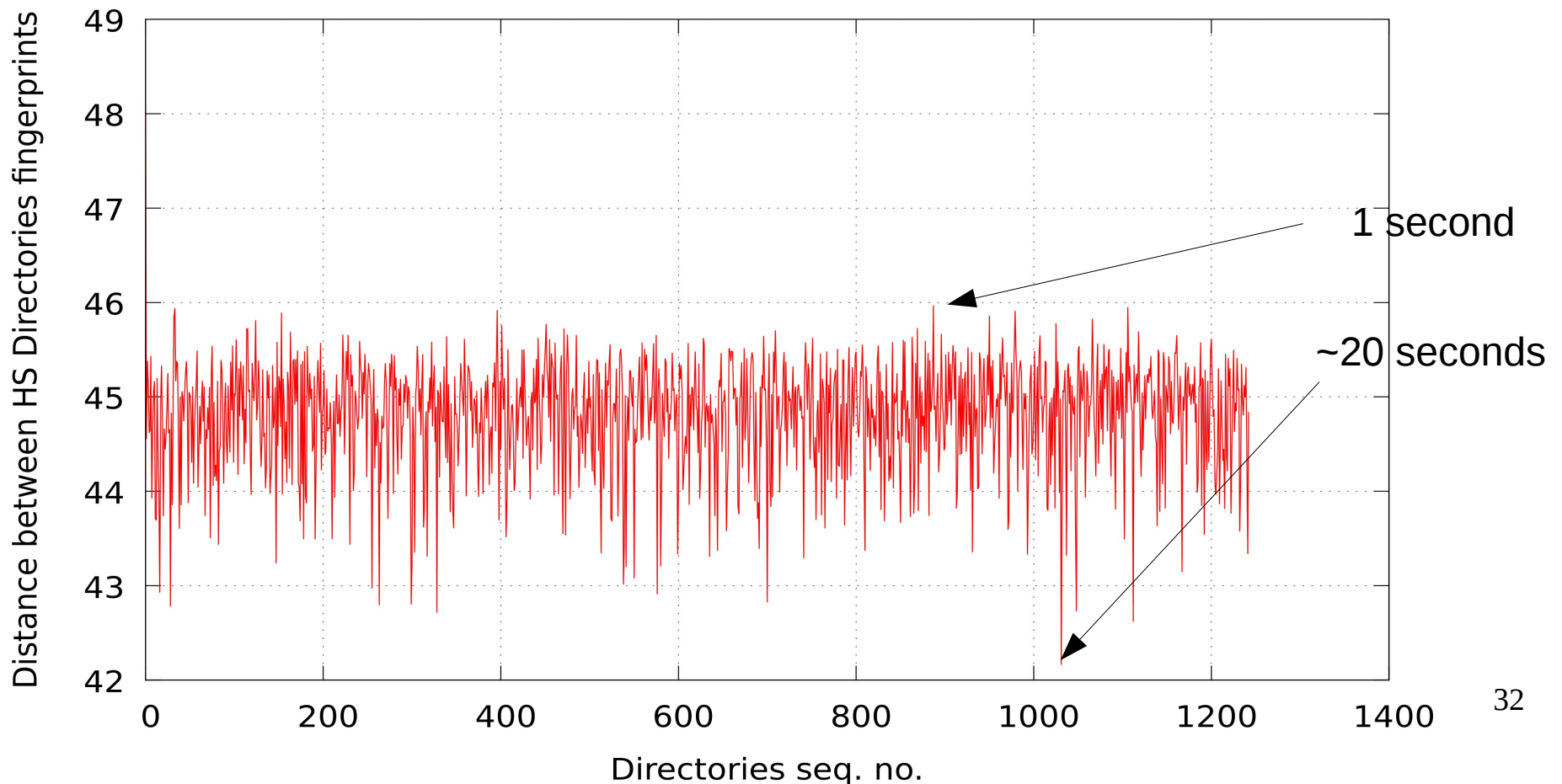


Impersonating Hidden service directory



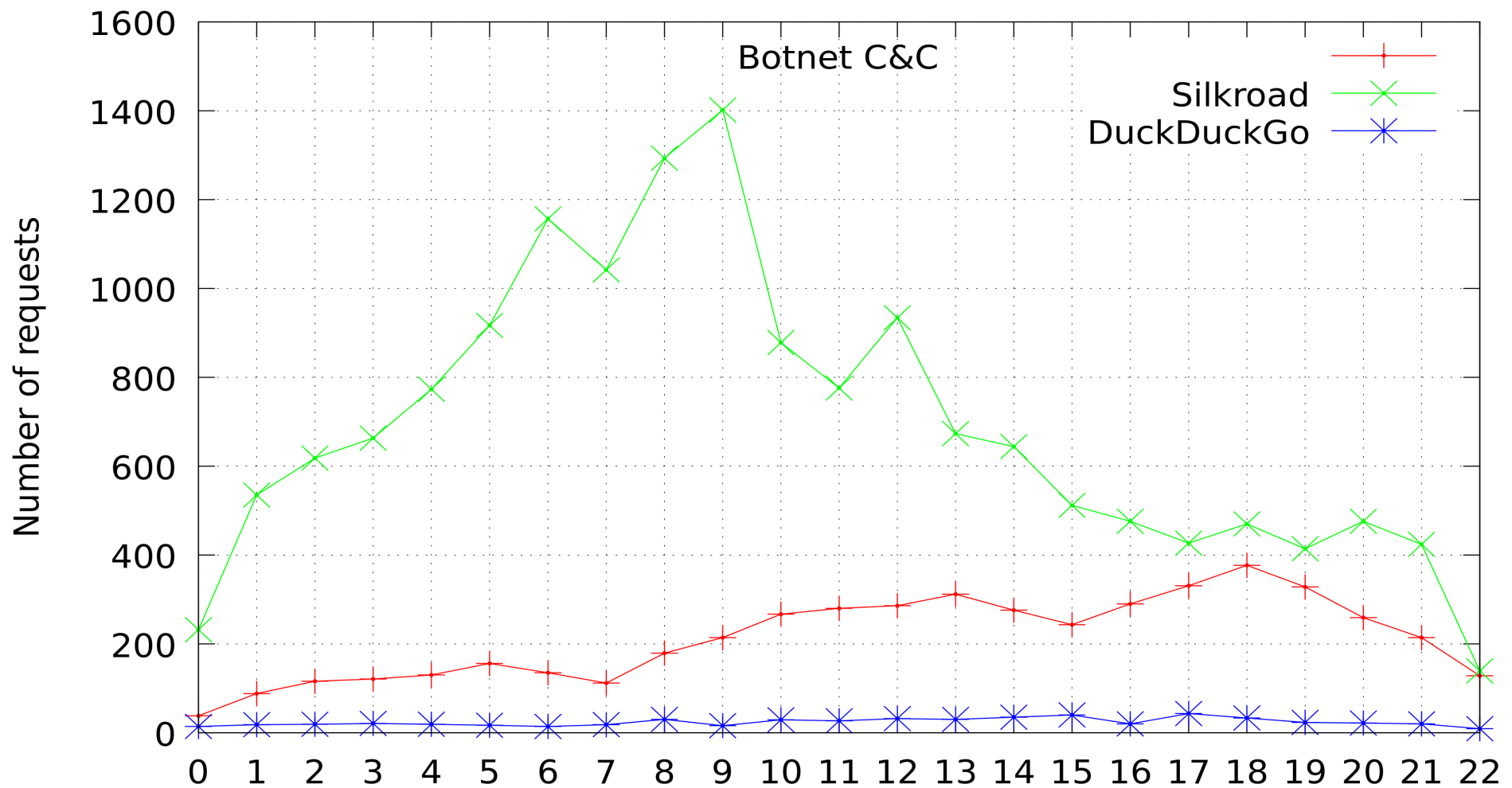
Impersonating Hidden service directory

- By impersonating 1 directory, we can track the popularity
- By impersonating all 6 directories, we can DoS.



Tracking popularity

- We tracked popularity of Skynet C&C, Silkroad, and DuckDuckGo



Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- **Harvesting onion addresses.**
- Revealing the guards.
- Opportunistic deanonymisation.

Shadowing

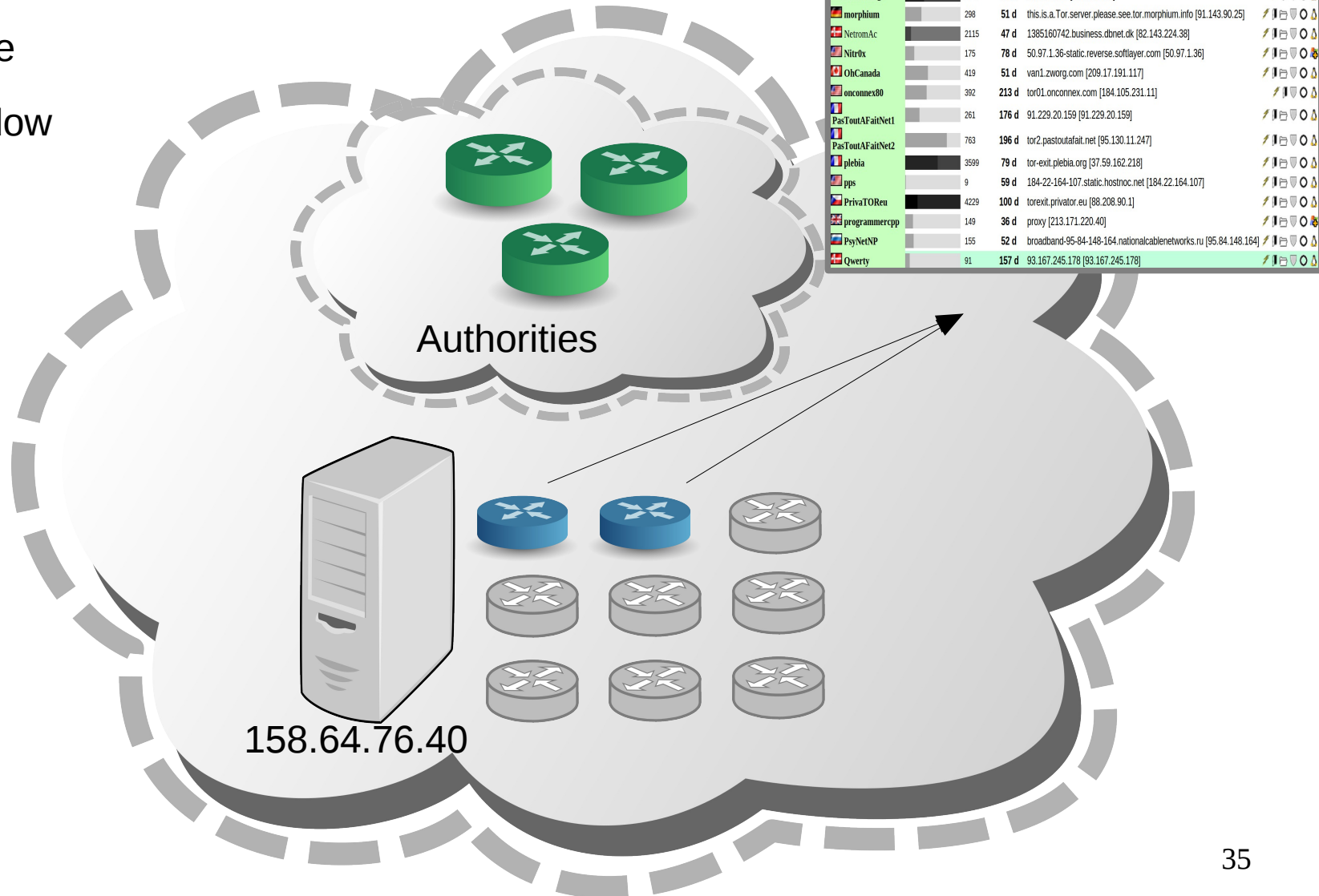
Consensus



- Active

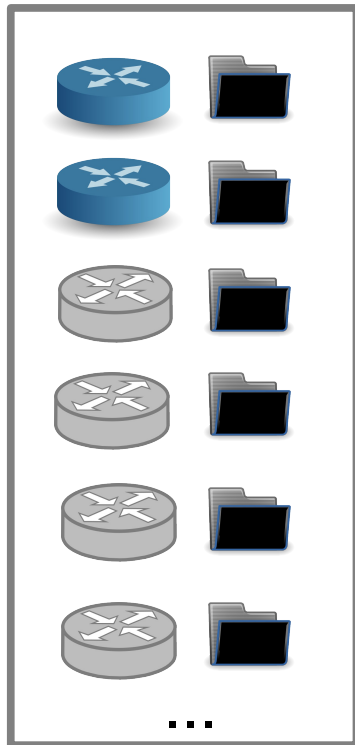


- Shadow

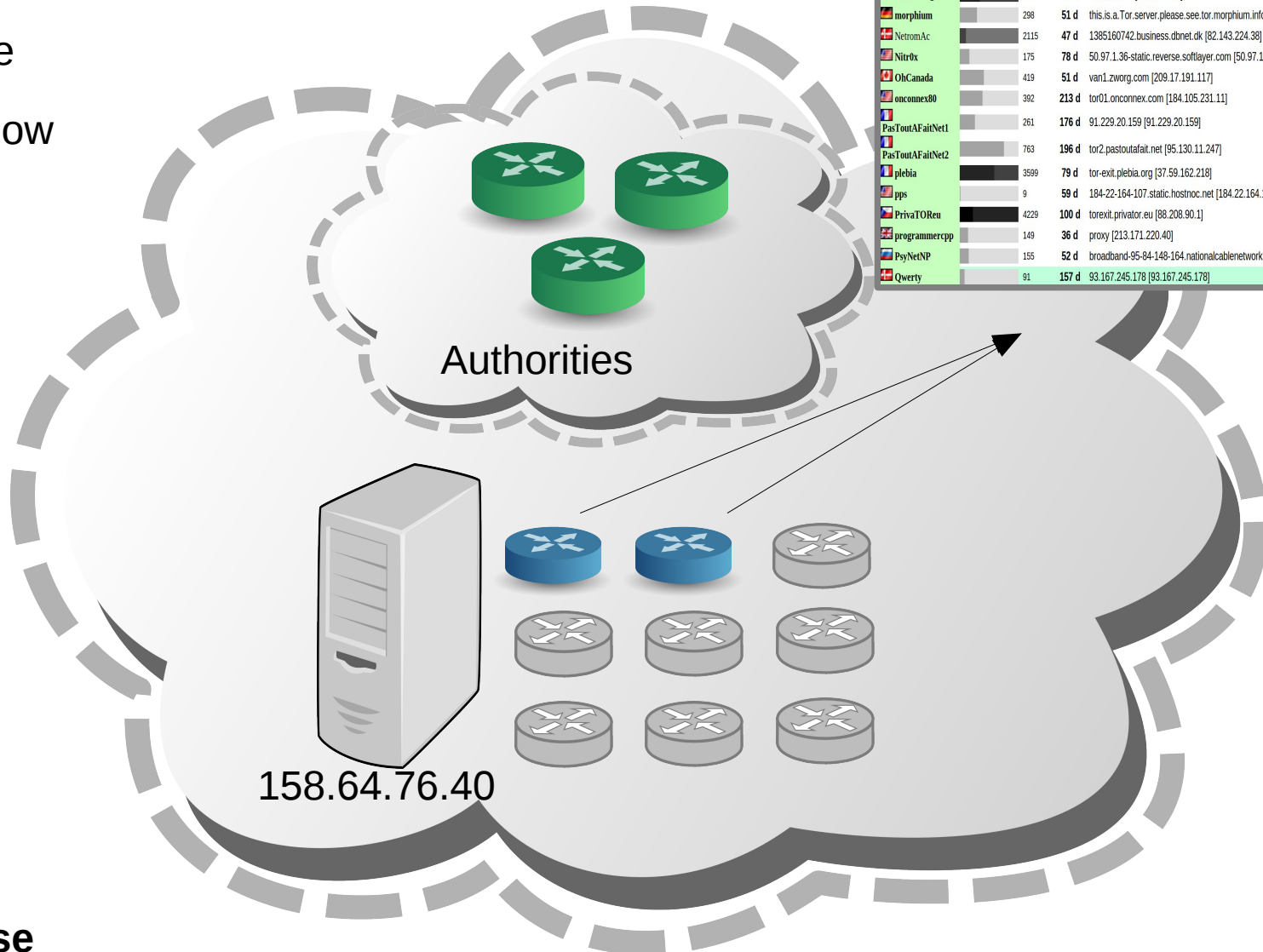


Shadowing

Consensus



Authorities
Internal database



menTor	1737	67 d	55863896.cust.multi.fi [85.134.56.150]	🚧🚧🚧🚧🚧🚧
microshaft	2820	66 d	tor-exit.microshaft.org [208.201.249.3]	🚧🚧🚧🚧🚧🚧
minisausage	3348	35 d	50.7.184.58 [50.7.184.58]	🚧🚧🚧🚧🚧🚧
morphism	298	51 d	this.is.a.Tor.server.please.see.tor.morphism.info [91.143.90.25]	🚧🚧🚧🚧🚧🚧
NetromAc	2115	47 d	1385160742.business.dnnet.dk [82.143.224.38]	🚧🚧🚧🚧🚧🚧
Nitrox	175	78 d	50.97.1.36-static.reverse.softlayer.com [50.97.1.36]	🚧🚧🚧🚧🚧🚧
OhCanada	419	51 d	van1.zworg.com [209.17.191.117]	🚧🚧🚧🚧🚧🚧
onconnex80	392	213 d	tor01.onconnex.com [184.105.231.11]	🚧🚧🚧🚧🚧🚧
PasTouAFaitNet1	261	176 d	91.229.20.159 [91.229.20.159]	🚧🚧🚧🚧🚧🚧
PasTouAFaitNet2	763	196 d	tor2.pastoutafait.net [95.130.11.247]	🚧🚧🚧🚧🚧🚧
plebia	3599	79 d	tor-exit.plebia.org [37.59.162.218]	🚧🚧🚧🚧🚧🚧
pps	9	59 d	184-22-164-107.static.hostnoc.net [184.22.164.107]	🚧🚧🚧🚧🚧🚧
PrivaTOreu	4229	100 d	toexit.privator.eu [88.208.90.1]	🚧🚧🚧🚧🚧🚧
programercpp	149	36 d	proxy [213.171.220.40]	🚧🚧🚧🚧🚧🚧
PsyNetNP	155	52 d	broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]	🚧🚧🚧🚧🚧🚧
Qwerty	91	157 d	93.167.245.178 [93.167.245.178]	🚧🚧🚧🚧🚧🚧

Shadowing

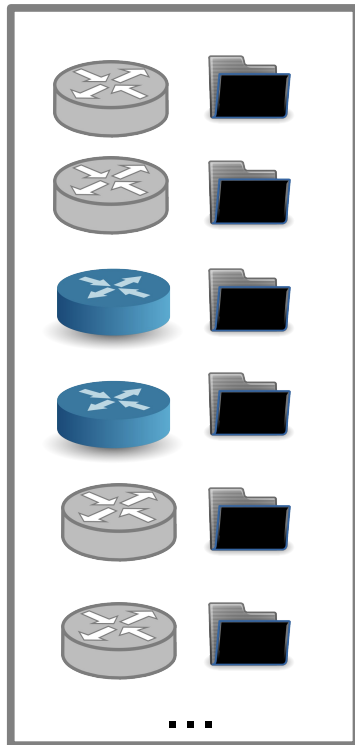
Consensus



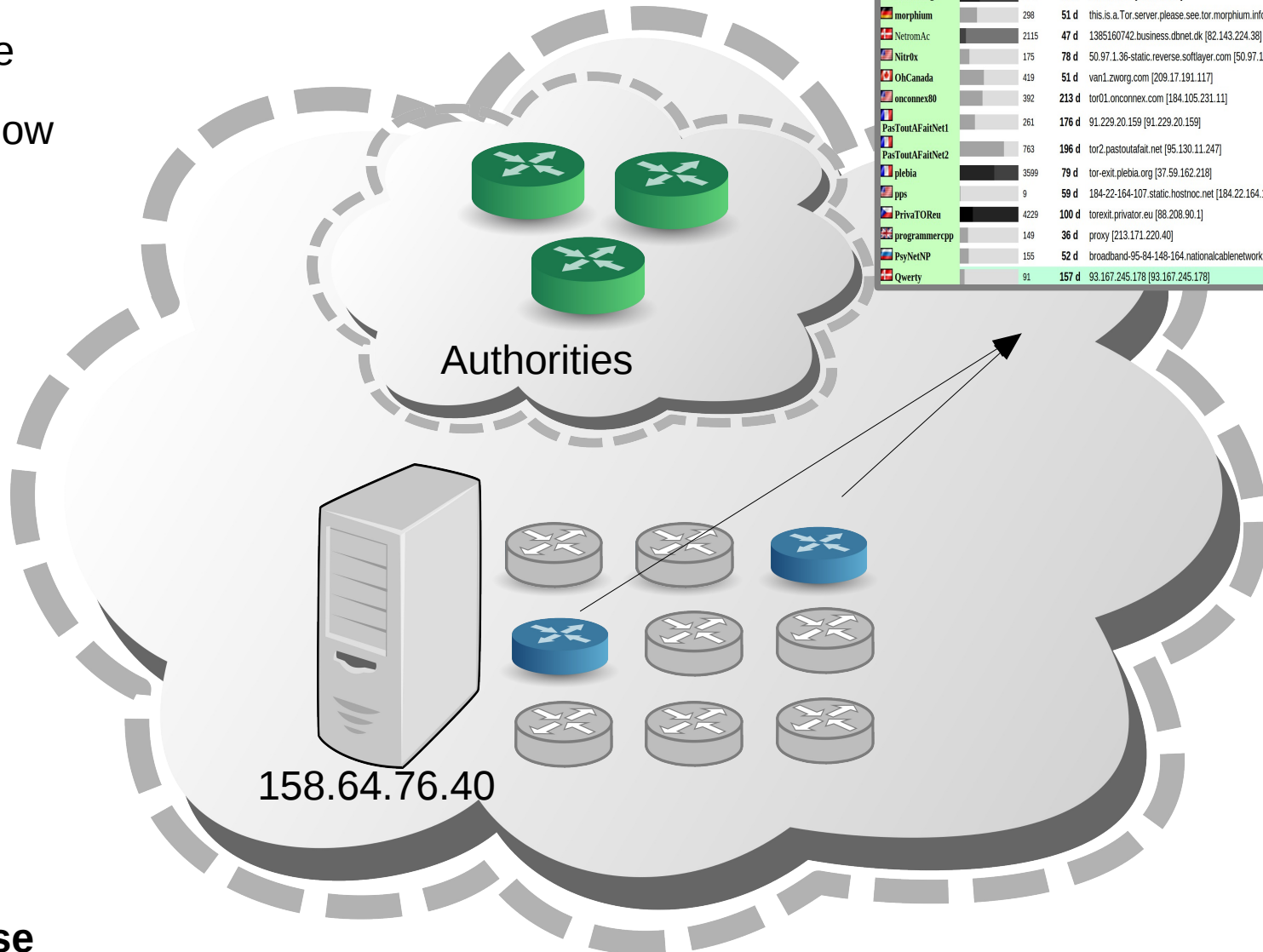
- Active



- Shadow



Authorities
Internal database



menTor	1737	67 d	55863896.cust.multi.fi [85.134.56.150]	🚧🚧🚧🚧🚧🚧
microshaft	2820	66 d	tor-exit.microshaft.org [208.201.249.3]	🚧🚧🚧🚧🚧🚧
minisausage	3348	35 d	50.7.184.58 [50.7.184.58]	🚧🚧🚧🚧🚧🚧
morphism	298	51 d	this.is.a.Tor.server.please.see.tor.morphism.info [91.143.90.25]	🚧🚧🚧🚧🚧🚧
NetromAc	2115	47 d	1385160742.business.dnnet.dk [82.143.224.38]	🚧🚧🚧🚧🚧🚧
Nitrox	175	78 d	50.97.1.36-static.reverse.softlayer.com [50.97.1.36]	🚧🚧🚧🚧🚧🚧
OhCanada	419	51 d	van1.zworg.com [209.17.191.117]	🚧🚧🚧🚧🚧🚧
onconnex80	392	213 d	tor01.onconnex.com [184.105.231.11]	🚧🚧🚧🚧🚧🚧
PasTouAFaitNet1	261	176 d	91.229.20.159 [91.229.20.159]	🚧🚧🚧🚧🚧🚧
PasTouAFaitNet2	763	196 d	tor2.pastoutafait.net [95.130.11.247]	🚧🚧🚧🚧🚧🚧
plebia	3599	79 d	tor-exit.plebia.org [37.59.162.218]	🚧🚧🚧🚧🚧🚧
pps	9	59 d	184-22-164-107.static.hostnoc.net [184.22.164.107]	🚧🚧🚧🚧🚧🚧
PrivaTOreu	4229	100 d	toexit.privator.eu [88.208.90.1]	🚧🚧🚧🚧🚧🚧
programercpp	149	36 d	proxy [213.171.220.40]	🚧🚧🚧🚧🚧🚧
PsyNetNP	155	52 d	broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]	🚧🚧🚧🚧🚧🚧
Qwerty	91	157 d	93.167.245.178 [93.167.245.178]	🚧🚧🚧🚧🚧🚧

Shadowing

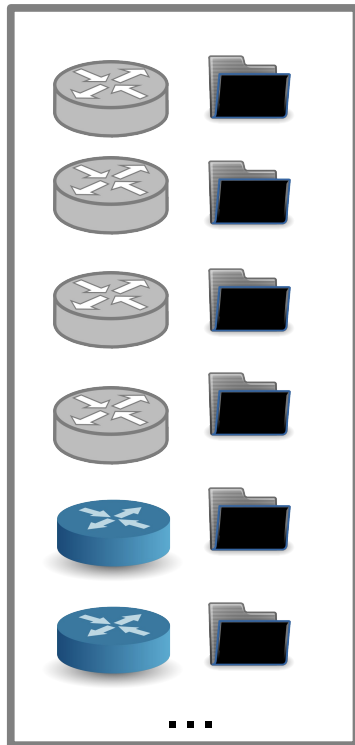
Consensus



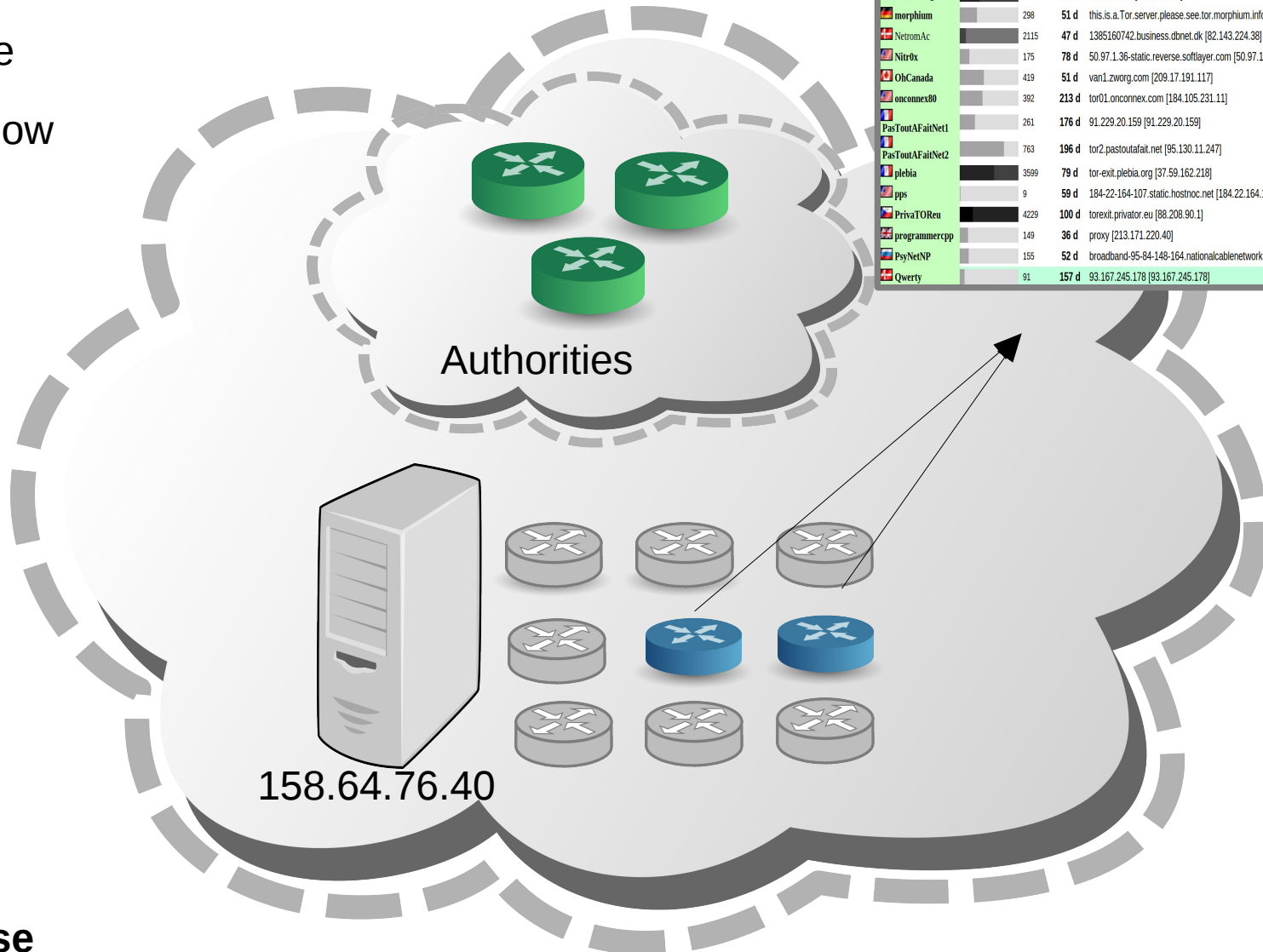
- Active



- Shadow



Authorities
Internal database



menTor	1737	67 d	55863896.cust.multi.fi [85.134.56.150]	🔥🔥🔥🔥🔥🔥
microshaft	2820	66 d	tor-exit.microshaft.org [208.201.249.3]	🔥🔥🔥🔥🔥🔥
minisausage	3348	35 d	50.7.184.58 [50.7.184.58]	🔥🔥🔥🔥🔥🔥
morphism	298	51 d	this.is.a.Tor.server.please.see.tor.morphism.info [91.143.90.25]	🔥🔥🔥🔥🔥🔥
NetromAc	2115	47 d	1385160742.business.dnnet.dk [82.143.224.38]	🔥🔥🔥🔥🔥🔥
Nitrox	175	78 d	50.97.1.36-static.reverse.softlayer.com [50.97.1.36]	🔥🔥🔥🔥🔥🔥
OhCanada	419	51 d	van1.zworg.com [209.17.191.117]	🔥🔥🔥🔥🔥🔥
onconnex80	392	213 d	tor01.onconnex.com [184.105.231.11]	🔥🔥🔥🔥🔥🔥
PasTouAFaitNet1	261	176 d	91.229.20.159 [91.229.20.159]	🔥🔥🔥🔥🔥🔥
PasTouAFaitNet2	763	196 d	tor2.pastoutafait.net [95.130.11.247]	🔥🔥🔥🔥🔥🔥
plebia	3599	79 d	tor-exit.plebia.org [37.59.162.218]	🔥🔥🔥🔥🔥🔥
pps	9	59 d	184-22-164-107.static.hostnoc.net [184.22.164.107]	🔥🔥🔥🔥🔥🔥
PrivaTOreu	4229	100 d	forexit.privator.eu [88.208.90.1]	🔥🔥🔥🔥🔥🔥
programmerc	149	36 d	proxy [213.171.220.40]	🔥🔥🔥🔥🔥🔥
PsyNetNP	155	52 d	broadband-95-84-148-164.nationalcablenetworks.ru [95.84.148.164]	🔥🔥🔥🔥🔥🔥
Qwerty	91	157 d	93.167.245.178 [93.167.245.178]	🔥🔥🔥🔥🔥🔥

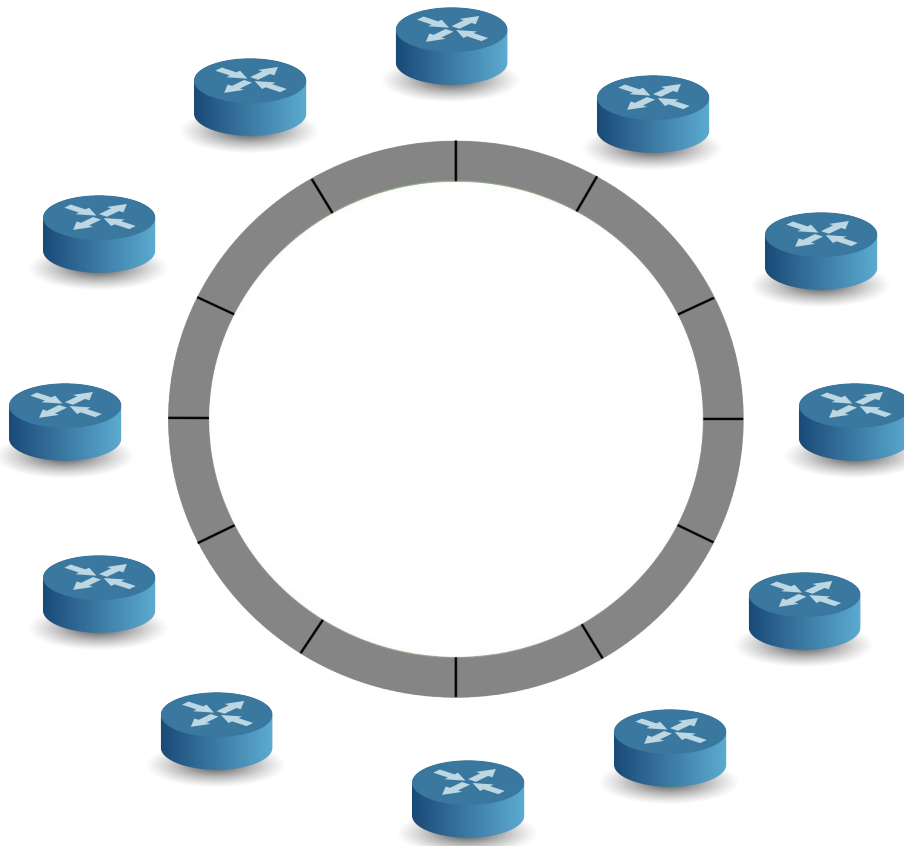
Collecting onion addresses



- Active



- Shadow



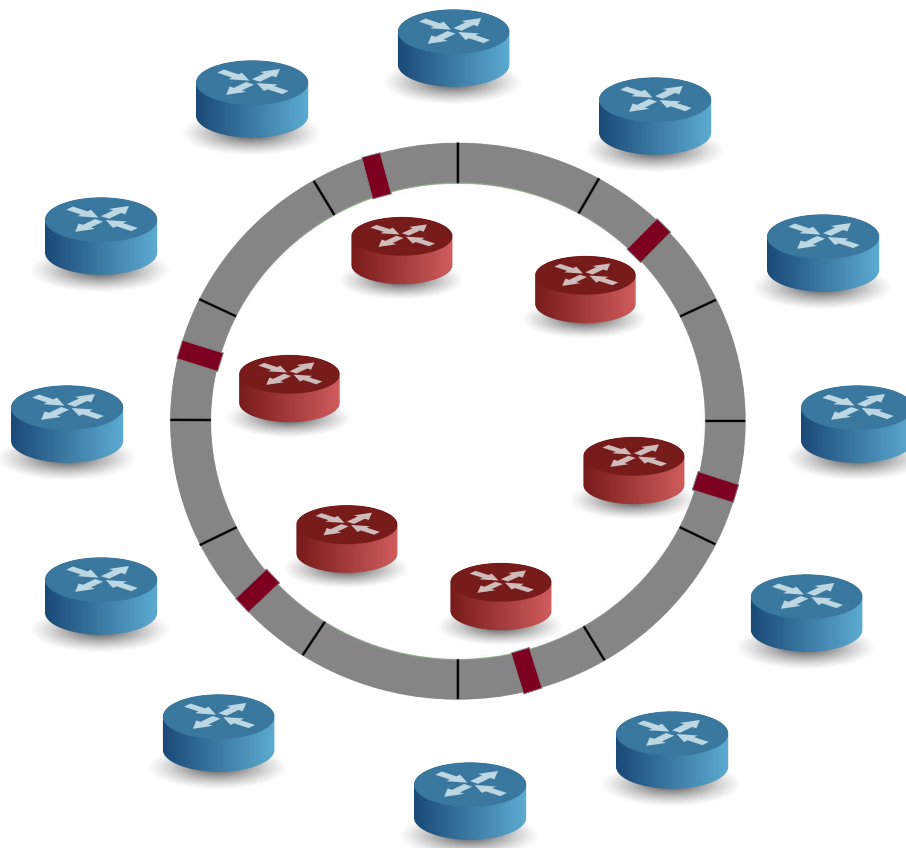
Collecting onion addresses



- Active

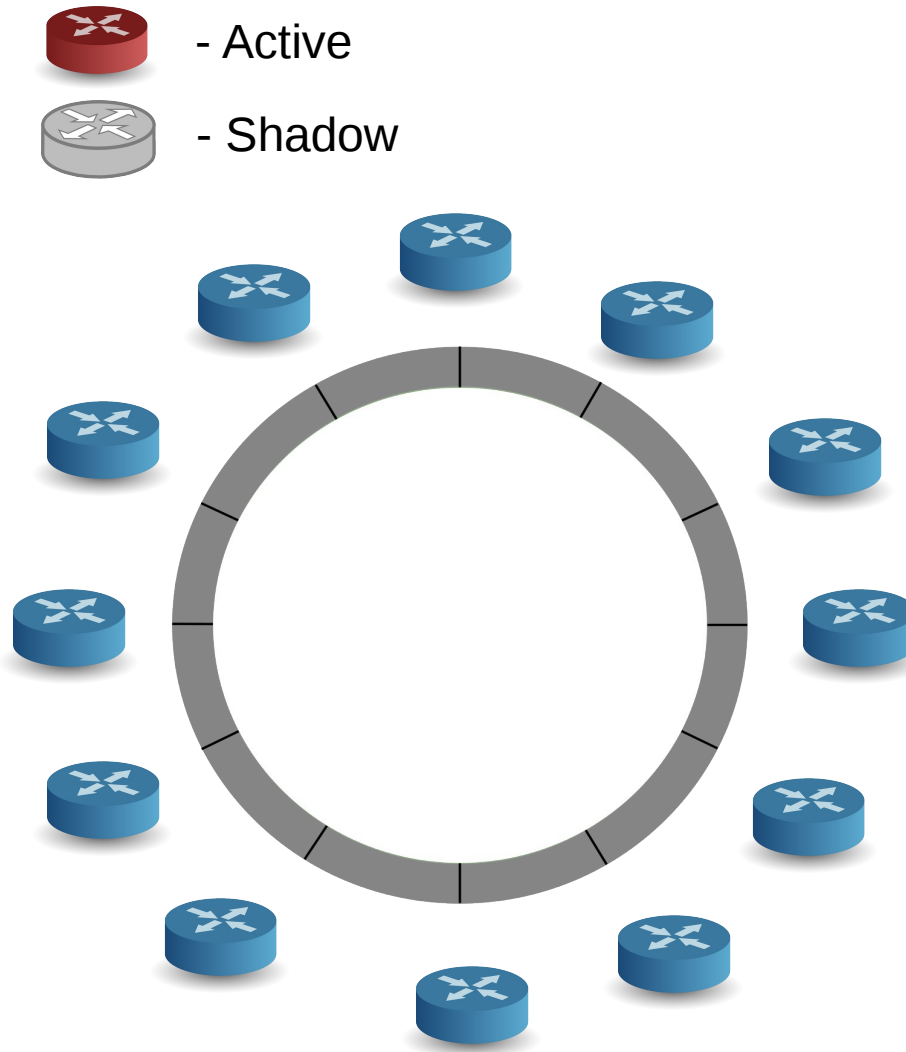


- Shadow



- Naive approach will require ~350 IP addresses.

Collecting onion addresses



- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.

Collecting onion addresses



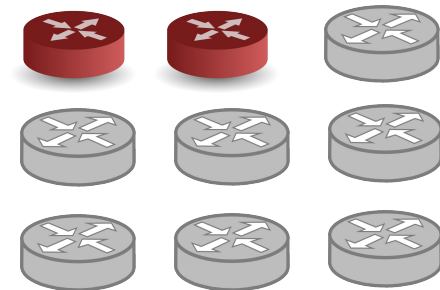
- Active



- Shadow



- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.



158.64.76.40

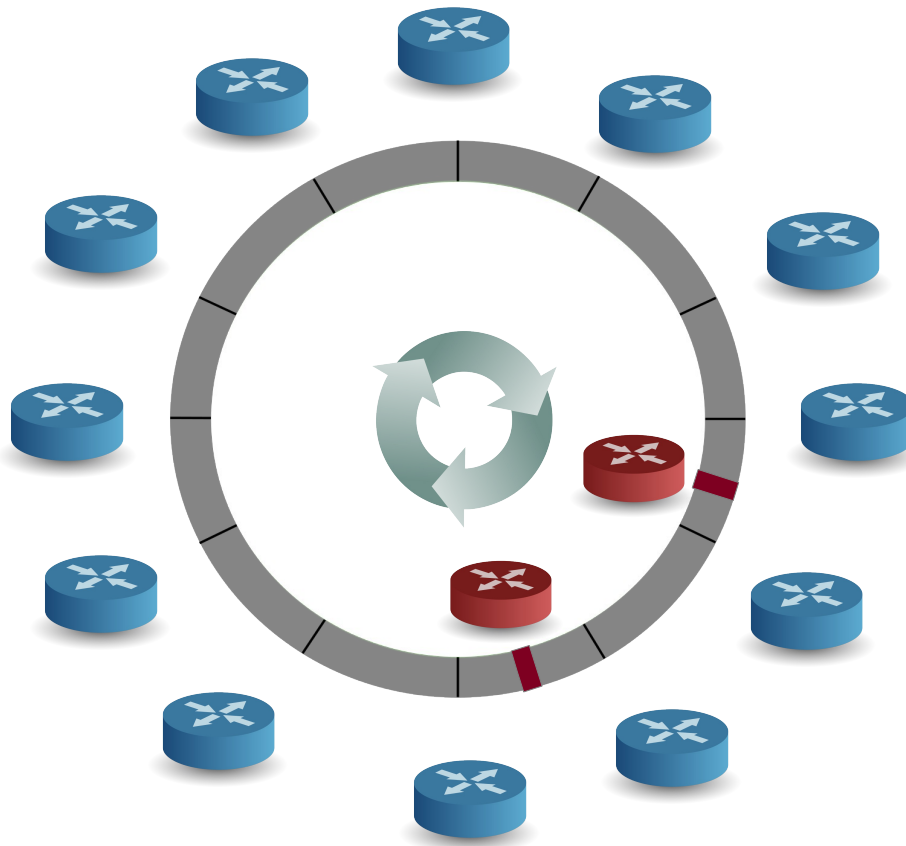
Collecting onion addresses



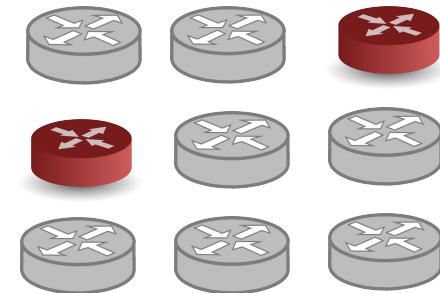
- Active



- Shadow



- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.



158.64.76.40

Collecting onion addresses



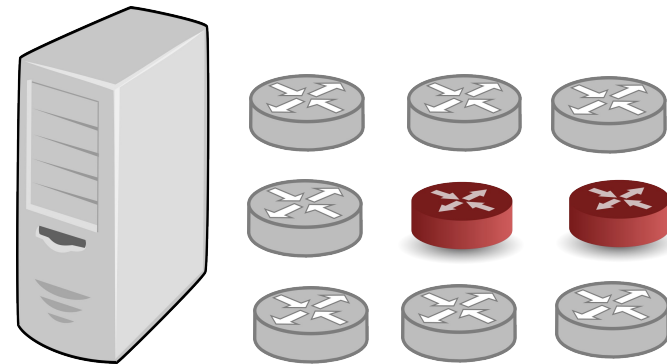
- Active



- Shadow



- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.



158.64.76.40

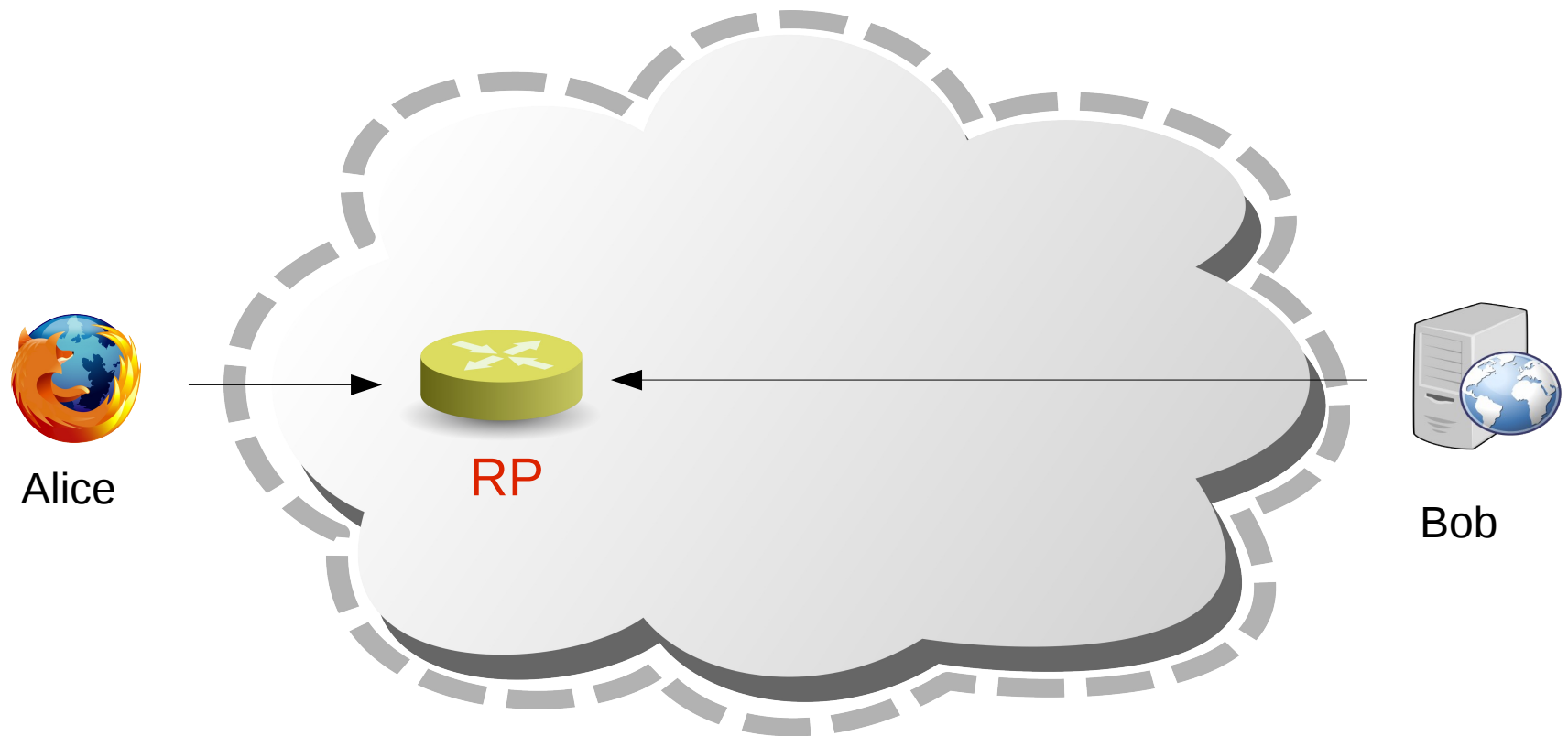
Harvest results

- We used 58 IP addresses from Amazon EC2 and spent 57 USD
- We collected 39824 unique onion addresses in 49 hours (on hidden wikis one can find ~2500 addresses only)
- Some interesting note: 12 onion addresses in the form `silkroad*****.onion`.

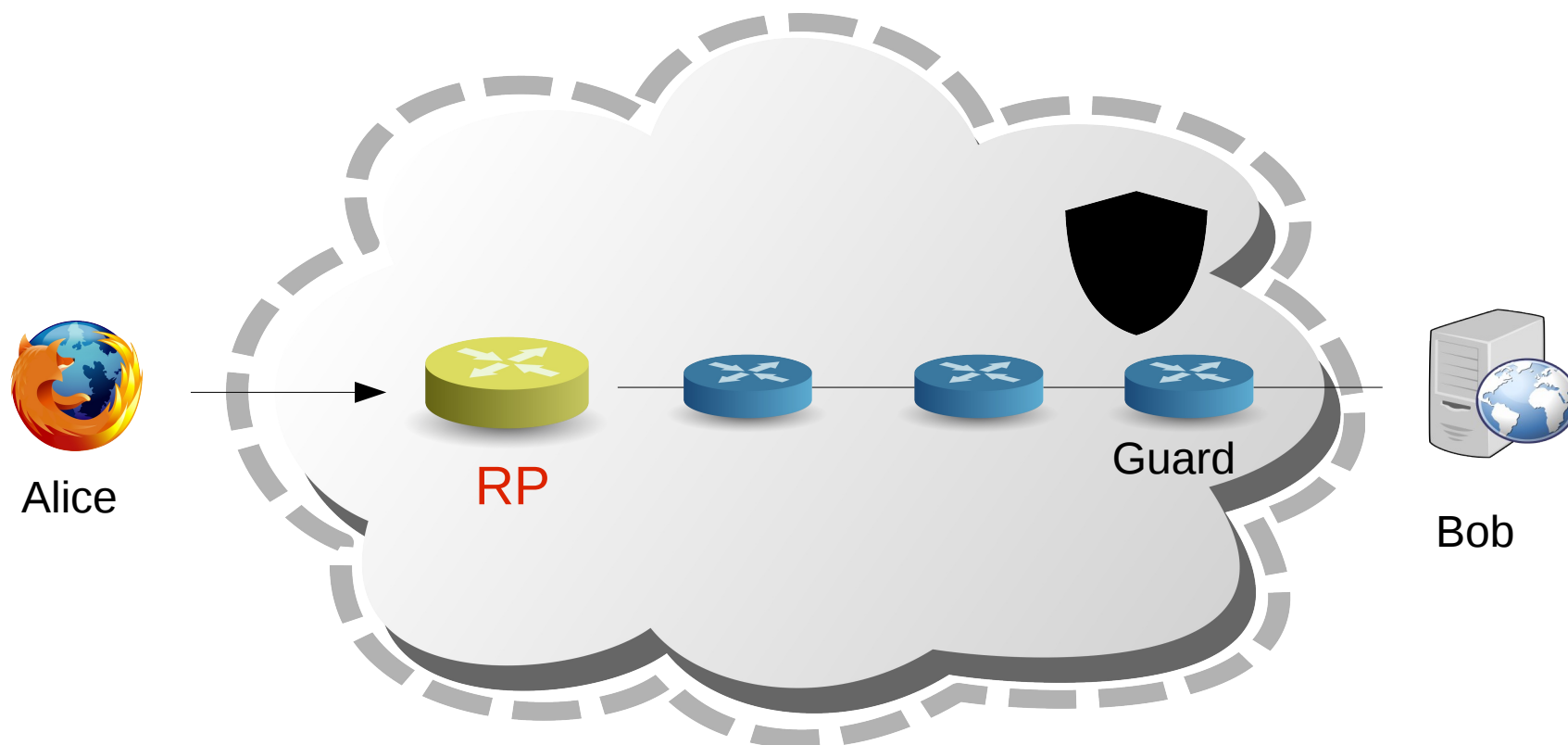
Overview

- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- **Revealing the guards.**
- **Opportunistic deanonymisation.**

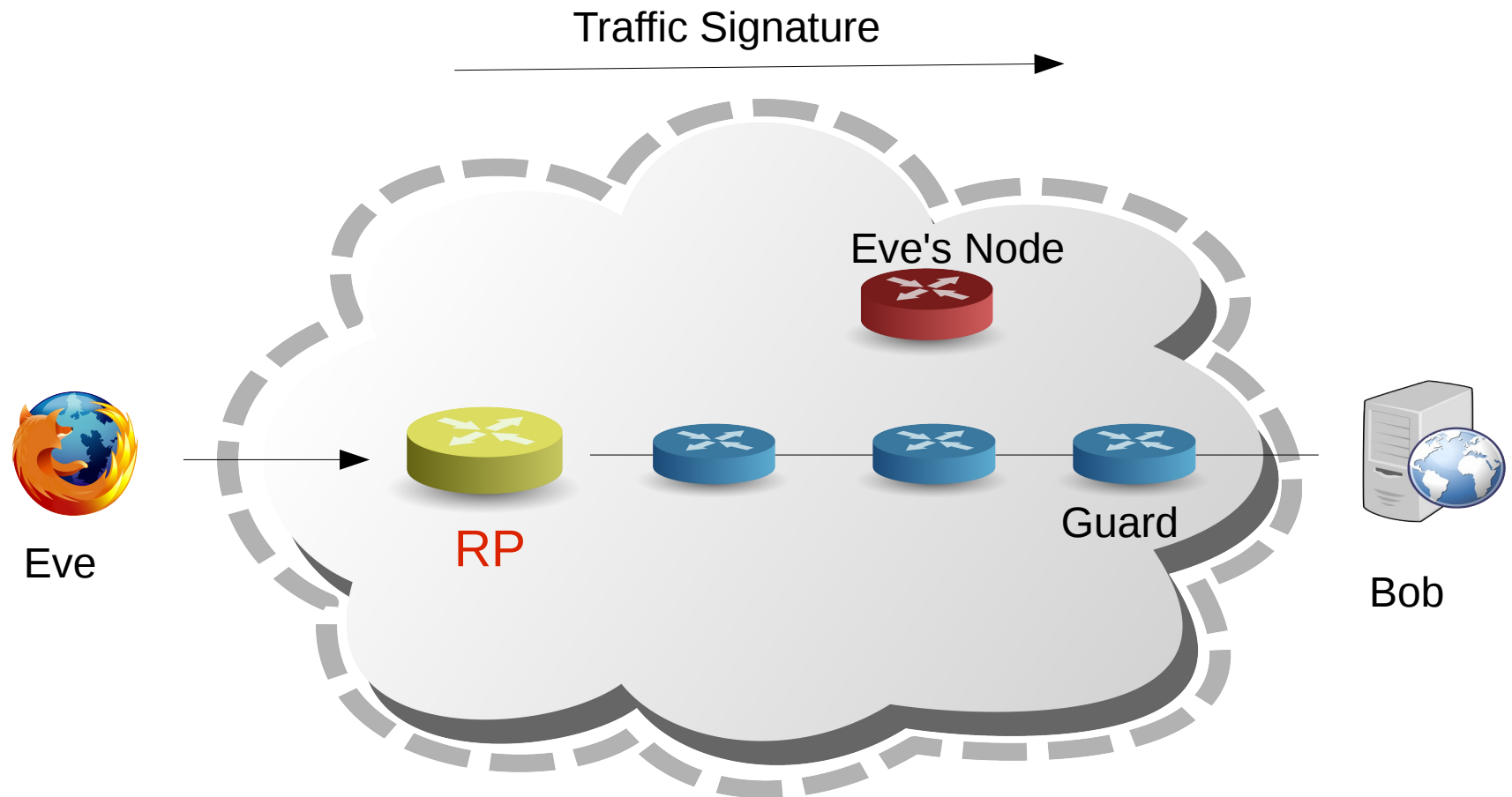
Revealing Guard Nodes



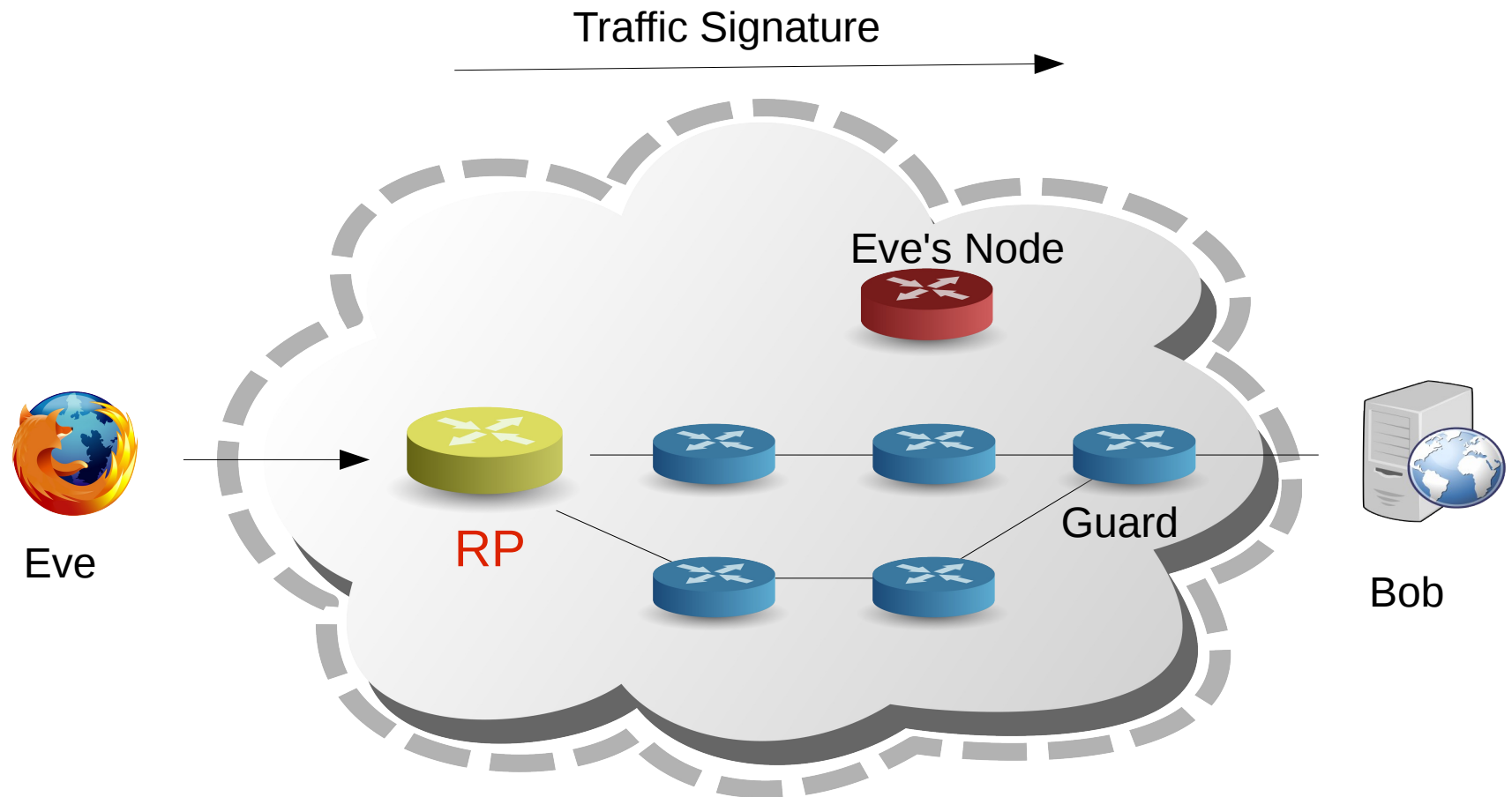
Revealing Guard Nodes



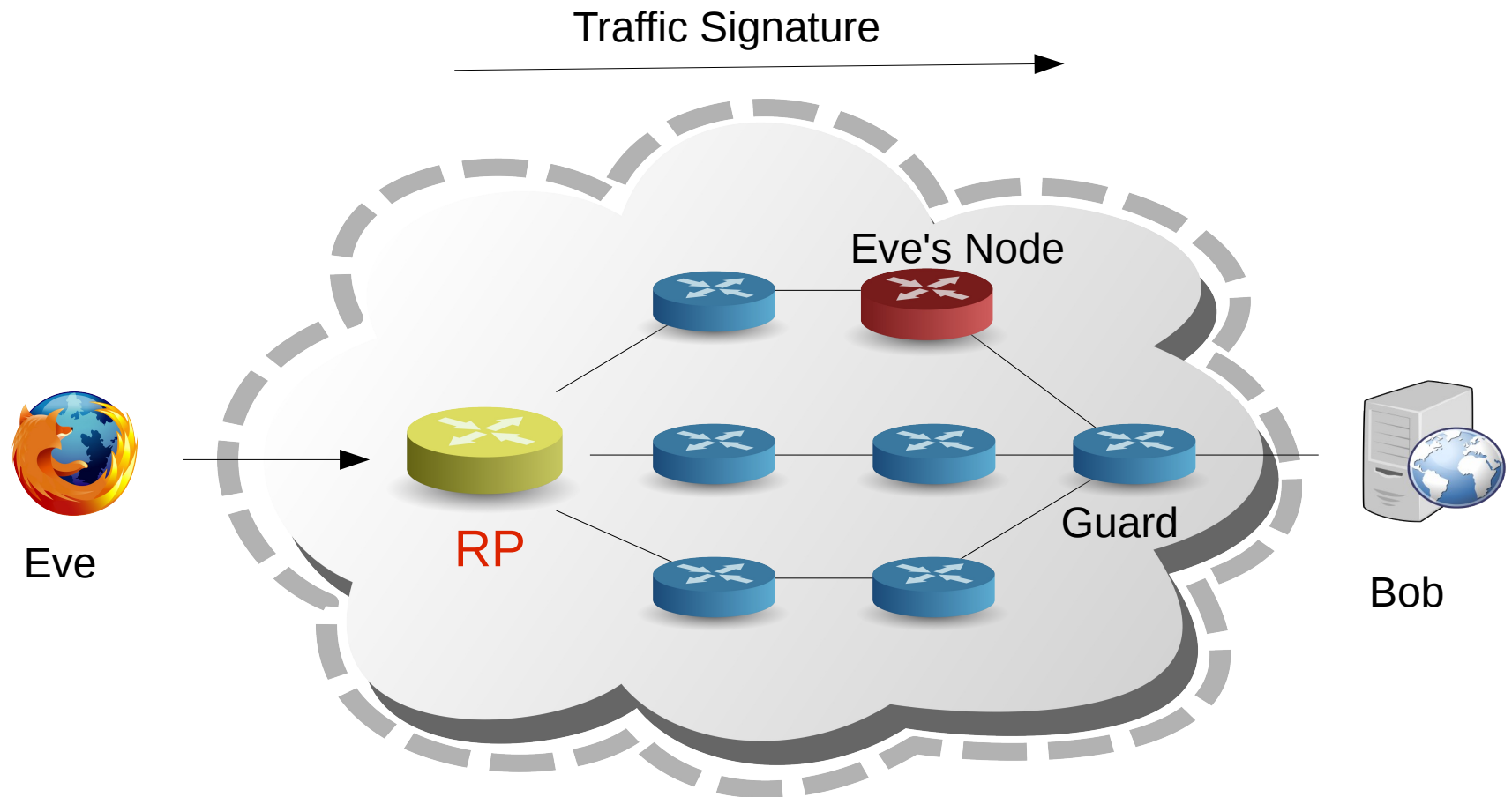
Revealing Guard Nodes



Revealing Guard Nodes

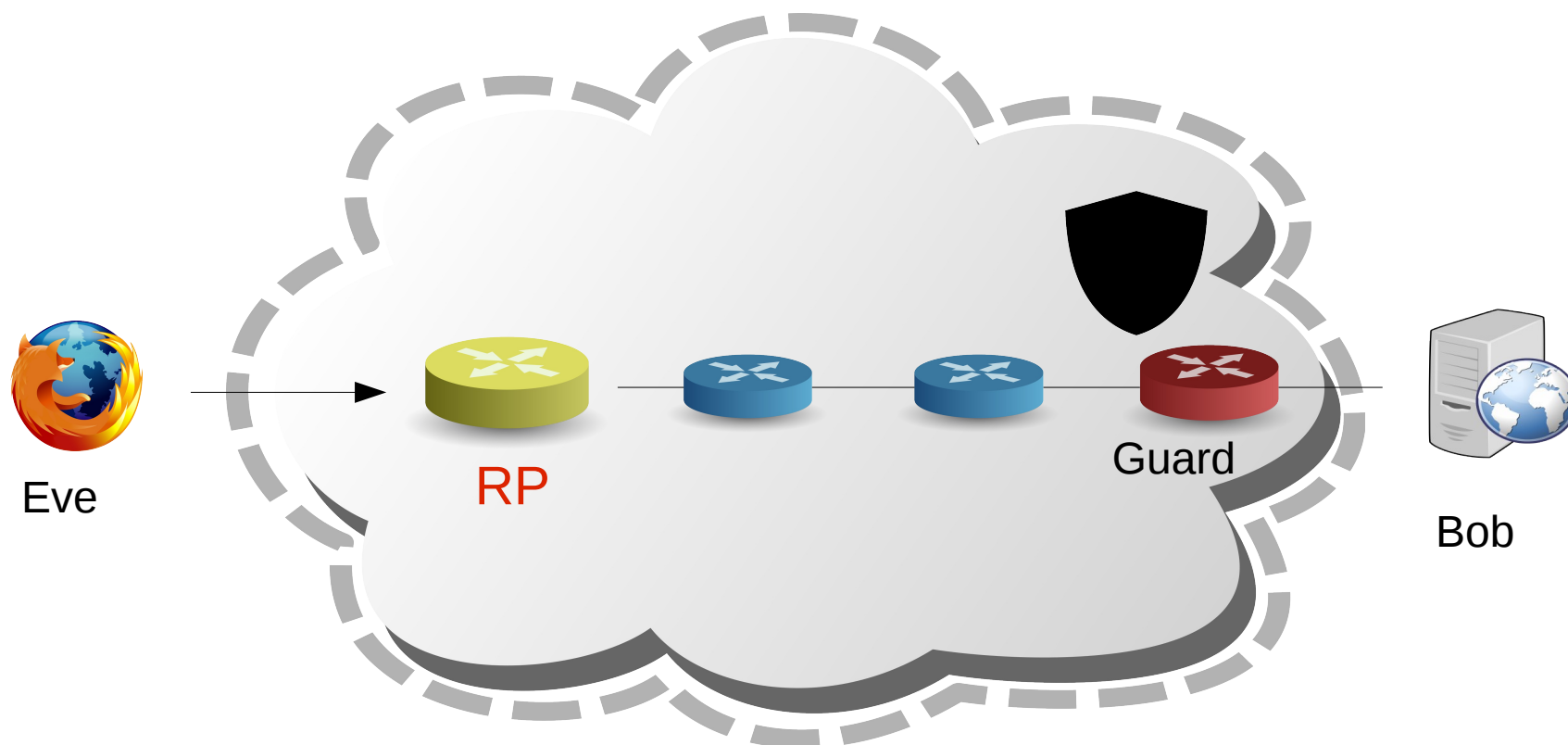


Revealing Guard Nodes

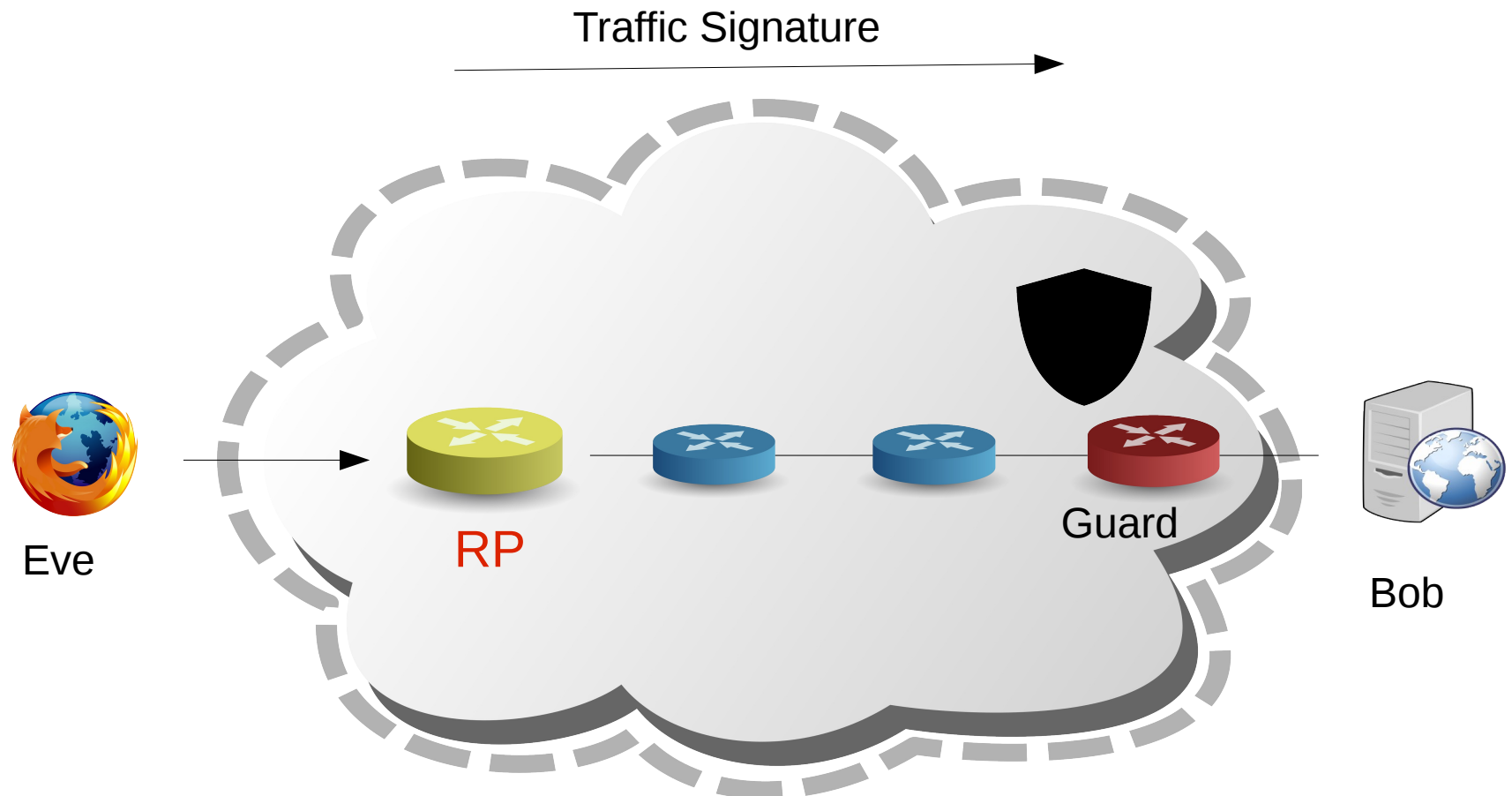


~40 minutes to reveal the guard nodes for a 5Mb/s node

Opportunistic deanonymisation



Opportunistic deanonymisation



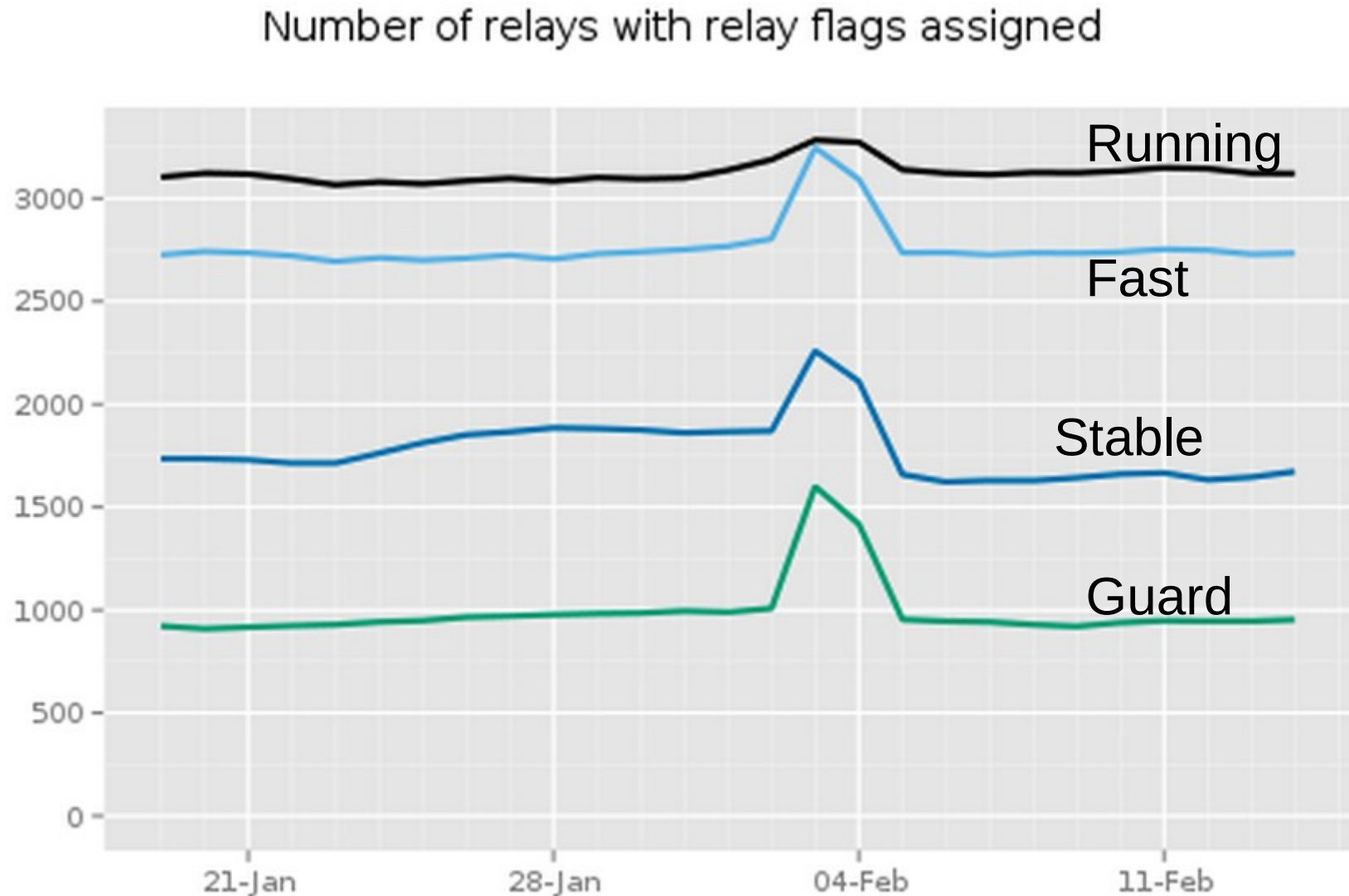
How long does it take to become
a Guard of a hidden service?

Opportunistic deanonymisation




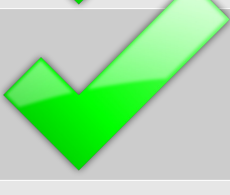

- Rent a server for 60 USD per month => 0.6% probability to be chosen as a Guard.
- Deanonymisation **~150 hidden services per month** (for **60 USD** per month)
- By running 23 such servers, the probability to deanonymize **any** long-running **hidden service** within **8 months** is **99%**. (~11 000 USD total).

Side effect (flag assignment)

- Large number of shadow relays with bw ≤ 1 accelerated flag assignment.



Conclusions

Tracking	
Denial of Service	
Collecting onion addresses	
Revealing Guard Nodes	
Deanonymisation	<ul style="list-style-type: none">• 150 addresses per month (60 USD)• Any HS (8 months+11000 USD) 

Support slide 1

- Triggered
 - #8243: Getting the HSDir flag should require more effort
 - #8243: Getting the HSDir flag should require more effort
- Related
 - Changing of the Guards: A Framework for Understanding and Improving Entry Guard Selection in Tor", WPES 2012
 - #8240: Raise our guard rotation period
(patch to raise it to 9.5 month still pending)

Support slide 2

- Not included into the presentation
 - Finding guard nodes using topological properties
 - Bandwidth inflation