

Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization

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

May 20, 2013

Overview

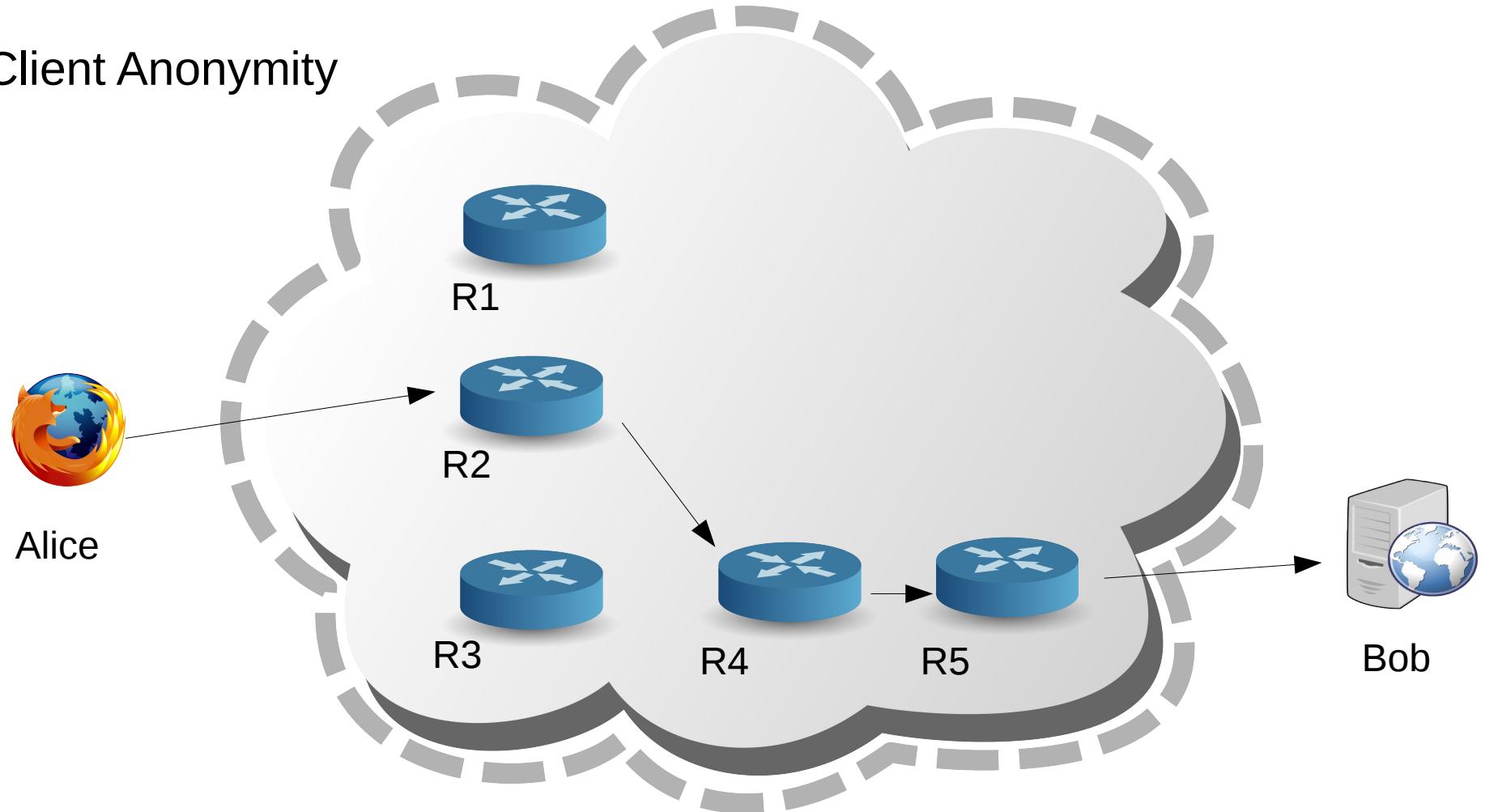
- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- Harvesting onion addresses.
- Revealing the guards.
- Opportunistic deanonymisation.

Overview

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

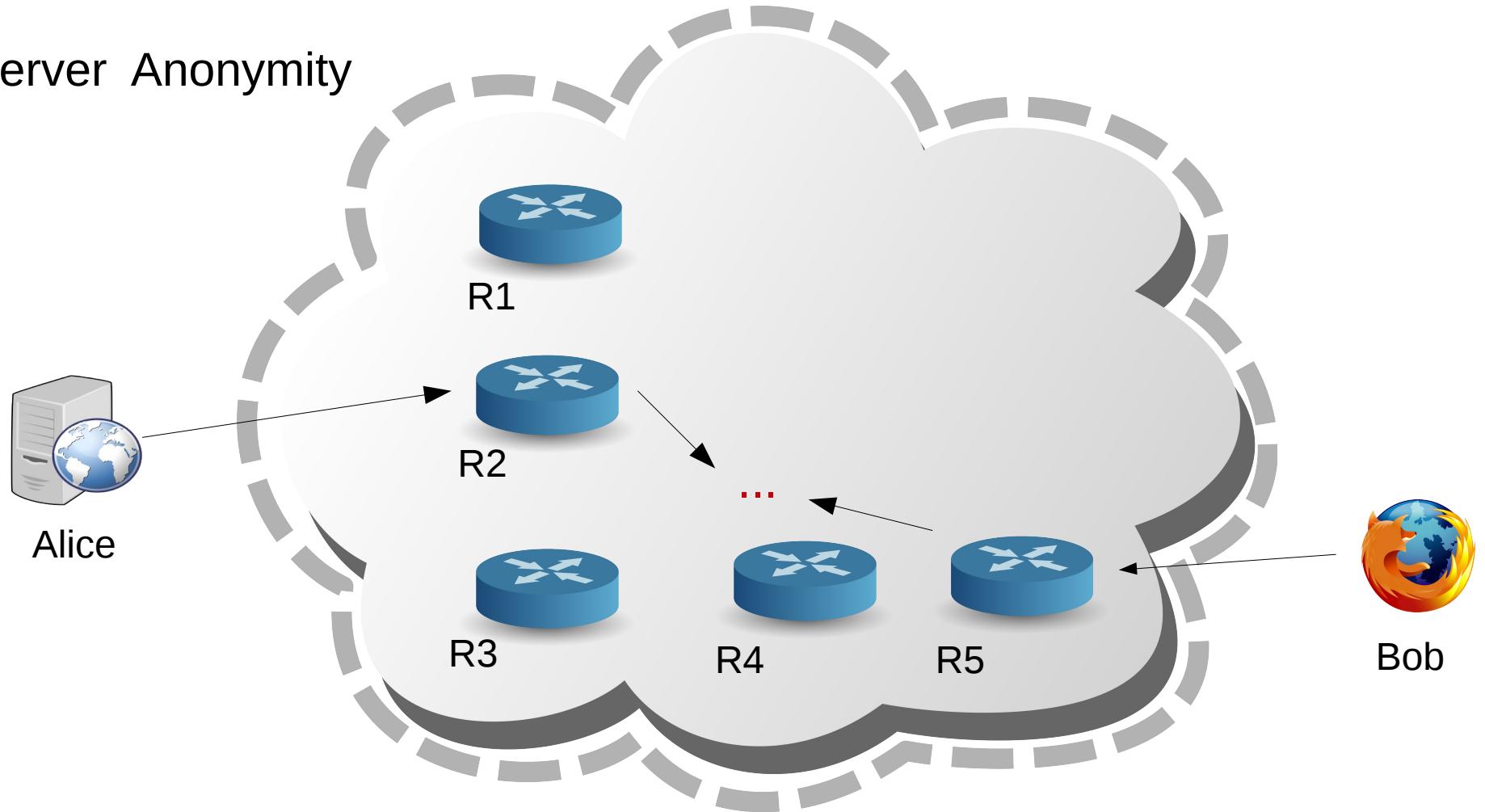
Tor anonymity network

Client Anonymity

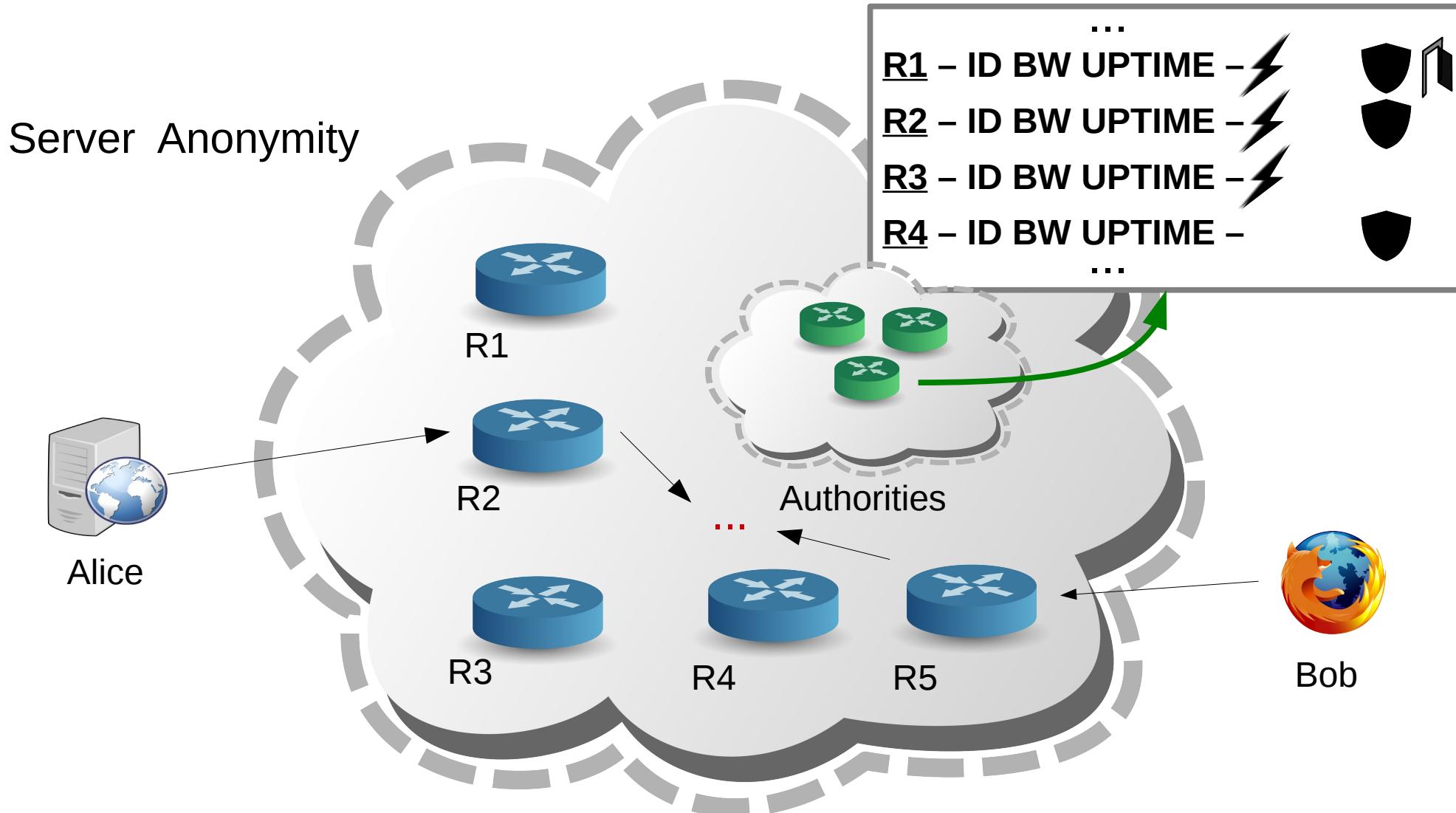


Tor anonymity network

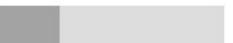
Server Anonymity



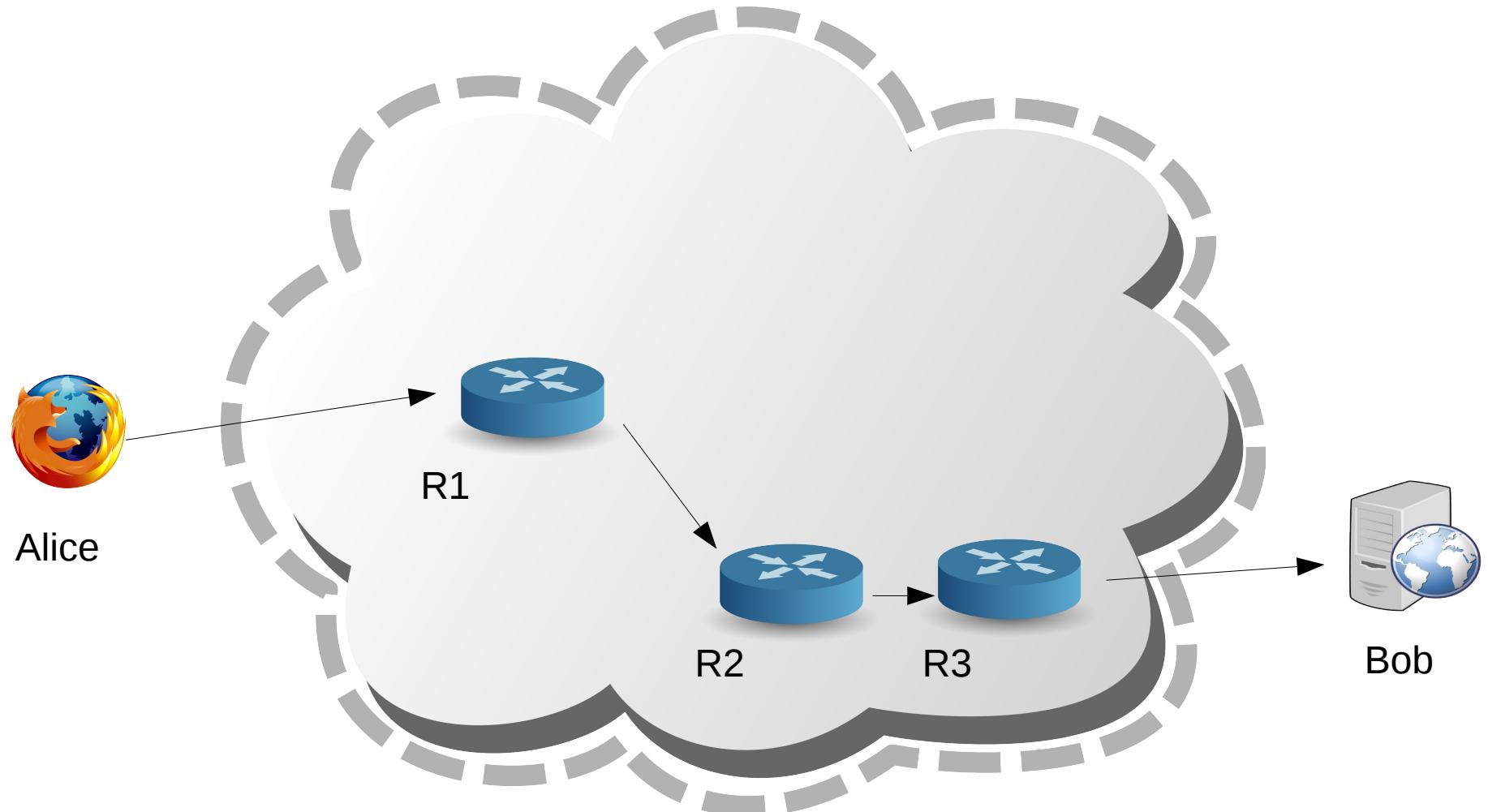
Tor anonymity network



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]	    		

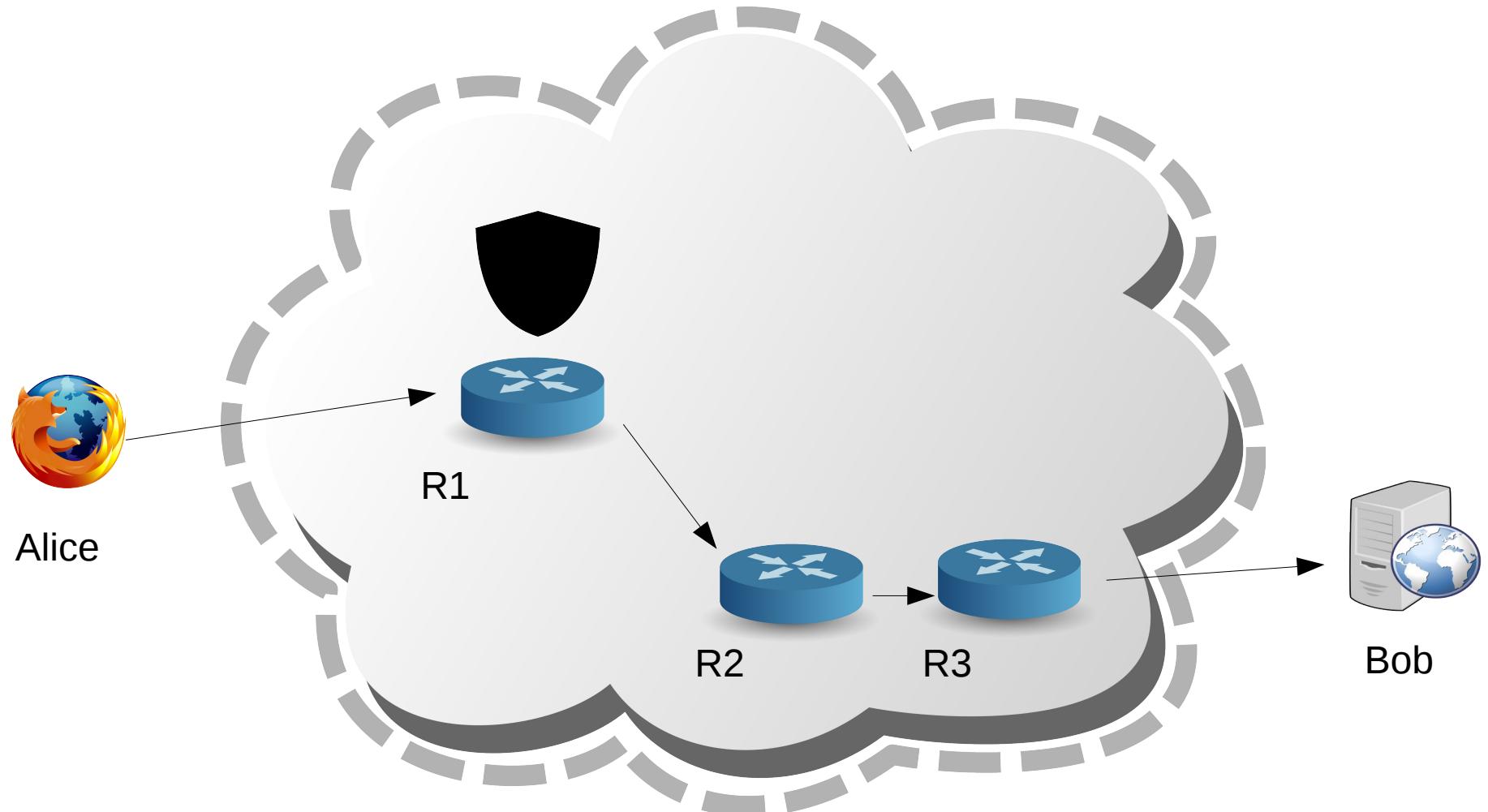
Guards



Guard = high uptime + high bandwidth

Every client has 3 Guard nodes

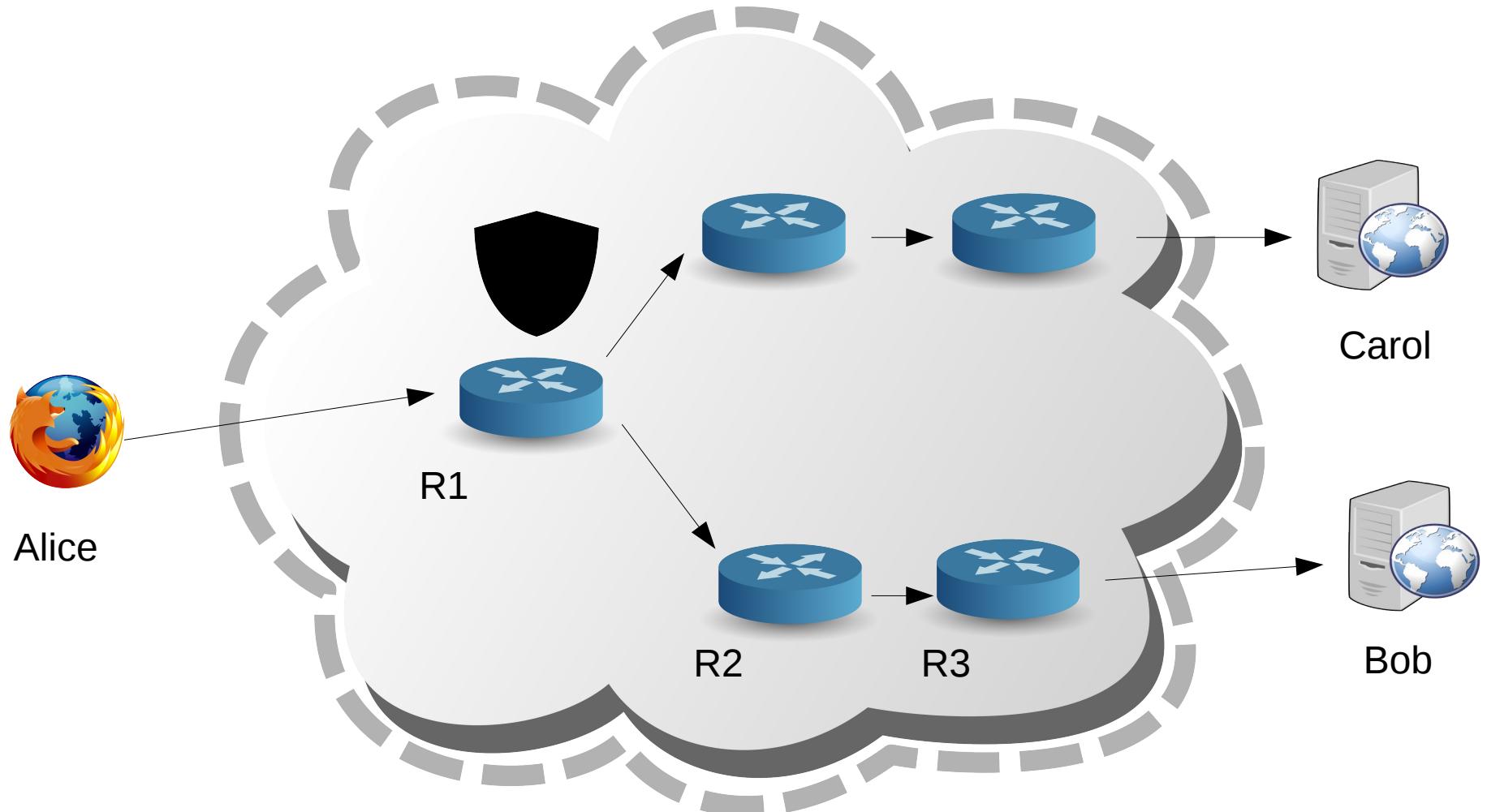
Guards



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

In Wikile

U.K. (2008)
contacts li

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

China (200

Examples of Tor HS



Public Library of US Diplomatic 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, !bang syntax and lots of other goodies.

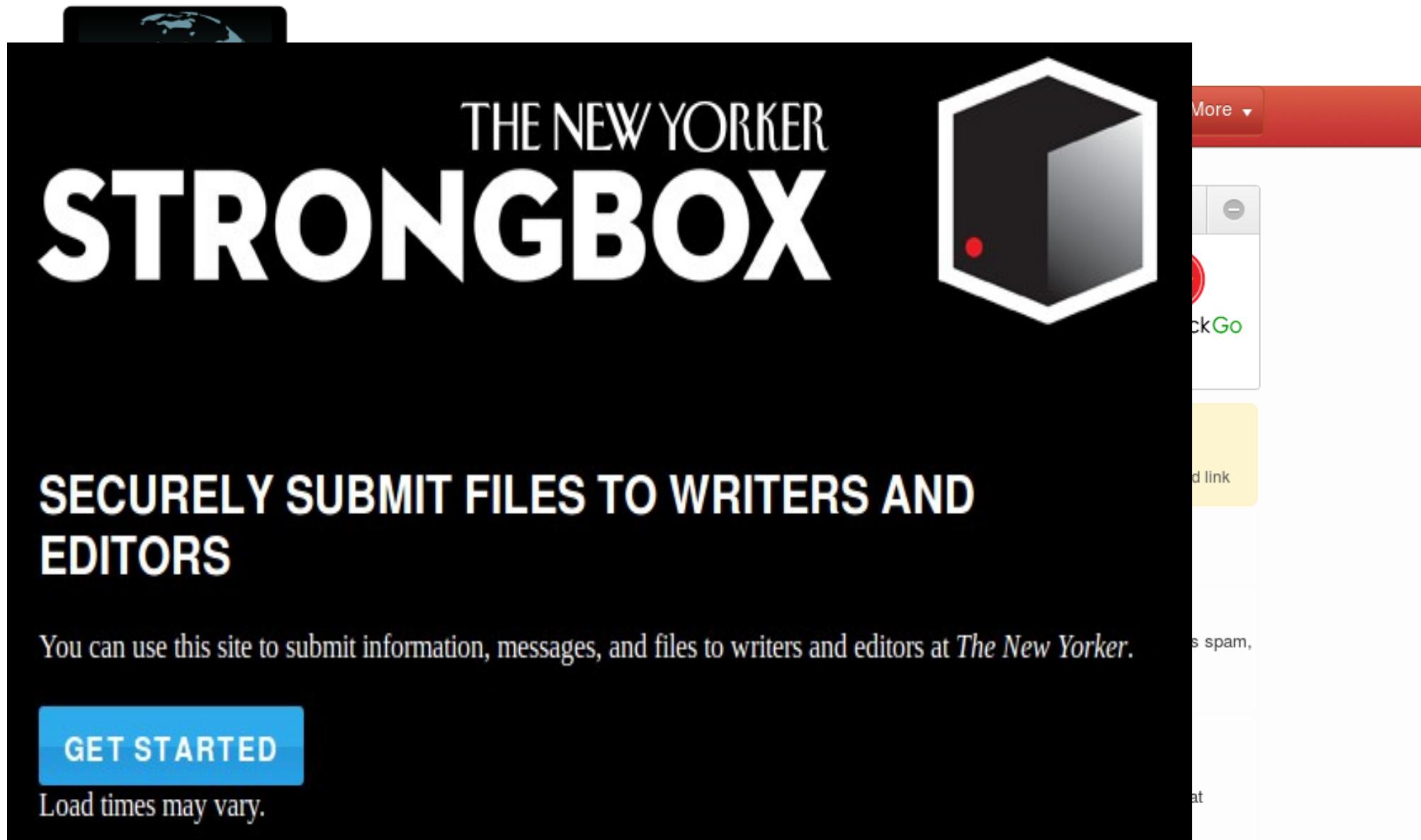
crunchbase.com/company/duck-duck-go More from crunchbase.com ▶

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 dark-themed website for "THE NEW YORKER STRONGBOX". At the top, the "THE NEW YORKER" logo is partially visible above a large, bold "STRONGBOX" text. To the right of the text is a 3D-style hexagonal icon with a small red dot on its front face. Below the main title, the text "SECURELY SUBMIT FILES TO WRITERS AND EDITORS" is displayed in large, white, sans-serif capital letters. A blue button labeled "GET STARTED" is located at the bottom left. At the very bottom, a small note says "Load times may vary." The right side of the image shows a portion of a web browser interface with a red "More" button, a search bar with a minus sign, and a "click Go" button.

THE NEW YORKER

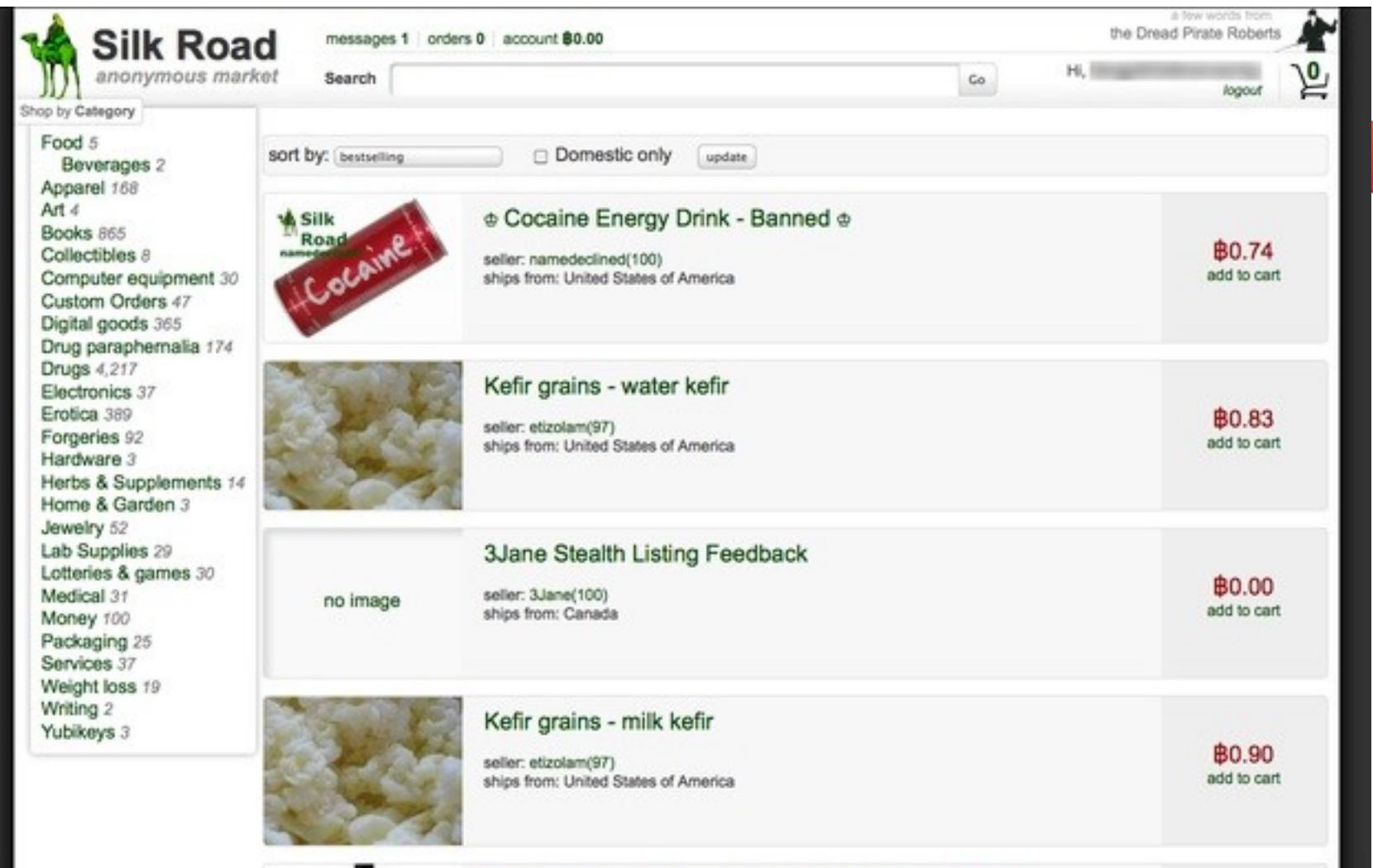
STRONGBOX

SECURELY SUBMIT FILES TO WRITERS AND EDITORS

GET STARTED

Load times may vary.

Examples of Tor HS



The screenshot shows the Silk Road anonymous market interface. On the left, a sidebar lists categories: Food (5), Beverages (2), Apparel (168), Art (4), Books (865), Collectibles (8), Computer equipment (30), Custom Orders (47), Digital goods (365), Drug paraphernalia (174), Drugs (4,217), Electronics (37), Erotica (389), Forgeries (92), Hardware (3), Herbs & Supplements (14), Home & Garden (3), Jewelry (52), Lab Supplies (29), Lotteries & games (30), Medical (31), Money (100), Packaging (25), Services (37), Weight loss (19), Writing (2), and Yubikeys (3). The main content area displays four product listings: 1. Cocaine Energy Drink - Banned (seller: namedeclined(100), \$0.74). 2. Kefir grains - water kefir (seller: etizolam(97), \$0.83). 3. 3Jane Stealth Listing Feedback (seller: 3Jane(100), \$0.00). 4. Kefir grains - milk kefir (seller: etizolam(97), \$0.90). The Silk Road logo, featuring a green camel, is visible in the top left of the main area. The top right shows a user profile with a message count of 1, order count of 0, and account balance of \$0.00. A search bar and a 'Go' button are also present.

ST
SECURE
EDITOR

You can use this

GET STARTED

Load times may vary.

messages 1 | orders 0 | account \$0.00

Search Go

Hi, [redacted] [logout](#)

Shop by Category

- Food 5
- Beverages 2
- Apparel 168
- Art 4
- Books 865
- Collectibles 8
- Computer equipment 30
- Custom Orders 47
- Digital goods 365
- Drug paraphernalia 174
- Drugs 4,217
- Electronics 37
- Erotica 389
- Forgeries 92
- Hardware 3
- Herbs & Supplements 14
- Home & Garden 3
- Jewelry 52
- Lab Supplies 29
- Lotteries & games 30
- Medical 31
- Money 100
- Packaging 25
- Services 37
- Weight loss 19
- Writing 2
- Yubikeys 3

sort by: bestselling Domestic only

 **Cocaine Energy Drink - Banned**
seller: namedeclined(100)
ships from: United States of America

 **Kefir grains - water kefir**
seller: etizolam(97)
ships from: United States of America

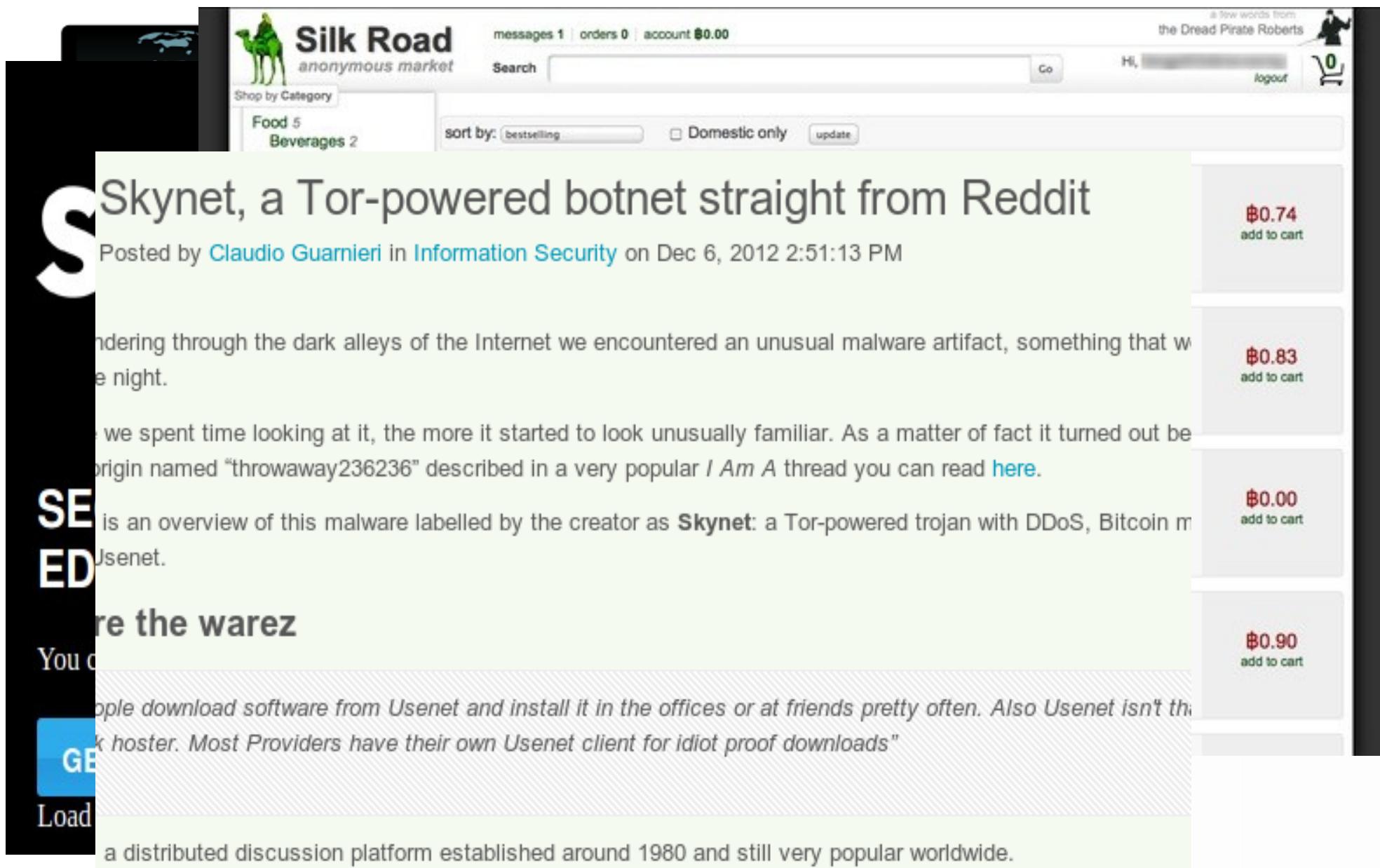
 **3Jane Stealth Listing Feedback**
no image
seller: 3Jane(100)
ships from: Canada

 **Kefir grains - milk kefir**
seller: etizolam(97)
ships from: United States of America

 **Red Wine Red Wine Dose Offdry Bottiglie 75cl**

wired.com/business/2011/01/duckduckgo-google-privacy/ More from wired.com >

Examples of Tor HS



The screenshot shows a news article on a website that appears to be a dark web market. The header of the news article is "Skynet, a Tor-powered botnet straight from Reddit". The article is posted by Claudio Guarnieri in Information Security on Dec 6, 2012 2:51:13 PM. The text of the article discusses the discovery of Skynet malware, which is described as a Tor-powered trojan with DDoS, Bitcoin mining, and Usenet download capabilities. The article also mentions that Usenet is a distributed discussion platform established around 1980 and still very popular worldwide.

Skynet, a Tor-powered botnet straight from Reddit

Posted by Claudio Guarnieri in Information Security on Dec 6, 2012 2:51:13 PM

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

The 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](#).

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

ED

re the warez

You

GE

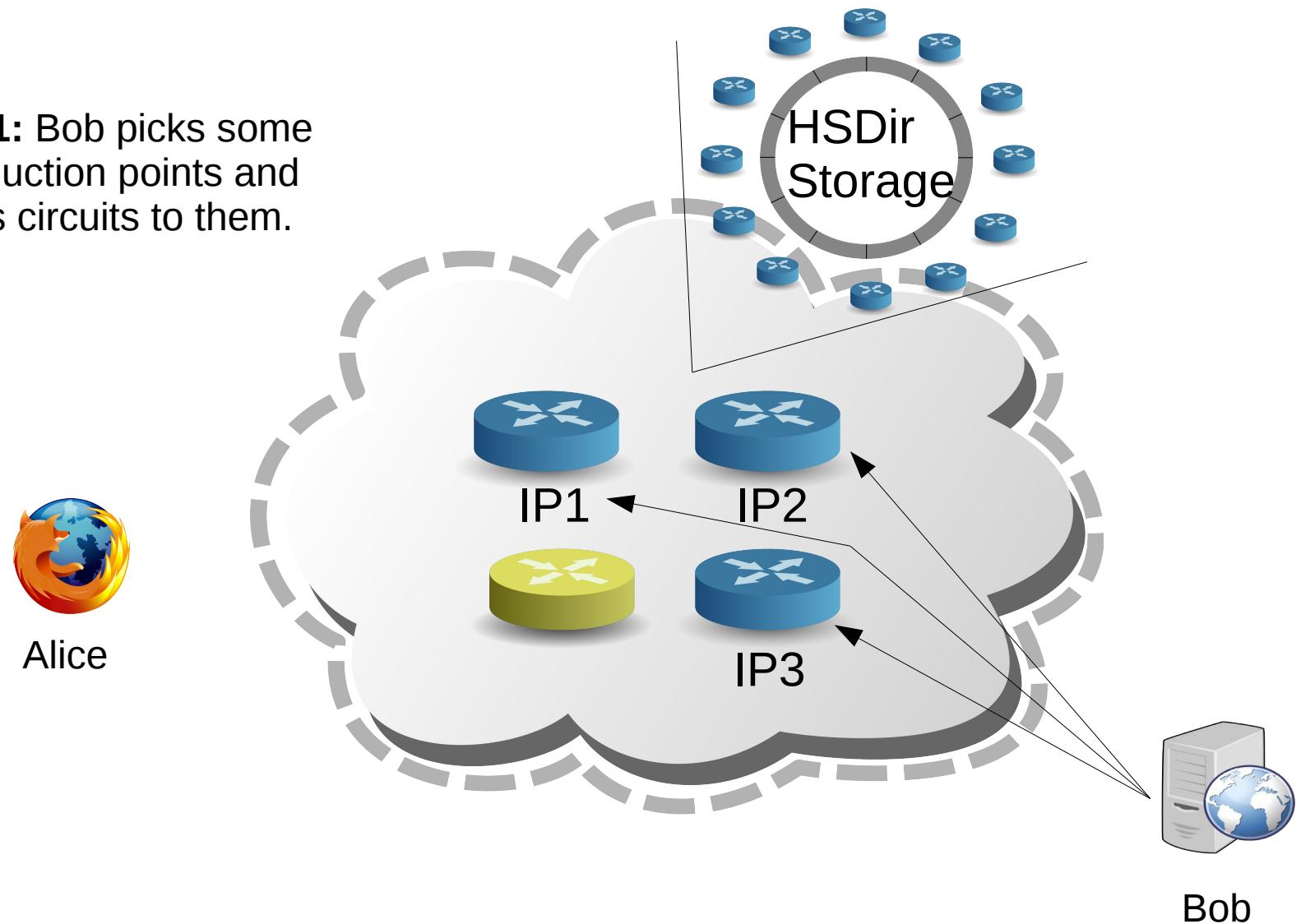
Load

People download software from Usenet and install it in the offices or at friends pretty often. Also Usenet isn't the 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.

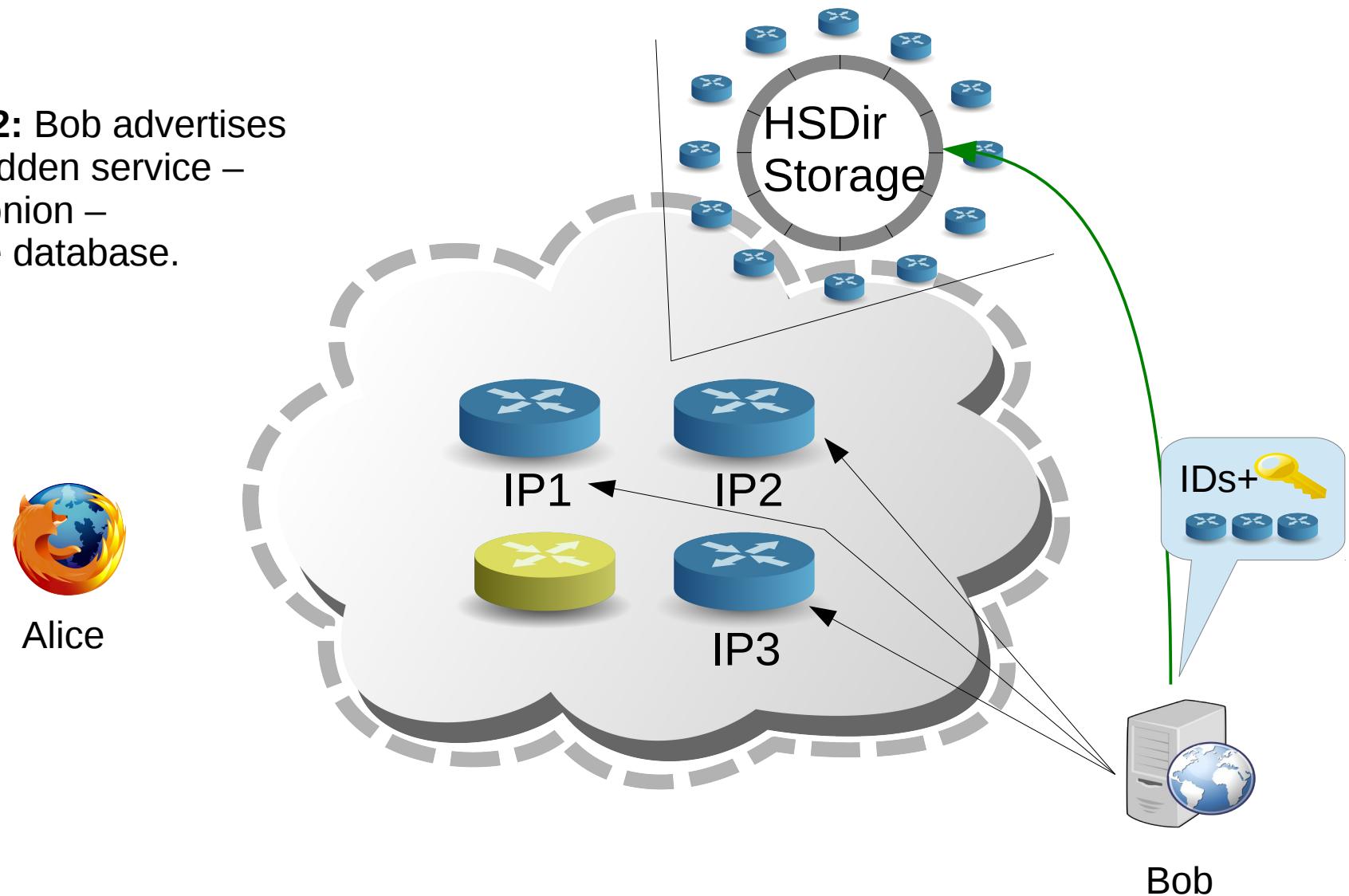
Tor rendezvous protocol

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

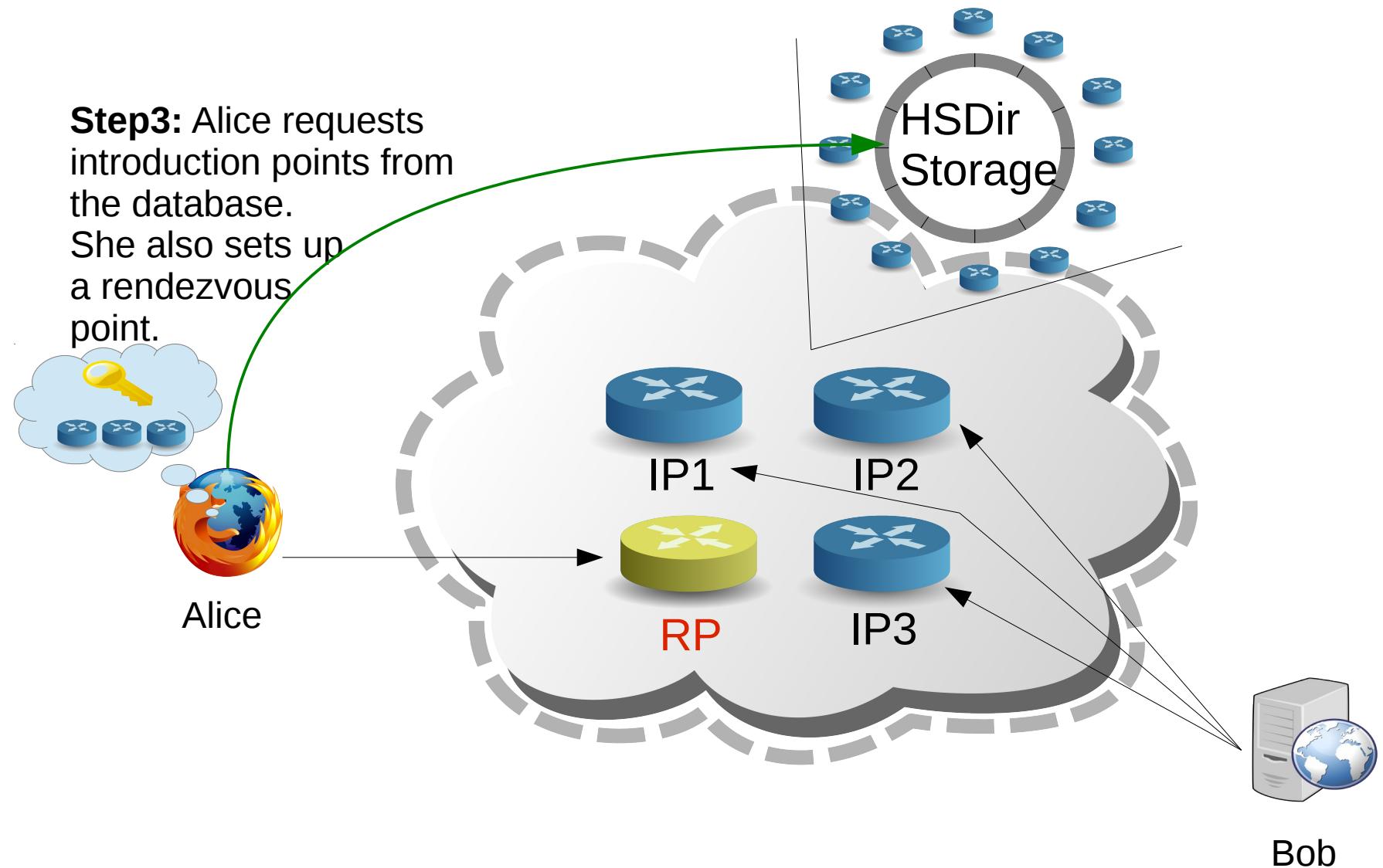


Tor rendezvous protocol

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

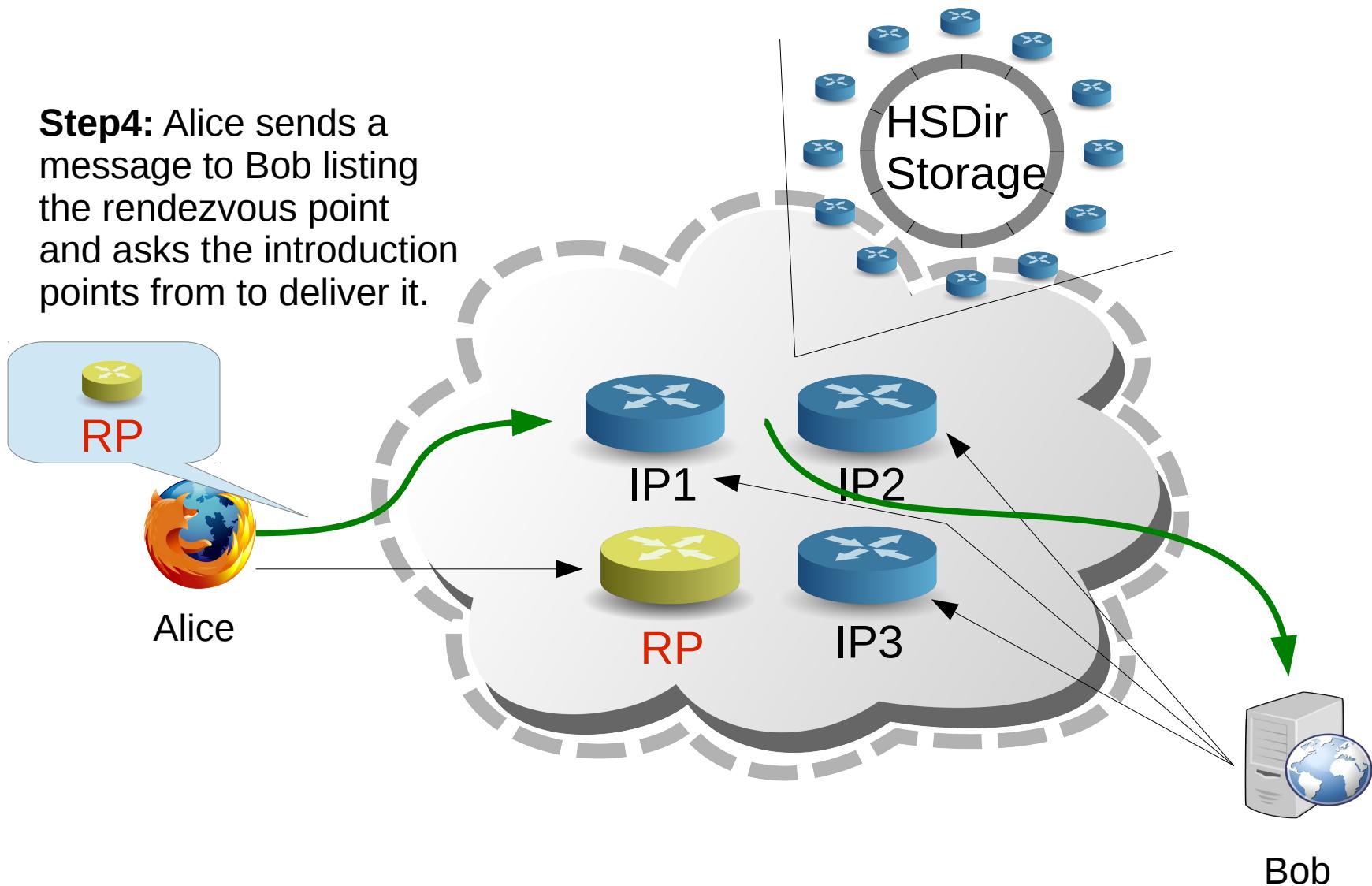


Tor rendezvous protocol



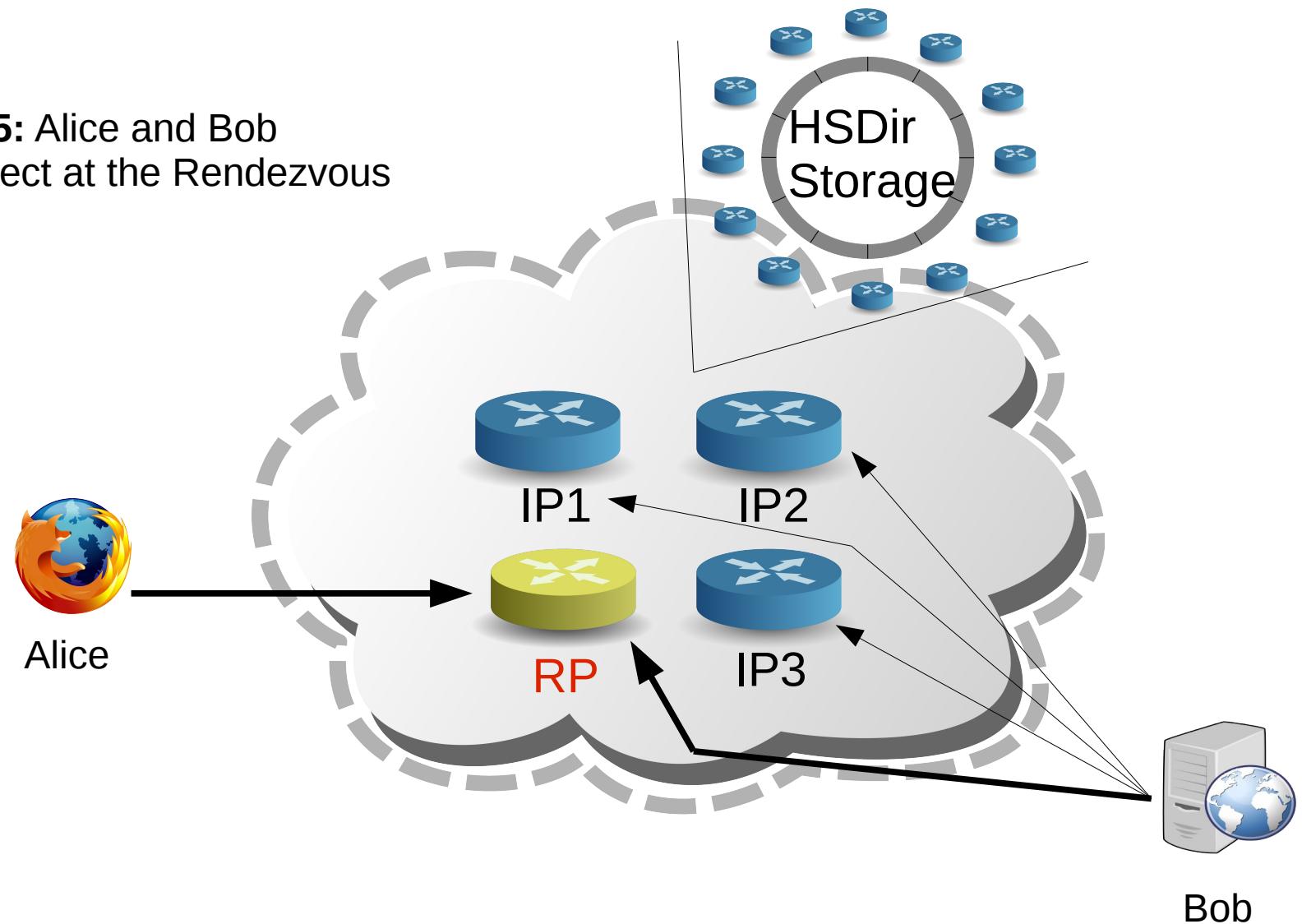
Tor rendezvous protocol

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

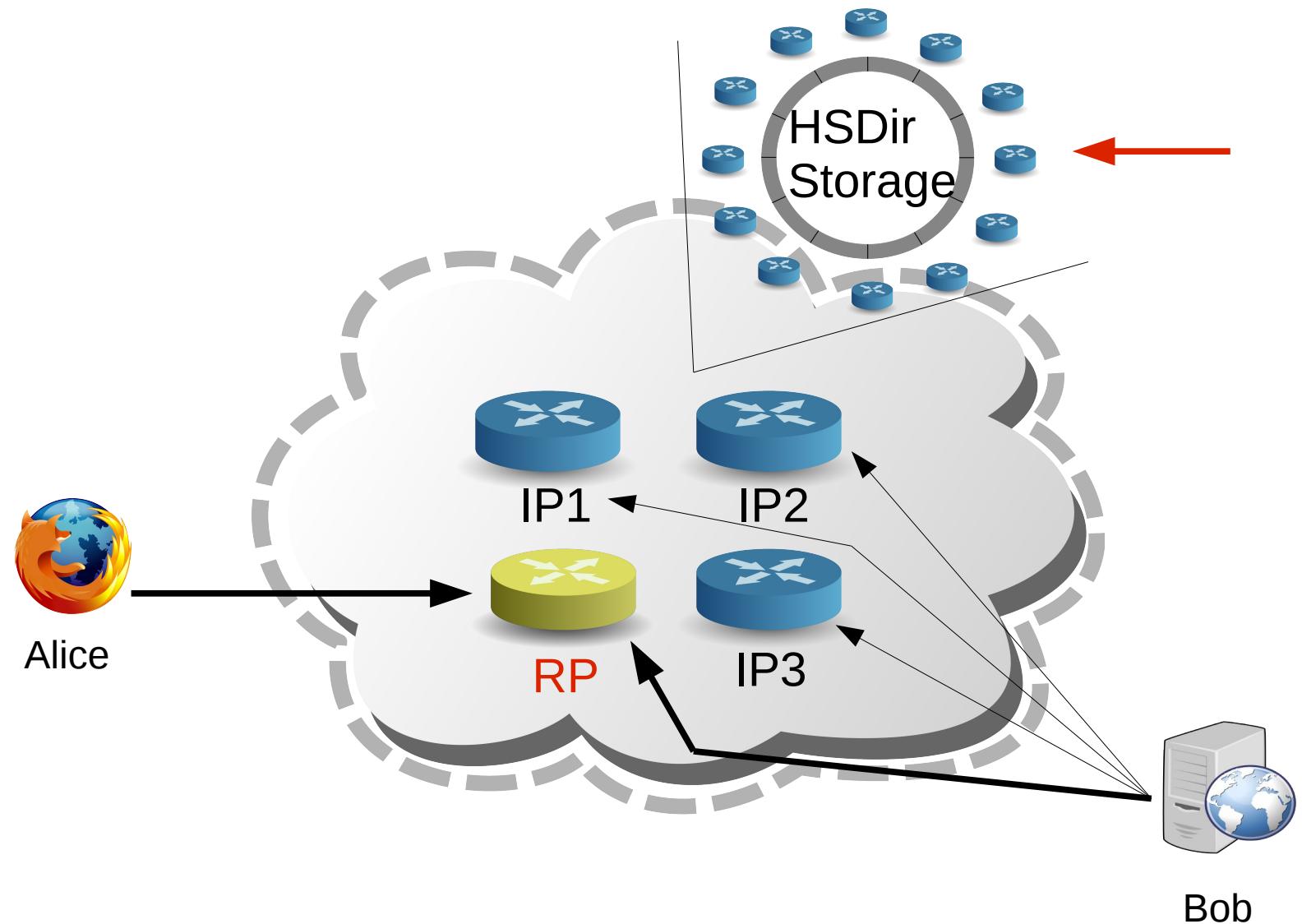


Tor rendezvous protocol

Step5: Alice and Bob Connect at the Rendezvous point

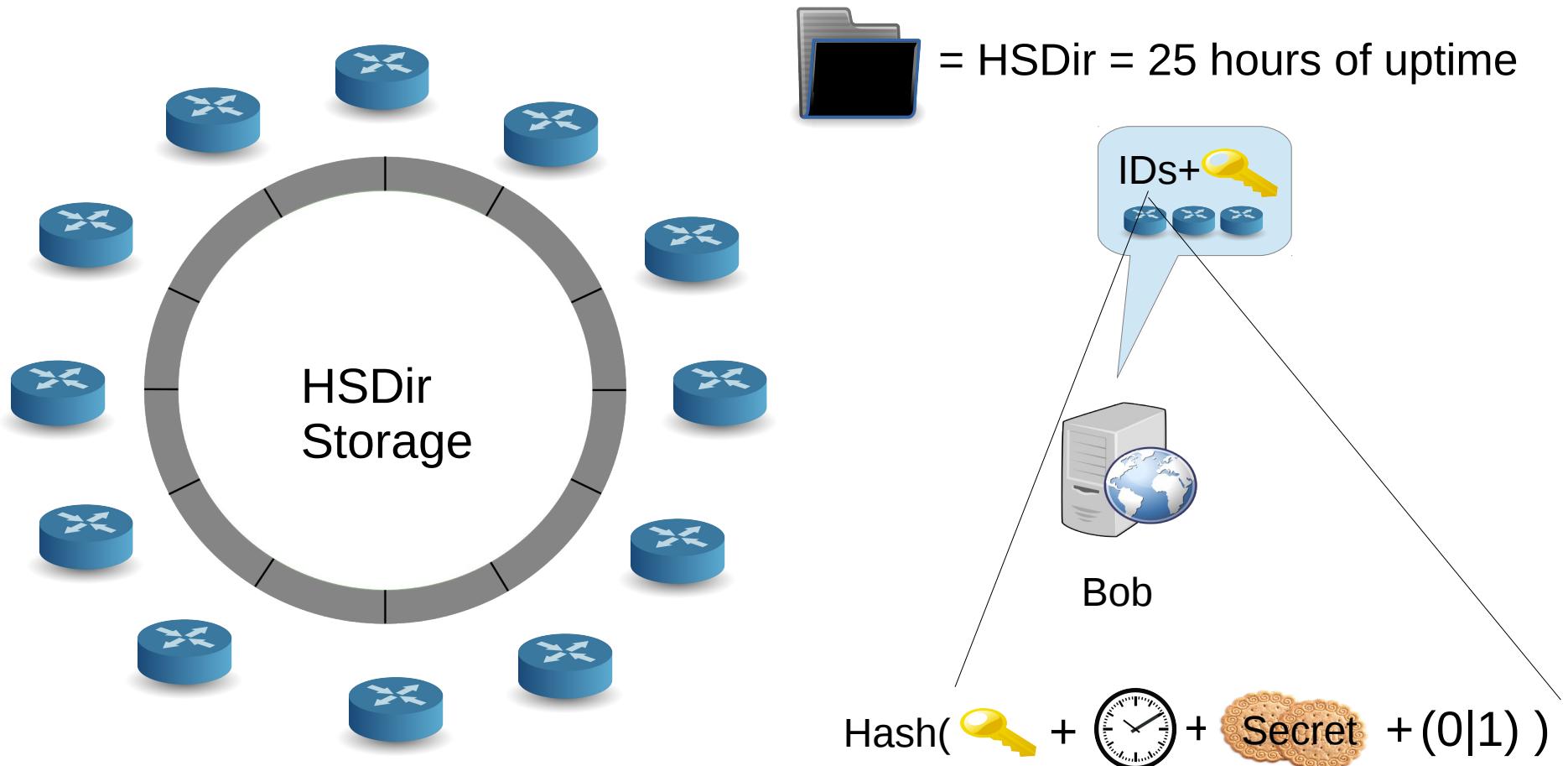


Tor rendezvous protocol

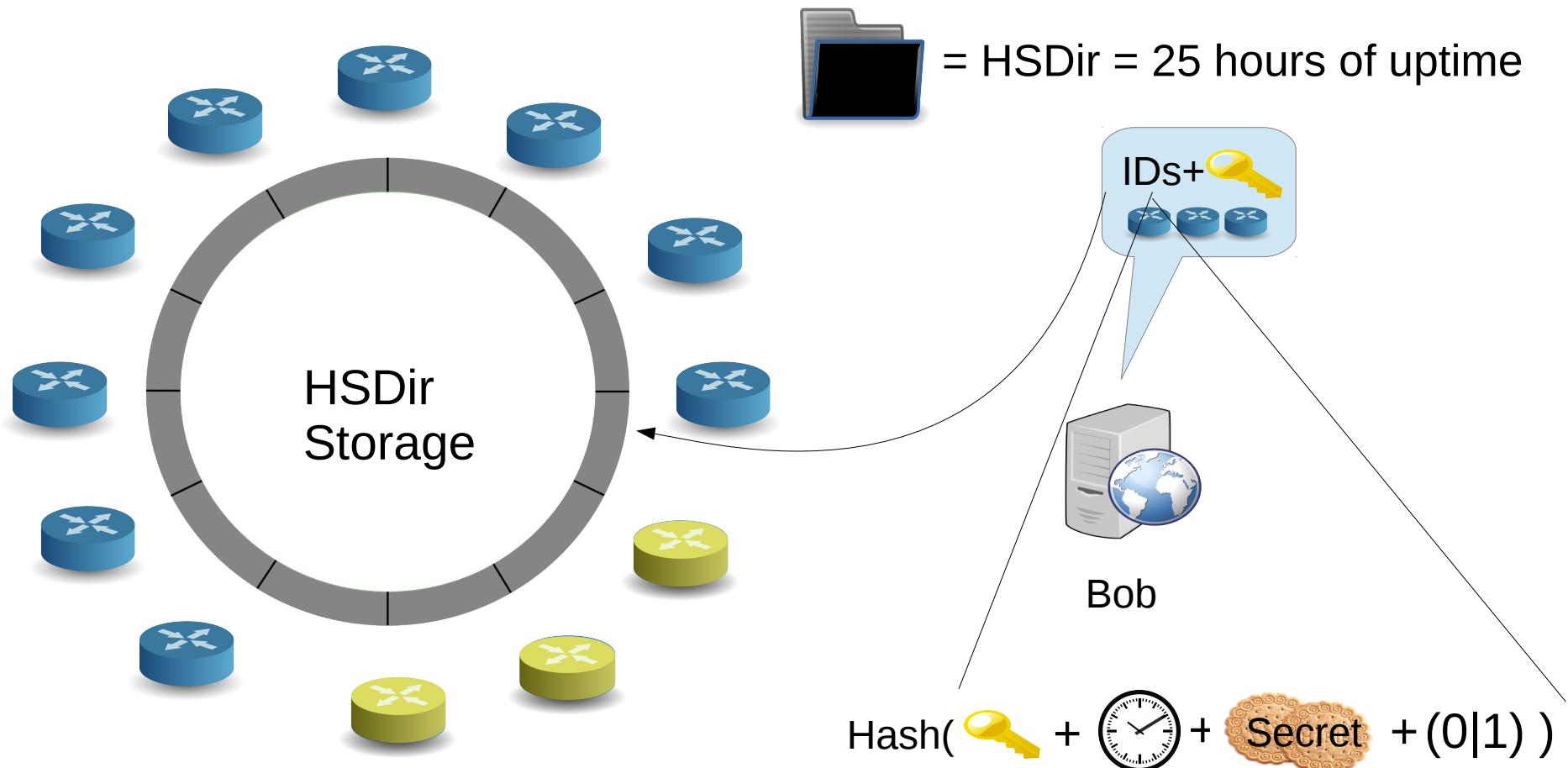


Bob

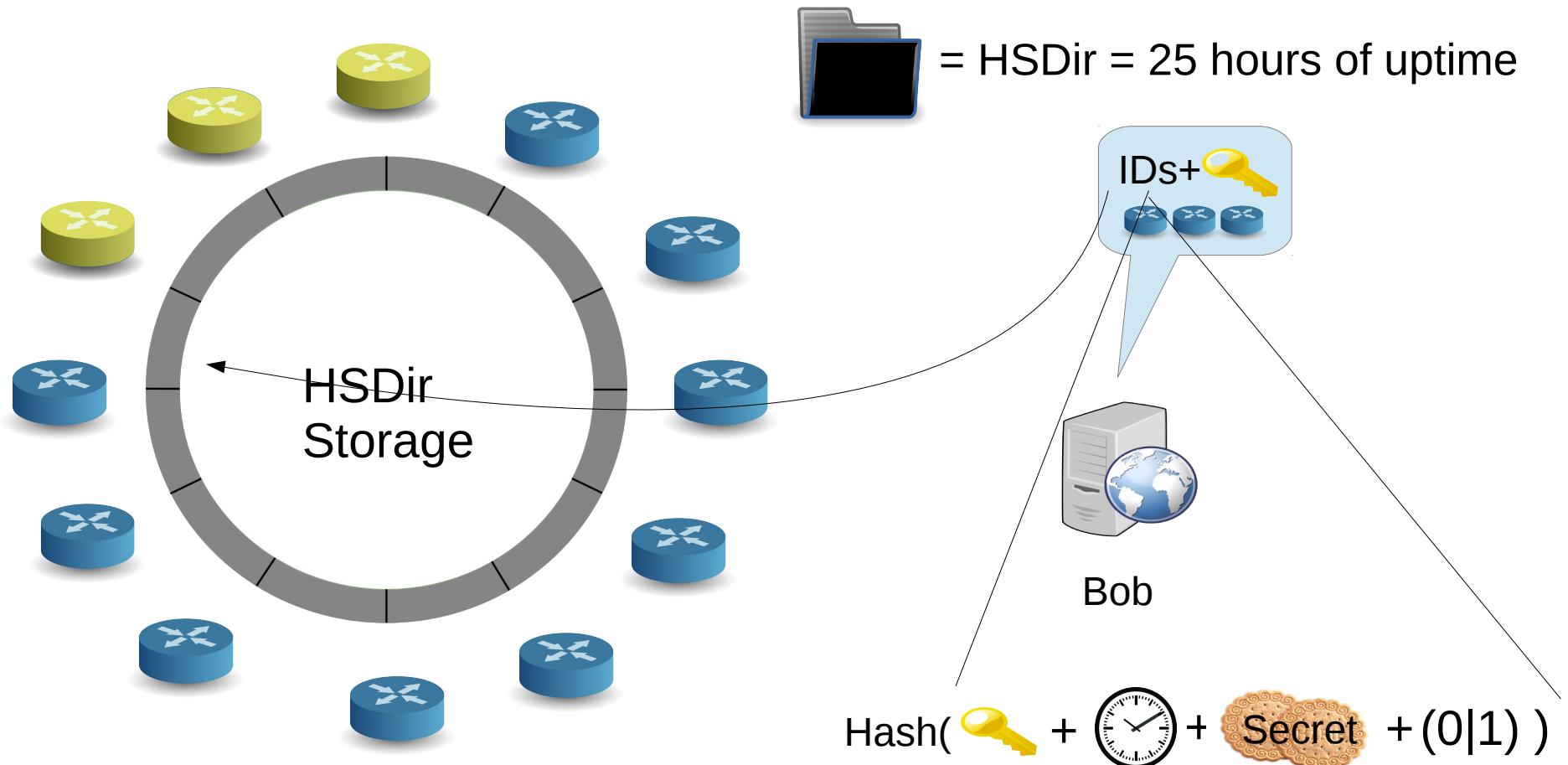
Responsible hidden service directories



Responsible hidden service directories



Responsible hidden service directories

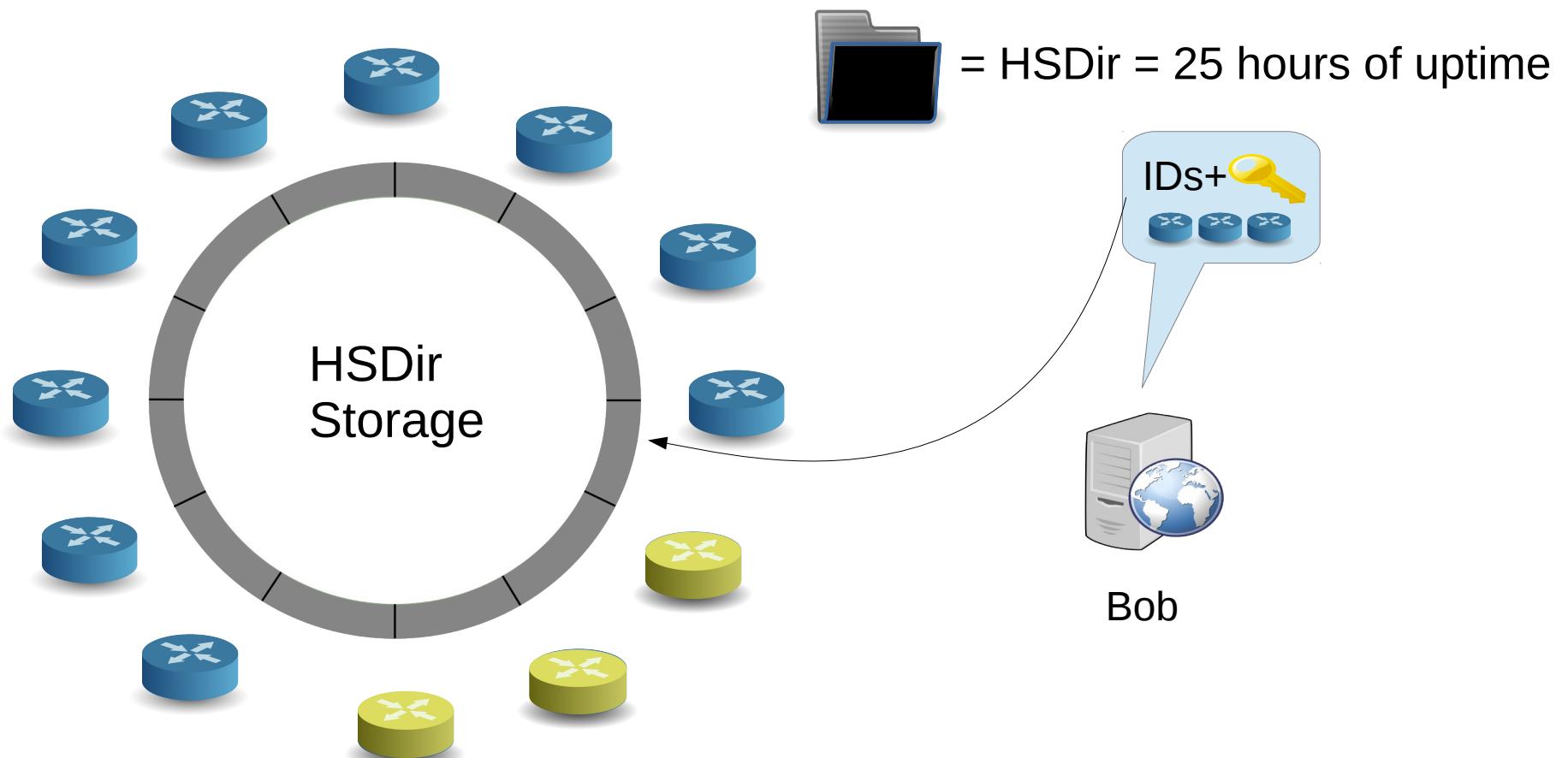


- IDs change every 24 hours at some time during the day
- Re-upload every hour

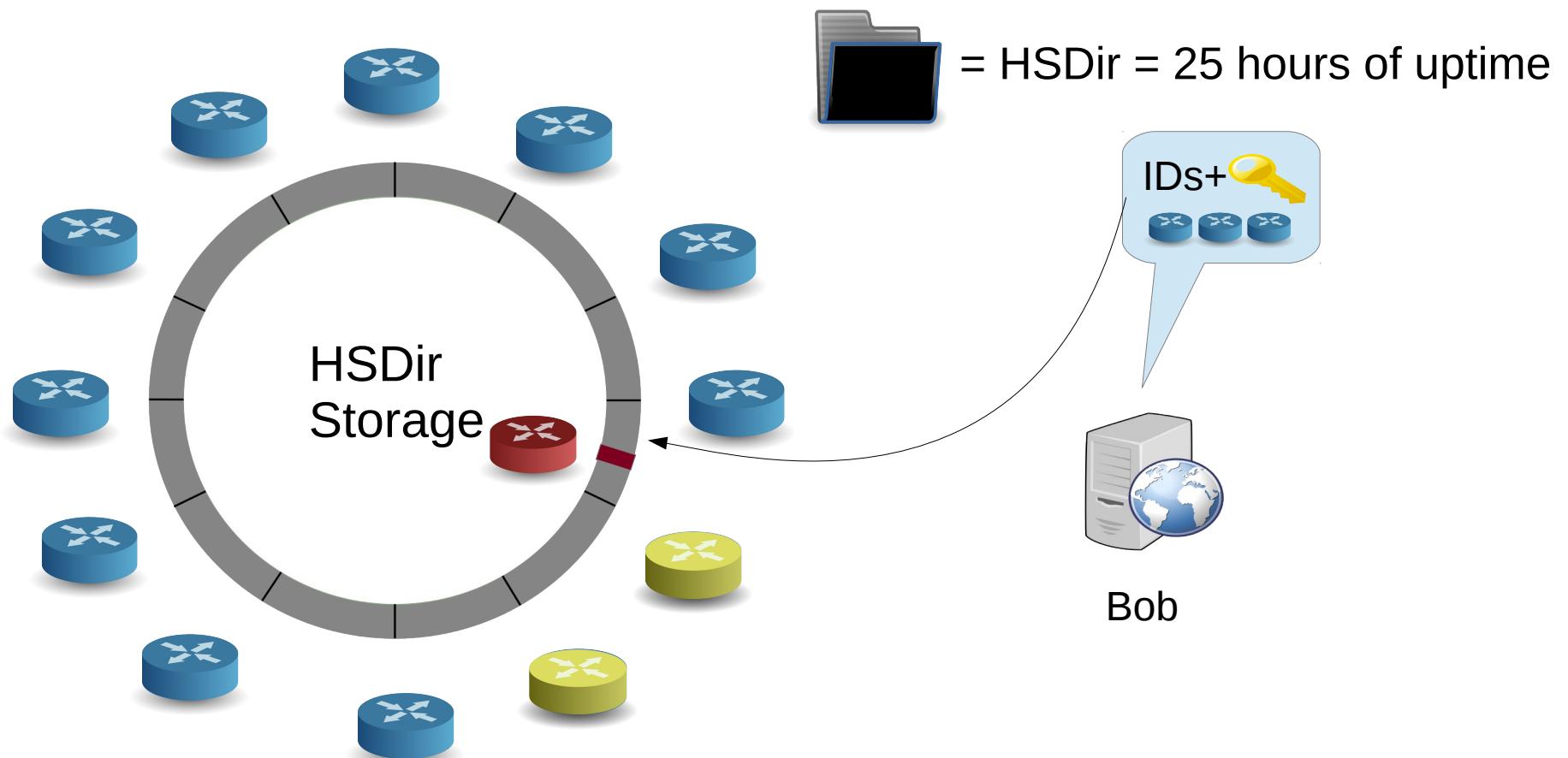
Overview

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

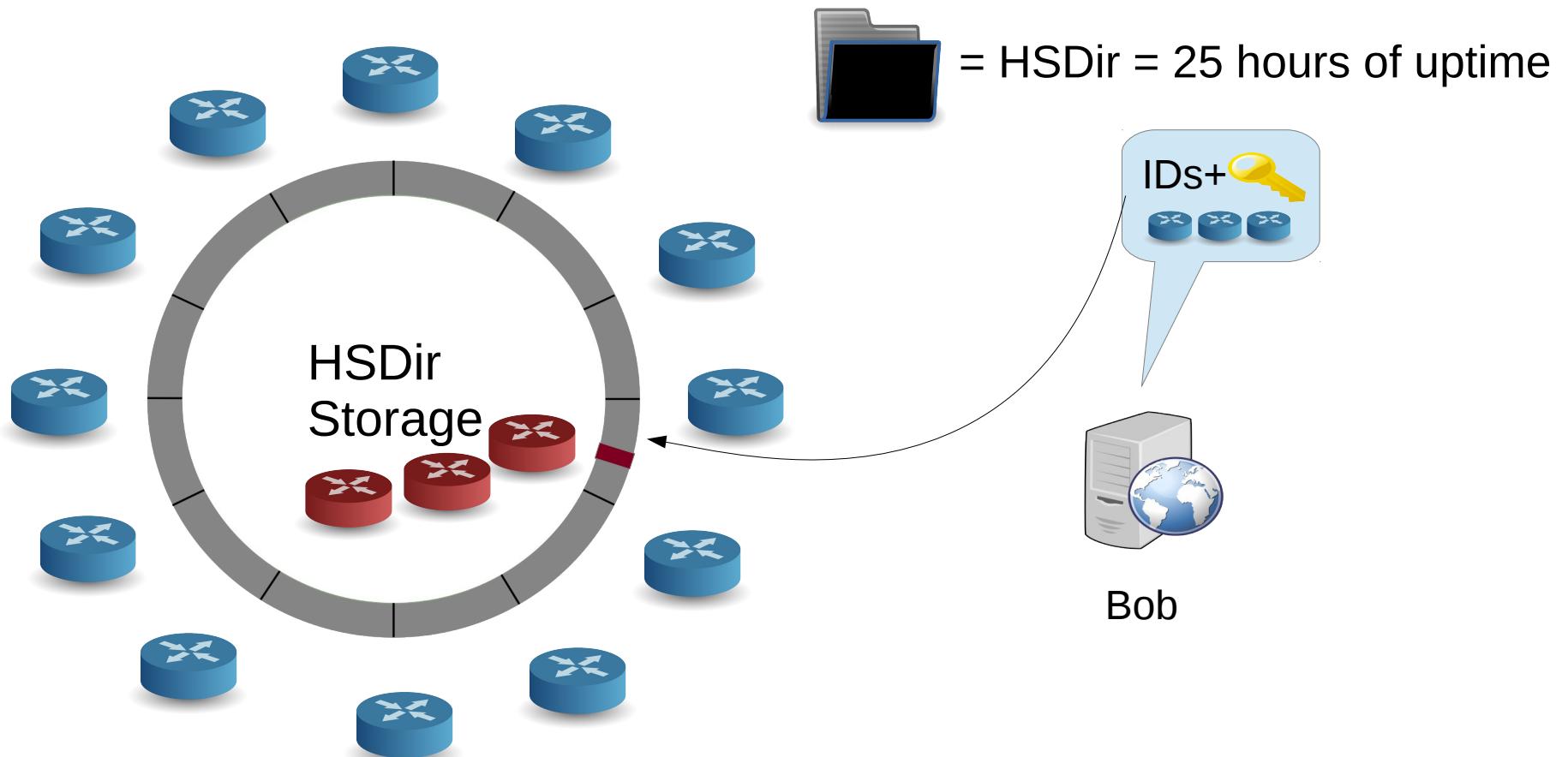
Impersonating Hidden service directory



Impersonating Hidden service directory

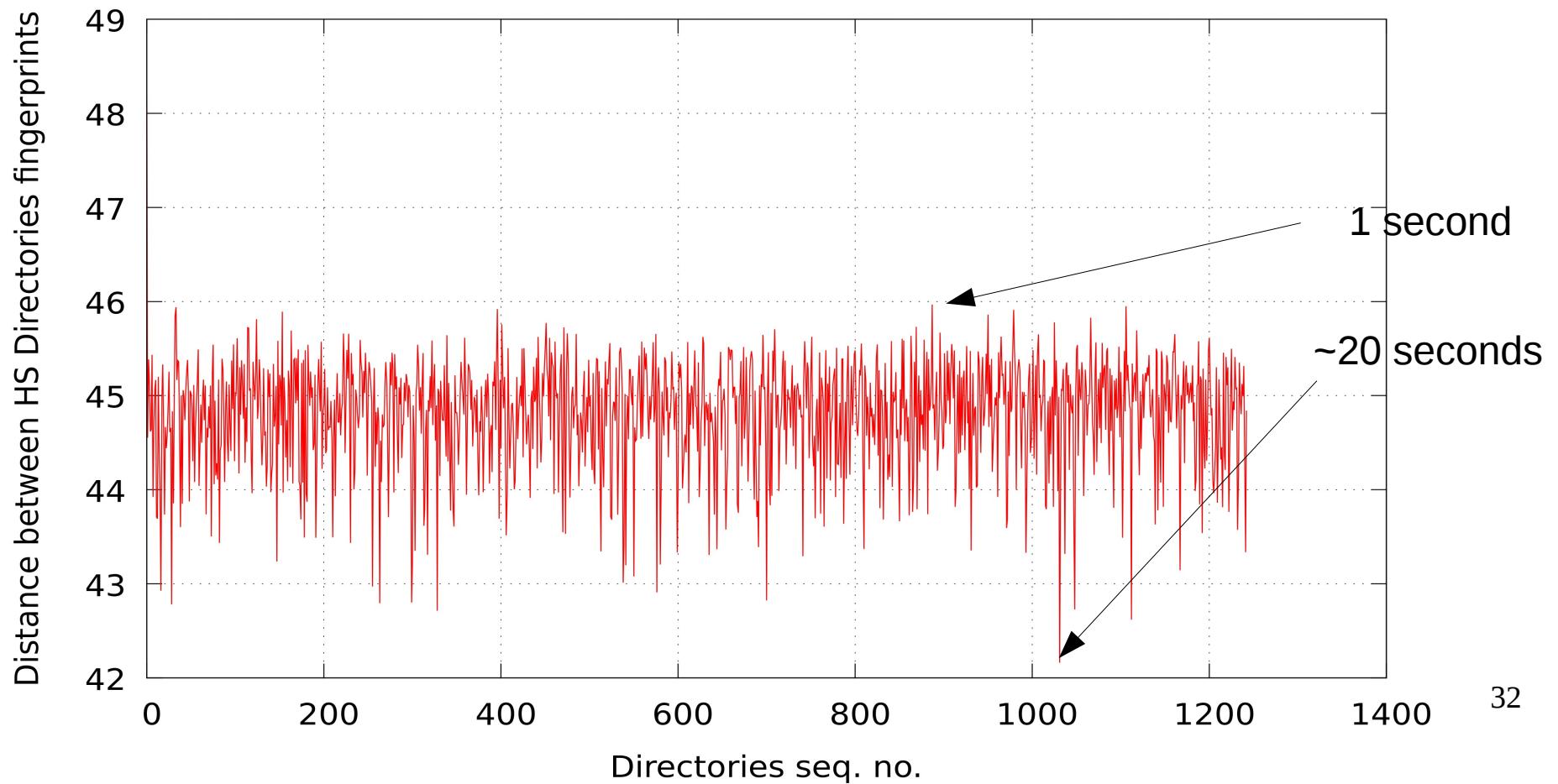


Impersonating Hidden service directory



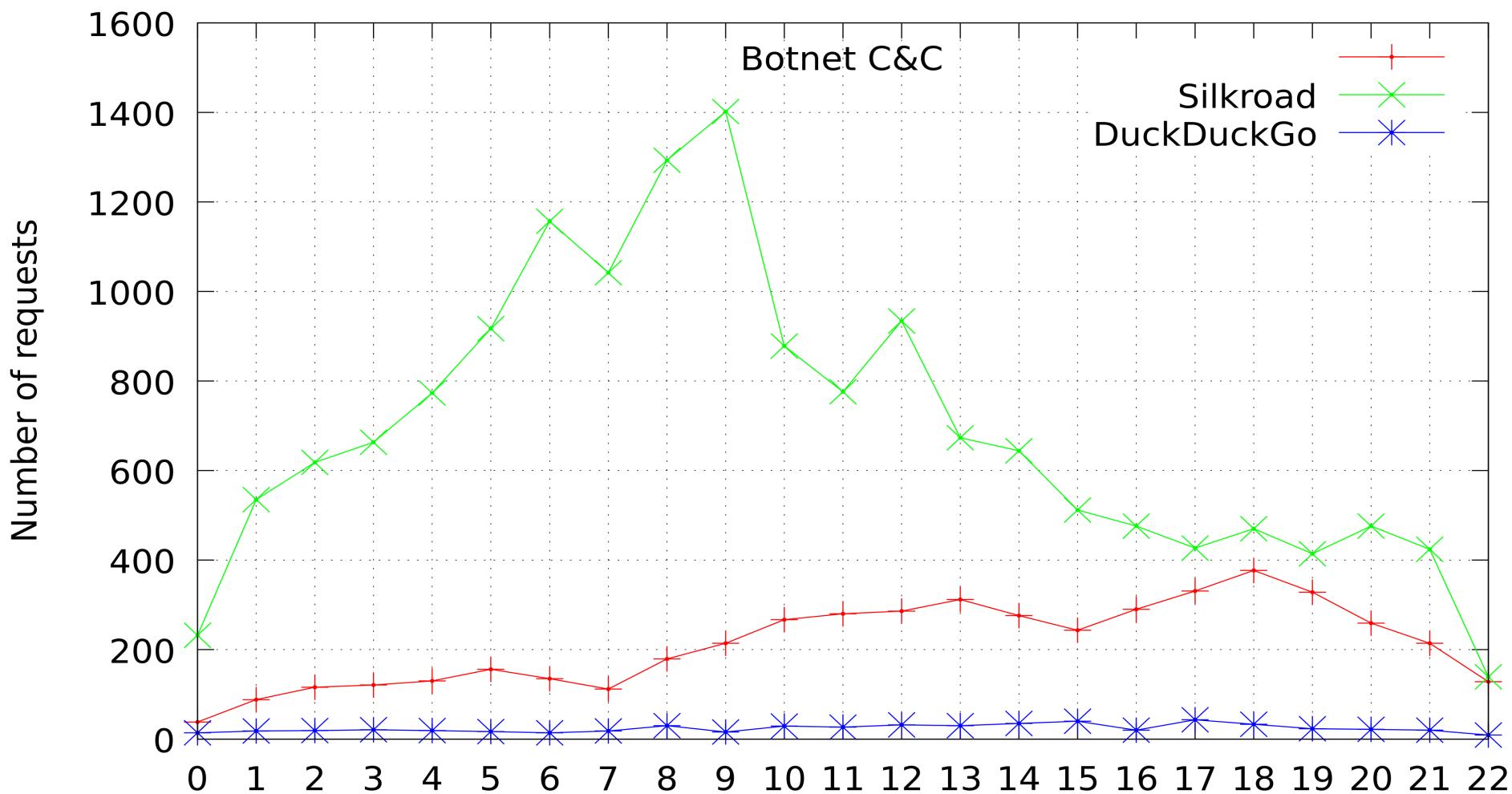
Impersonating Hidden service directory

- 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

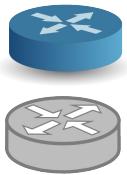


Overview

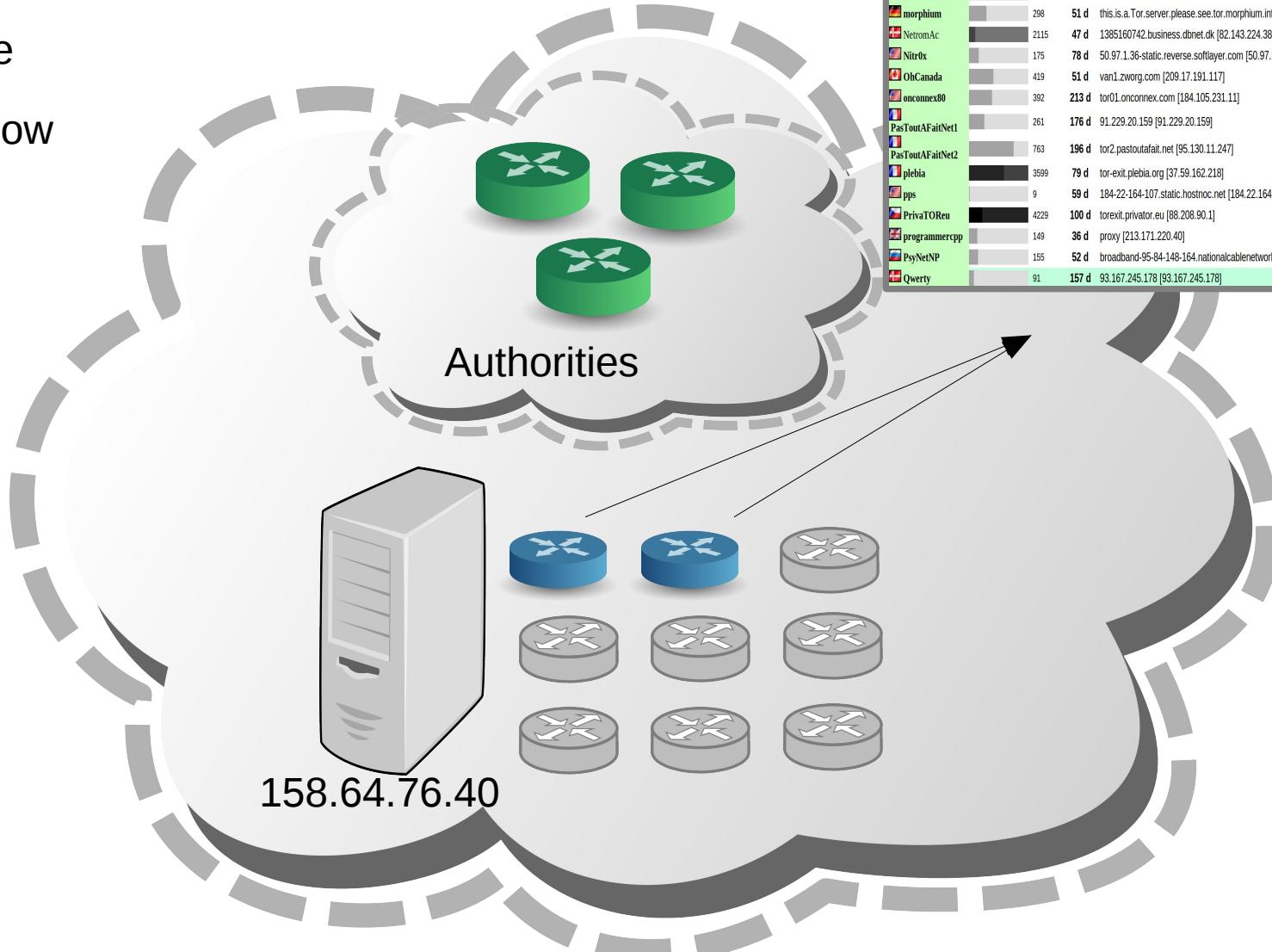
- Background
- Measuring the popularity of hidden services
- DoSing hidden services.
- **Harvesting onion addresses.**
- Revealing the guards.
- Opportunistic deanonymisation.

Shadowing

Consensus

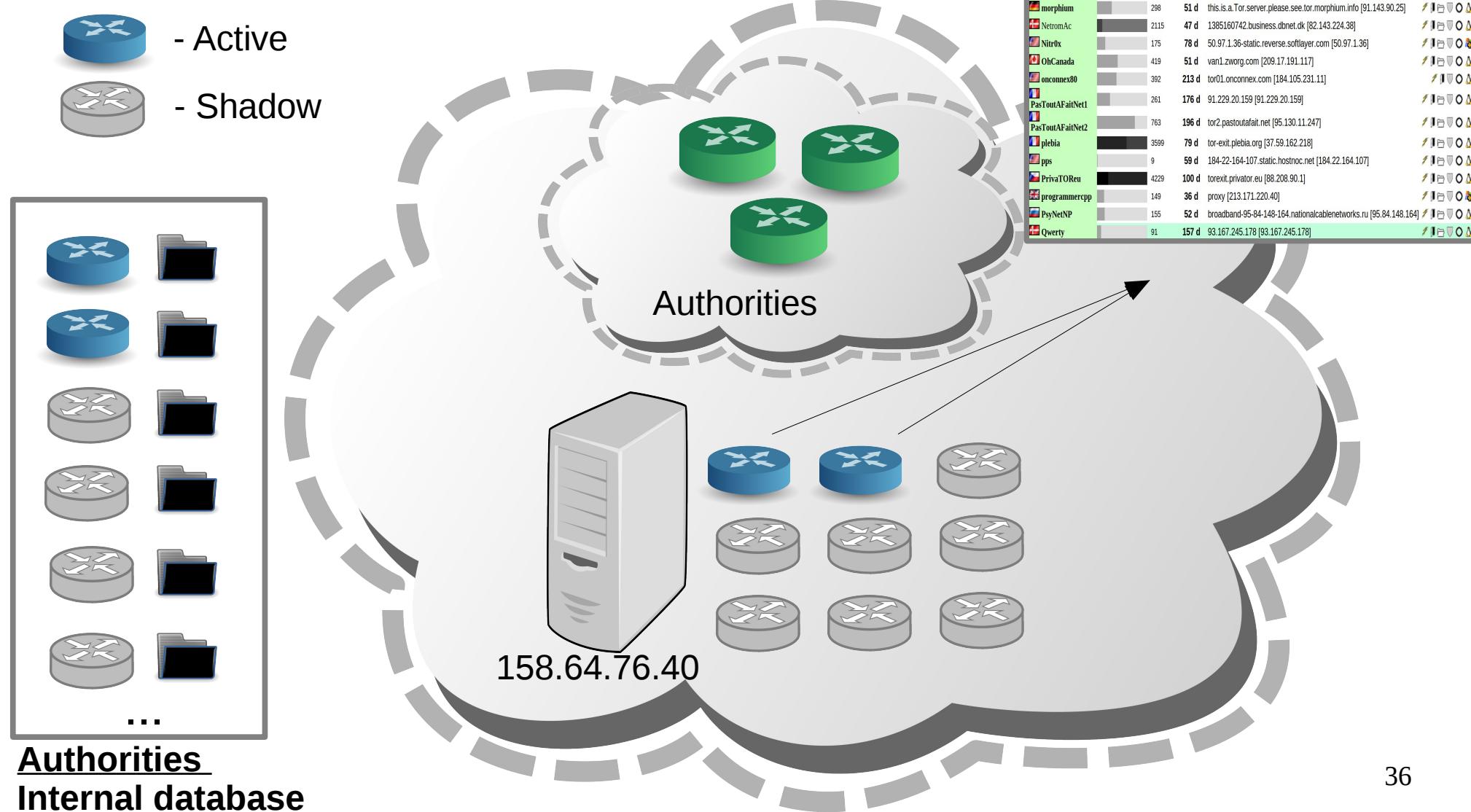


- Active
- Shadow



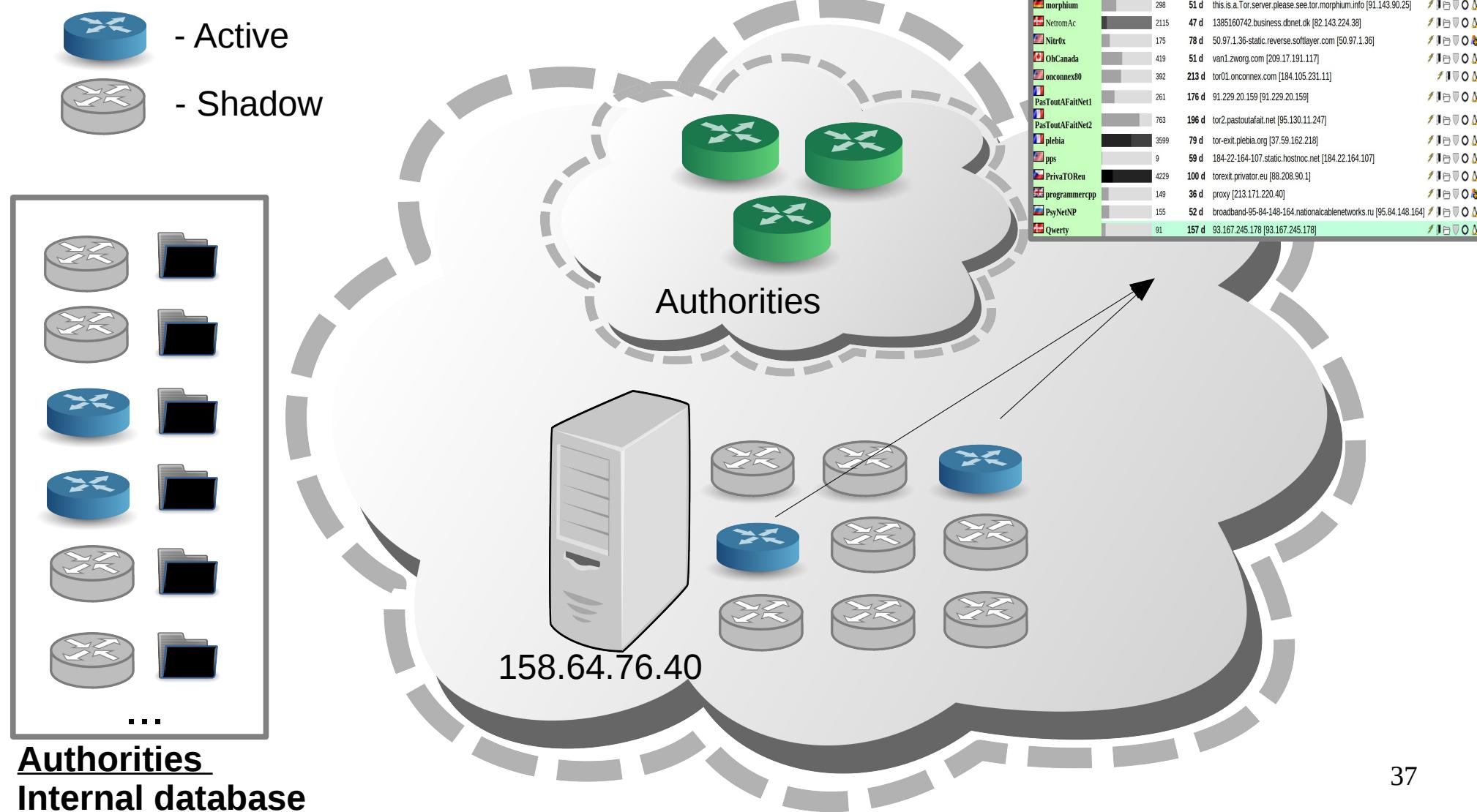
Shadowing

Consensus



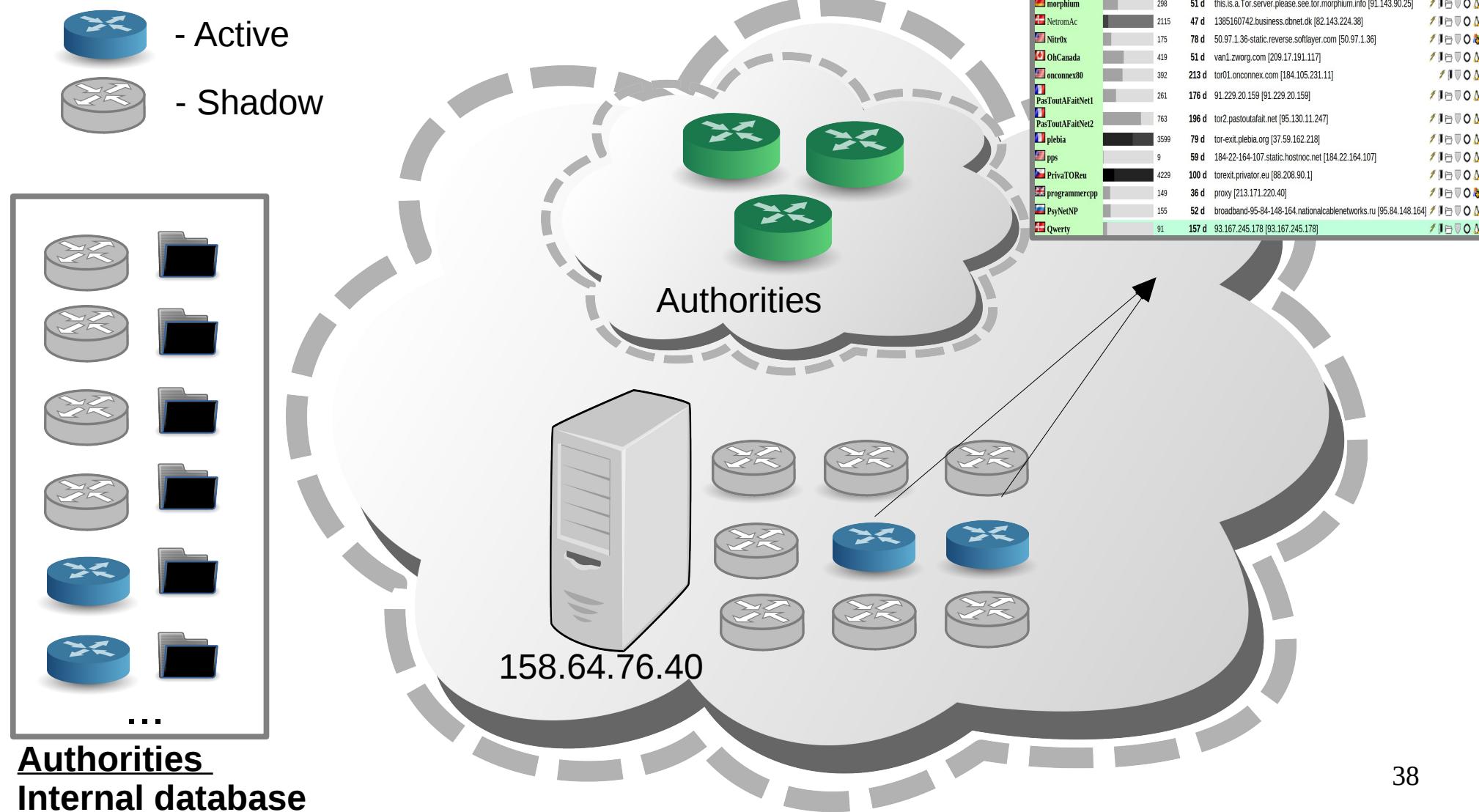
Shadowing

Consensus

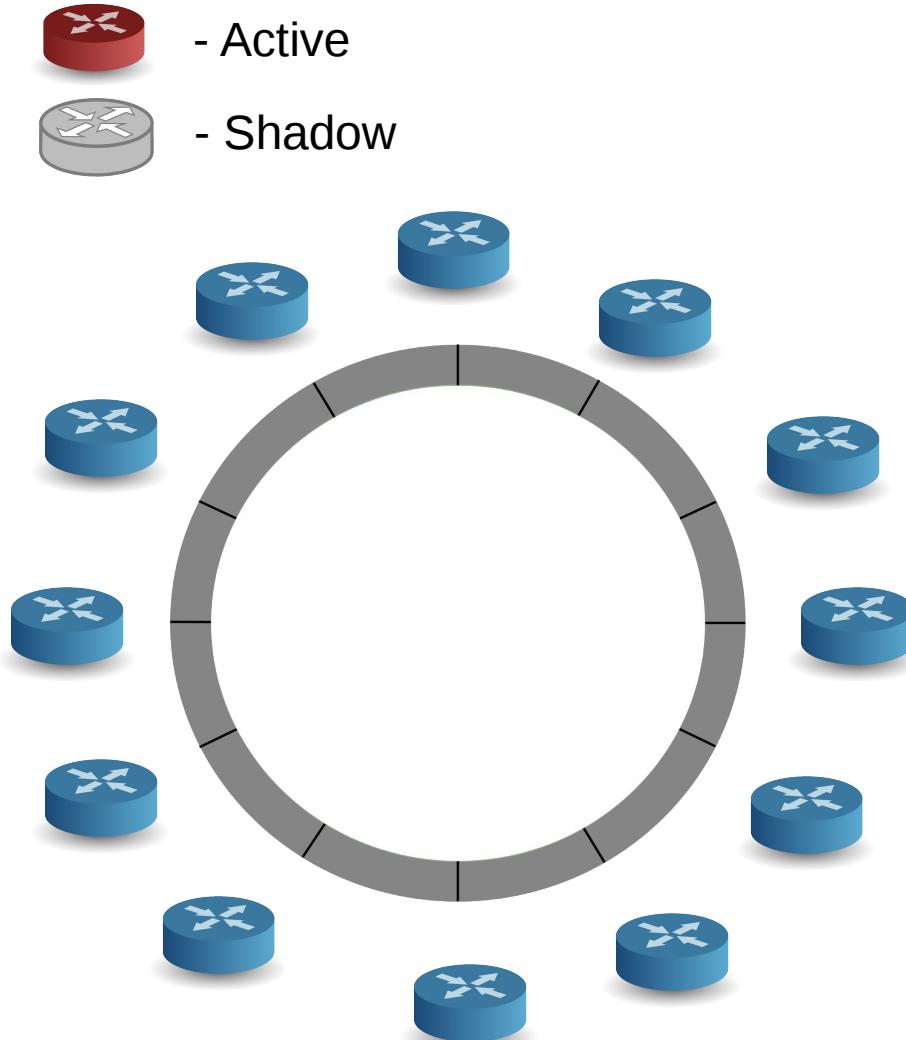


Shadowing

Consensus



Collecting onion addresses

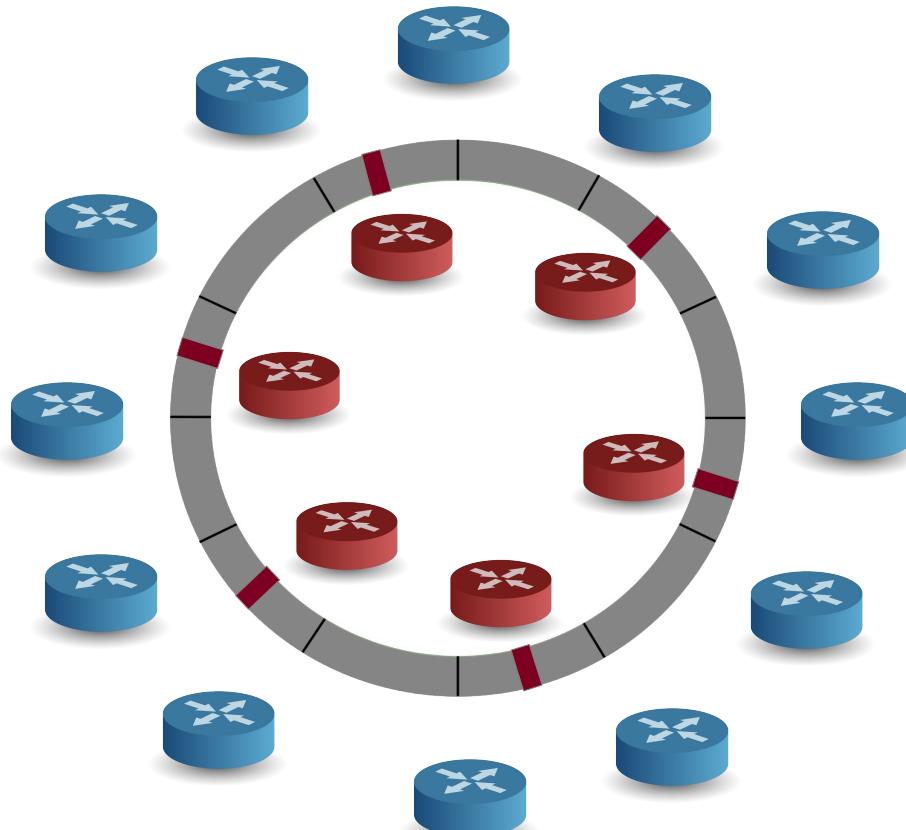


Collecting onion addresses

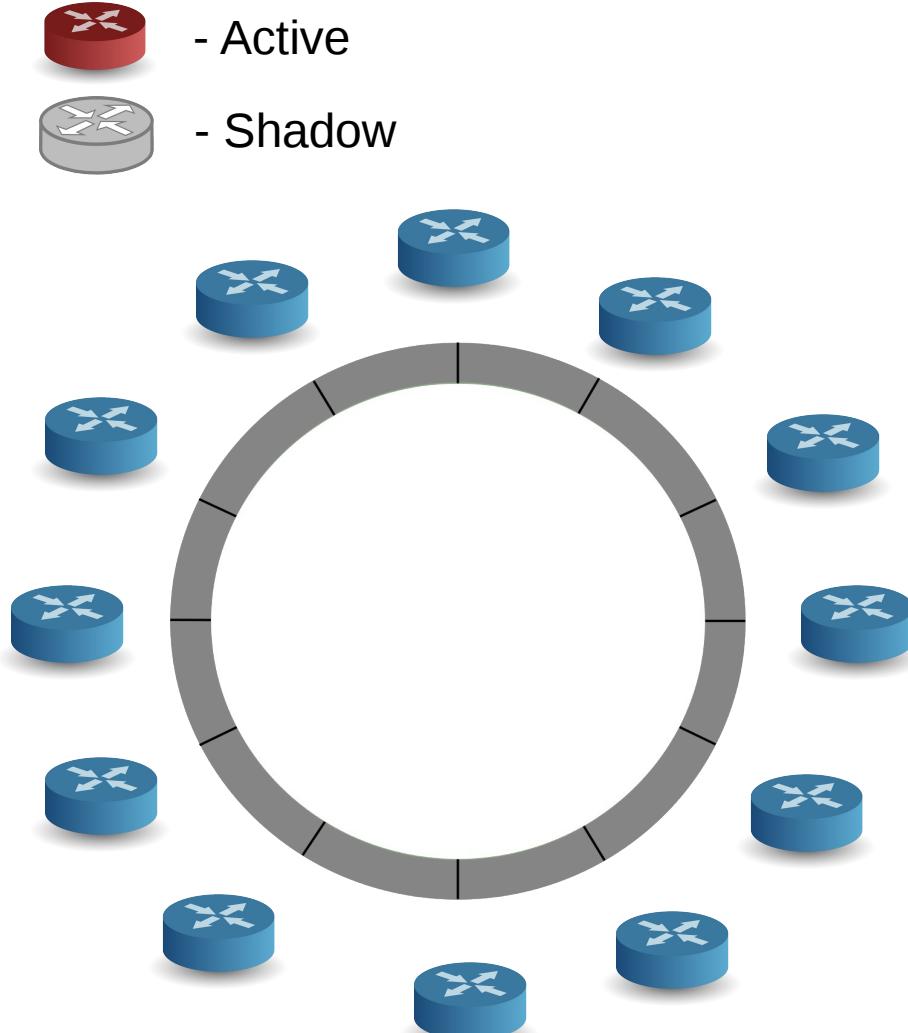


- Active
- Shadow

- Naive approach will require ~350 IP addresses.



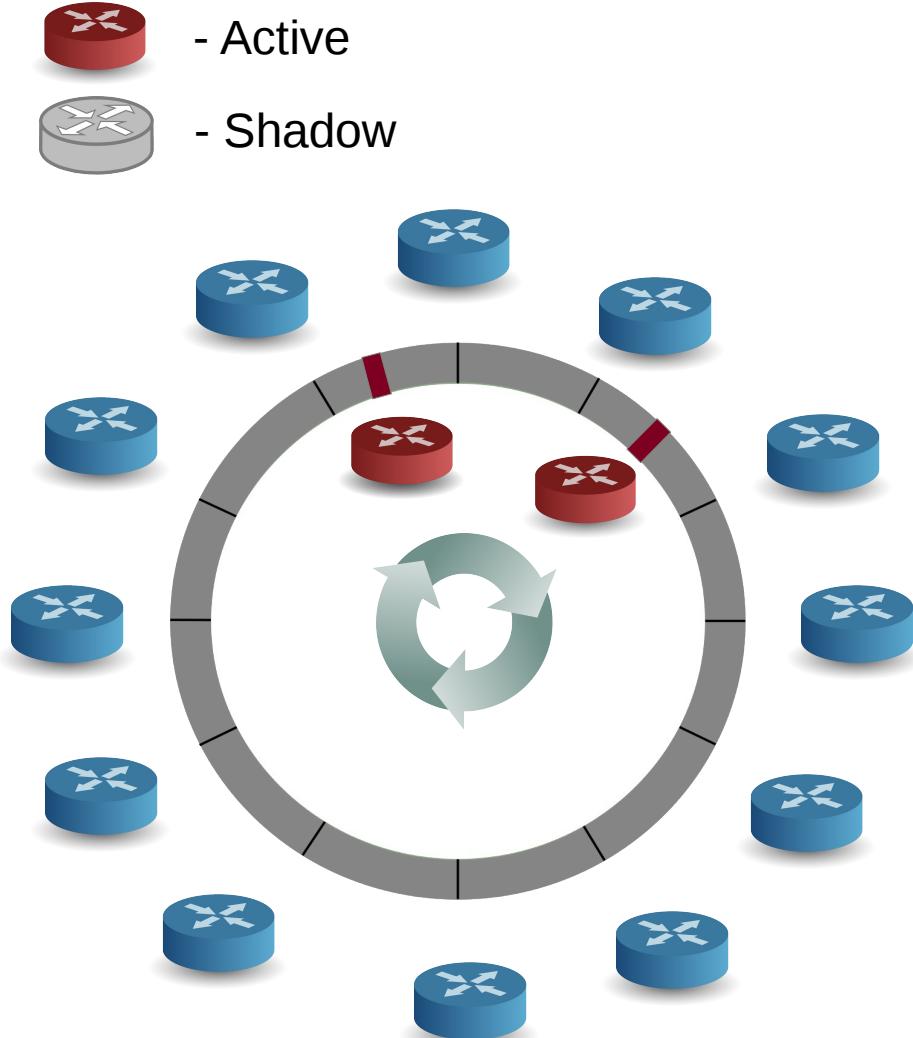
Collecting onion addresses



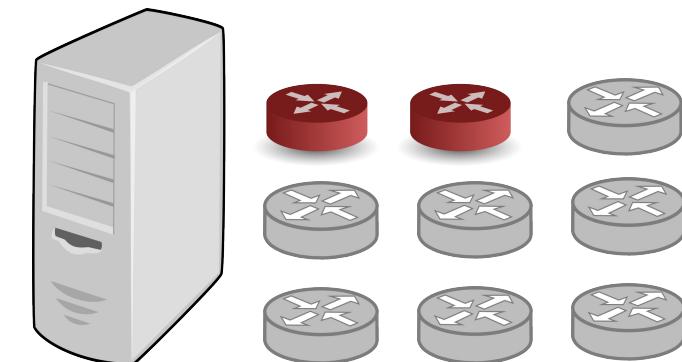
- Active
- Shadow

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

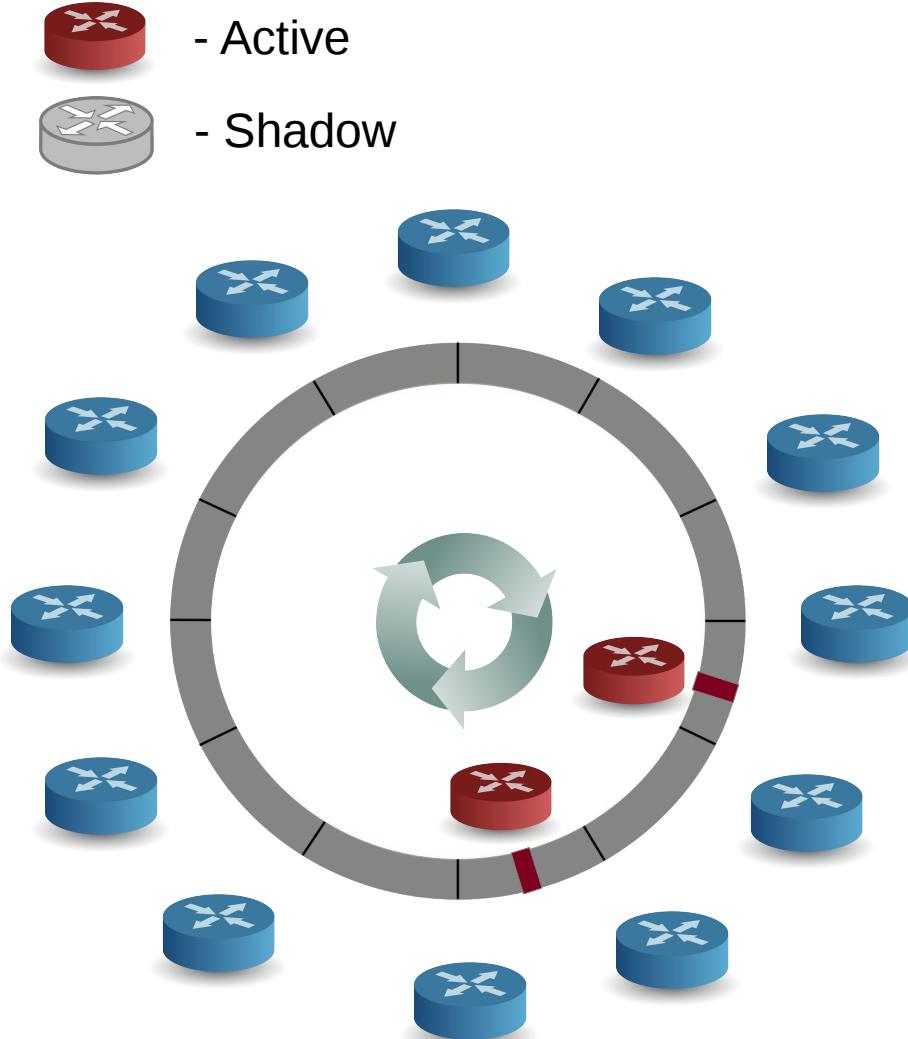
Collecting onion addresses



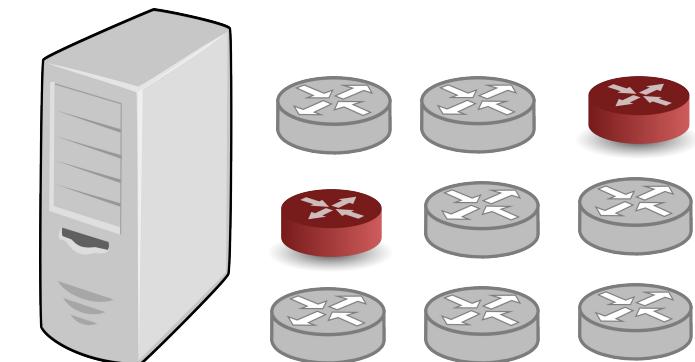
- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.



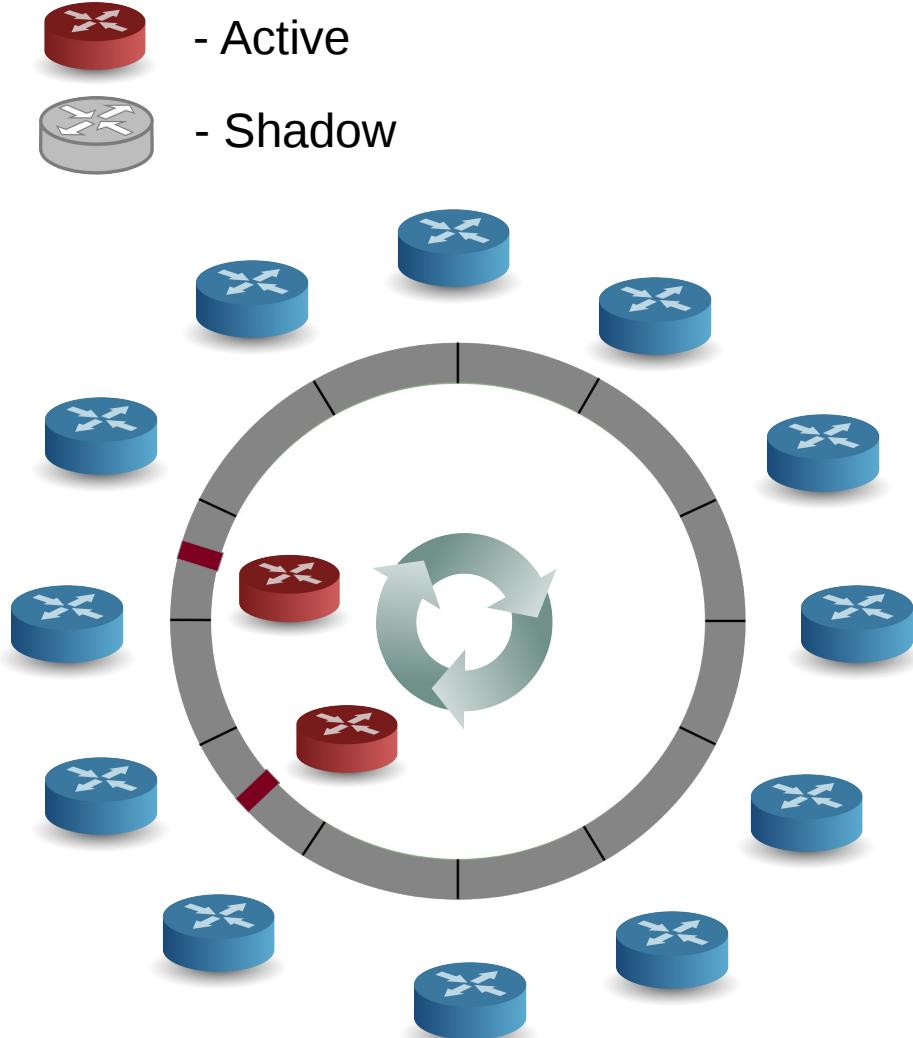
Collecting onion addresses



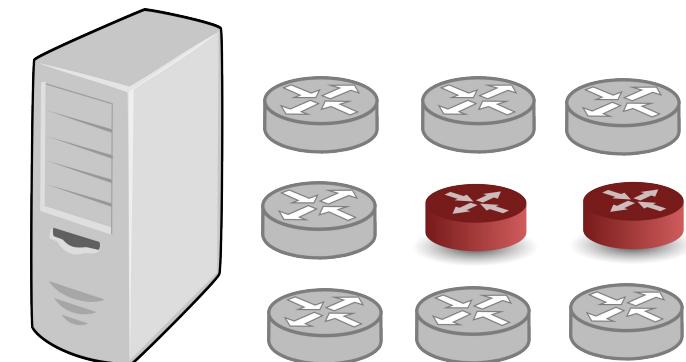
- Naive approach will require ~350 IP addresses.
- Descriptors don't relocate within 24 hours.
- Prepare shadow HSDir relays and gradually pull to consensus.



Collecting onion addresses



- 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

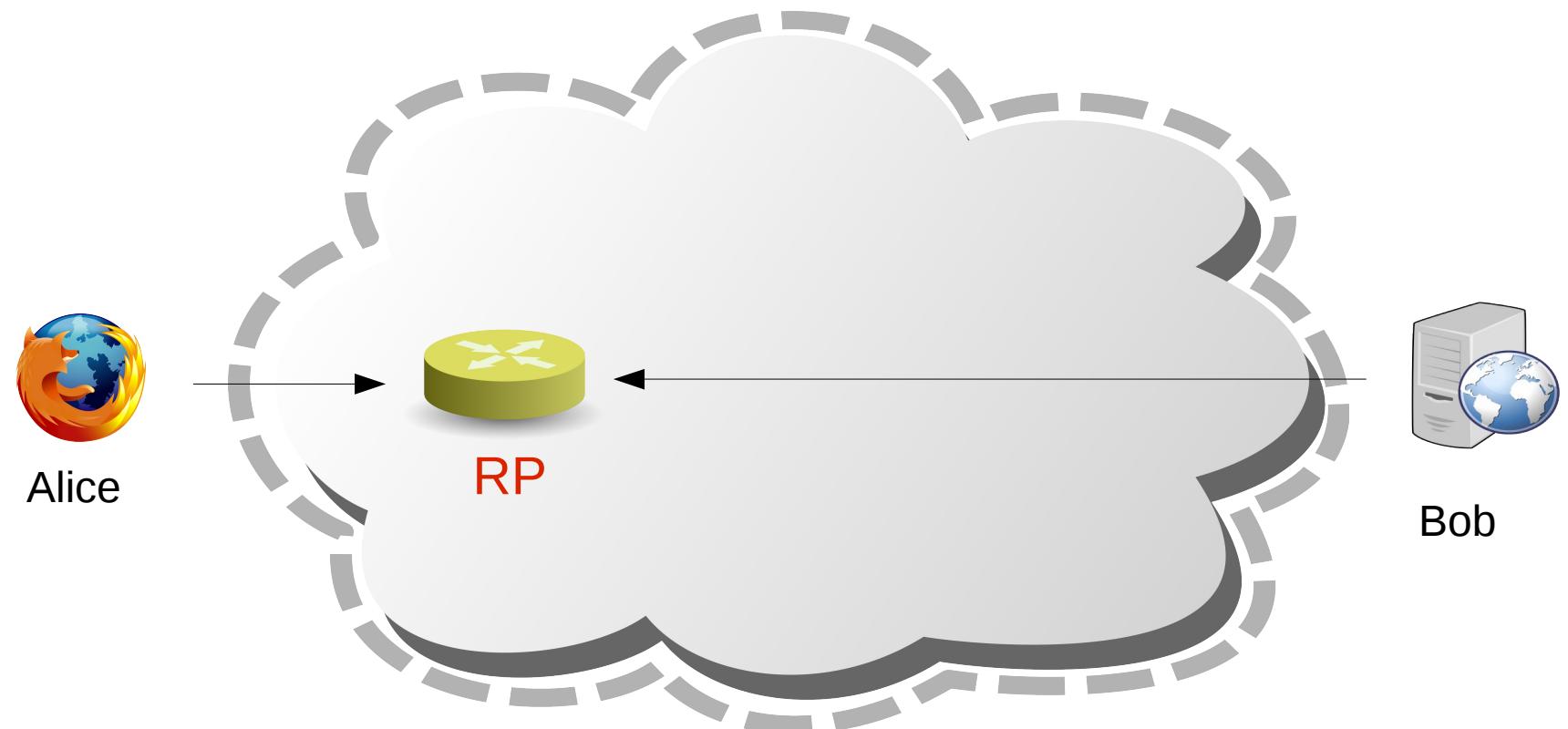
Harvest results

- 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.

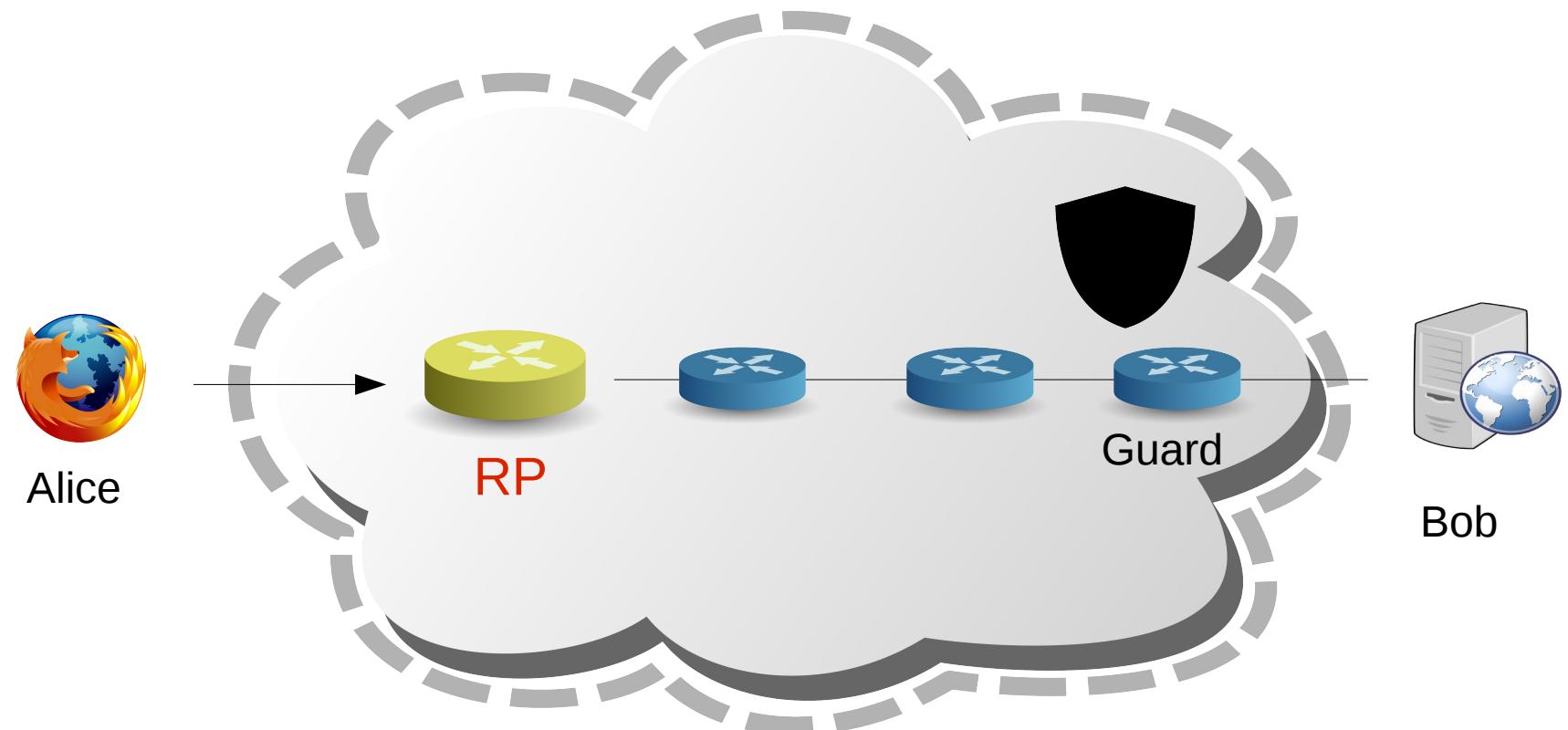
Overview

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

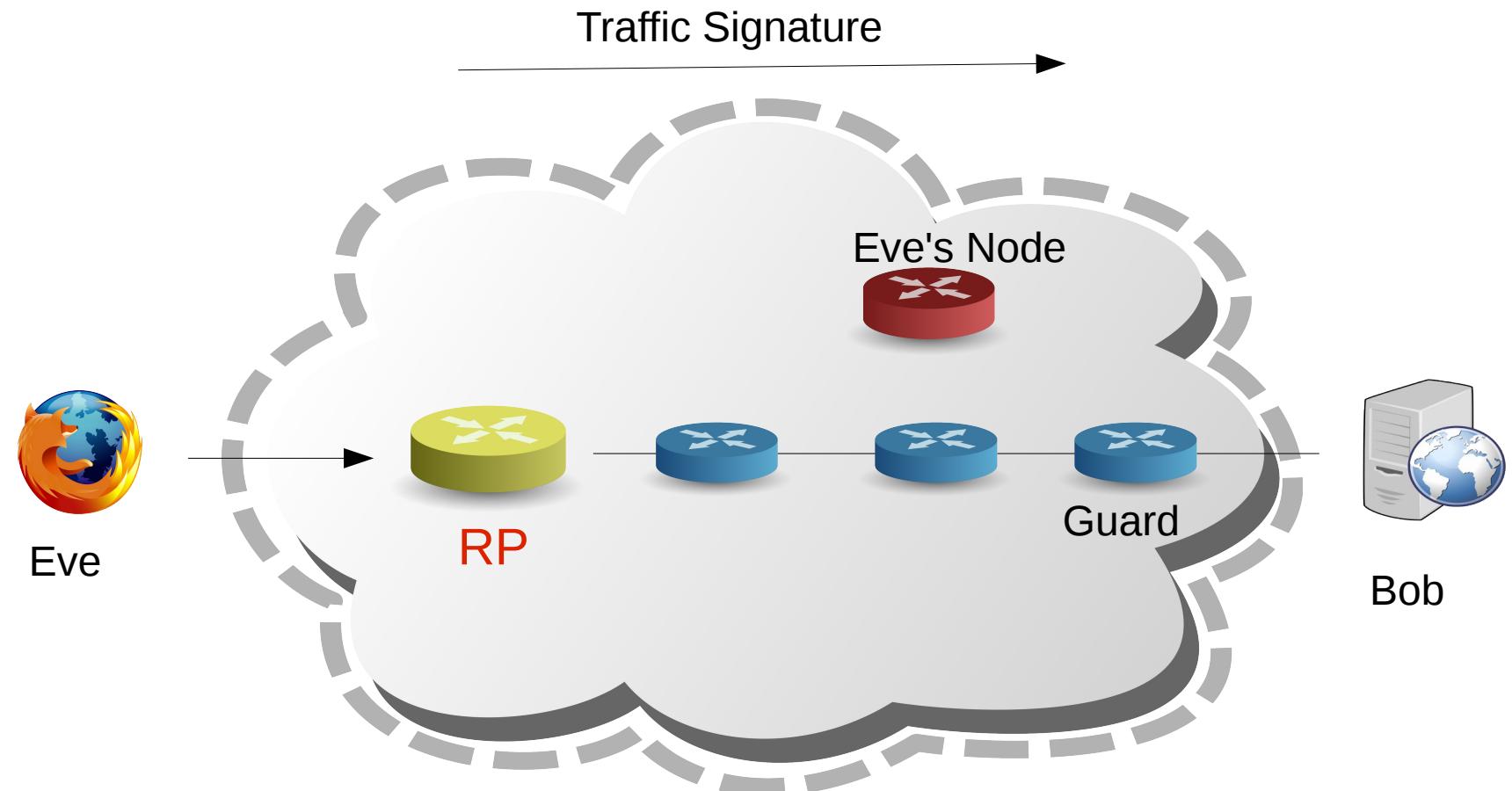
Revealing Guard Nodes



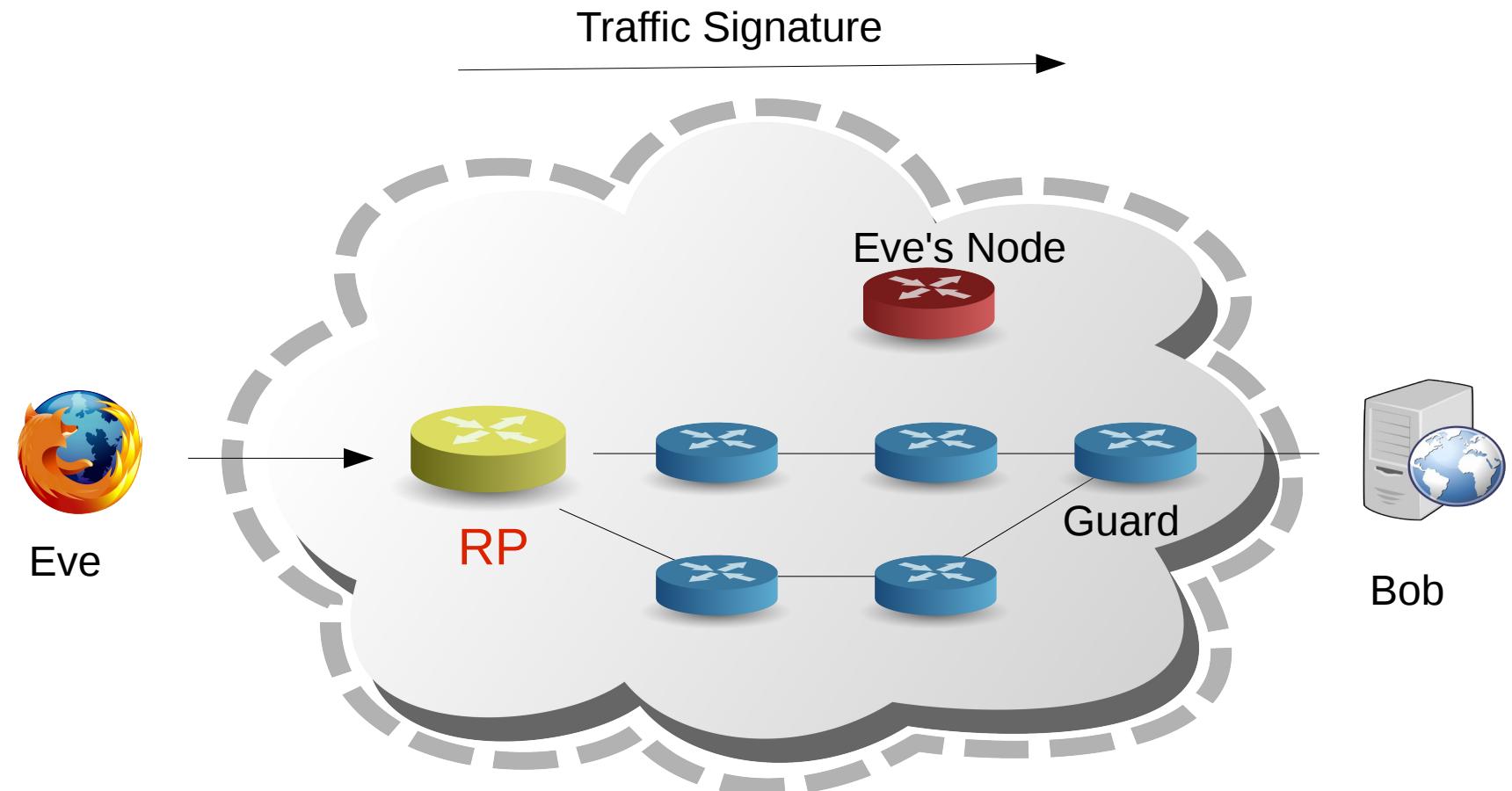
Revealing Guard Nodes



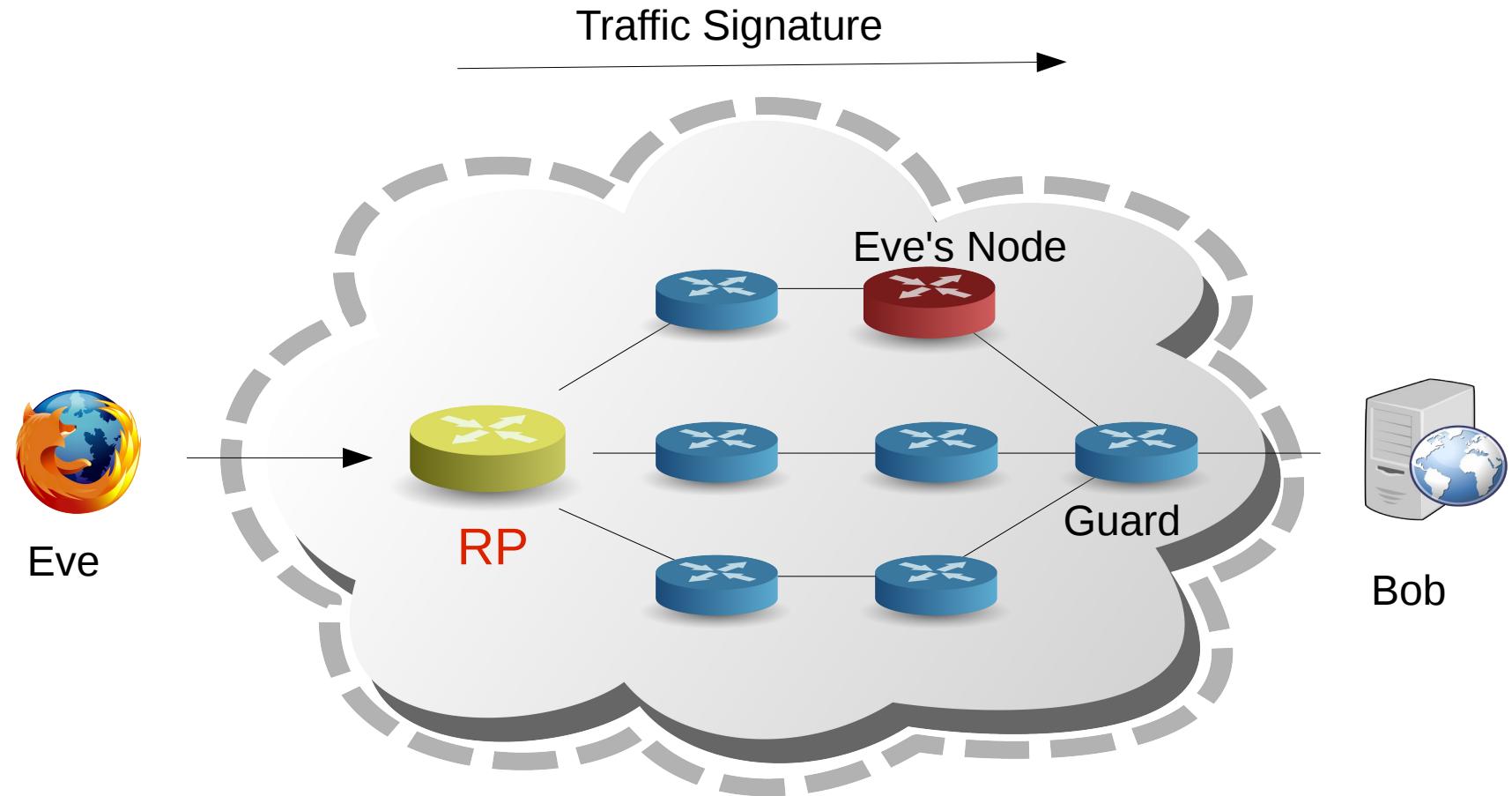
Revealing Guard Nodes



Revealing Guard Nodes

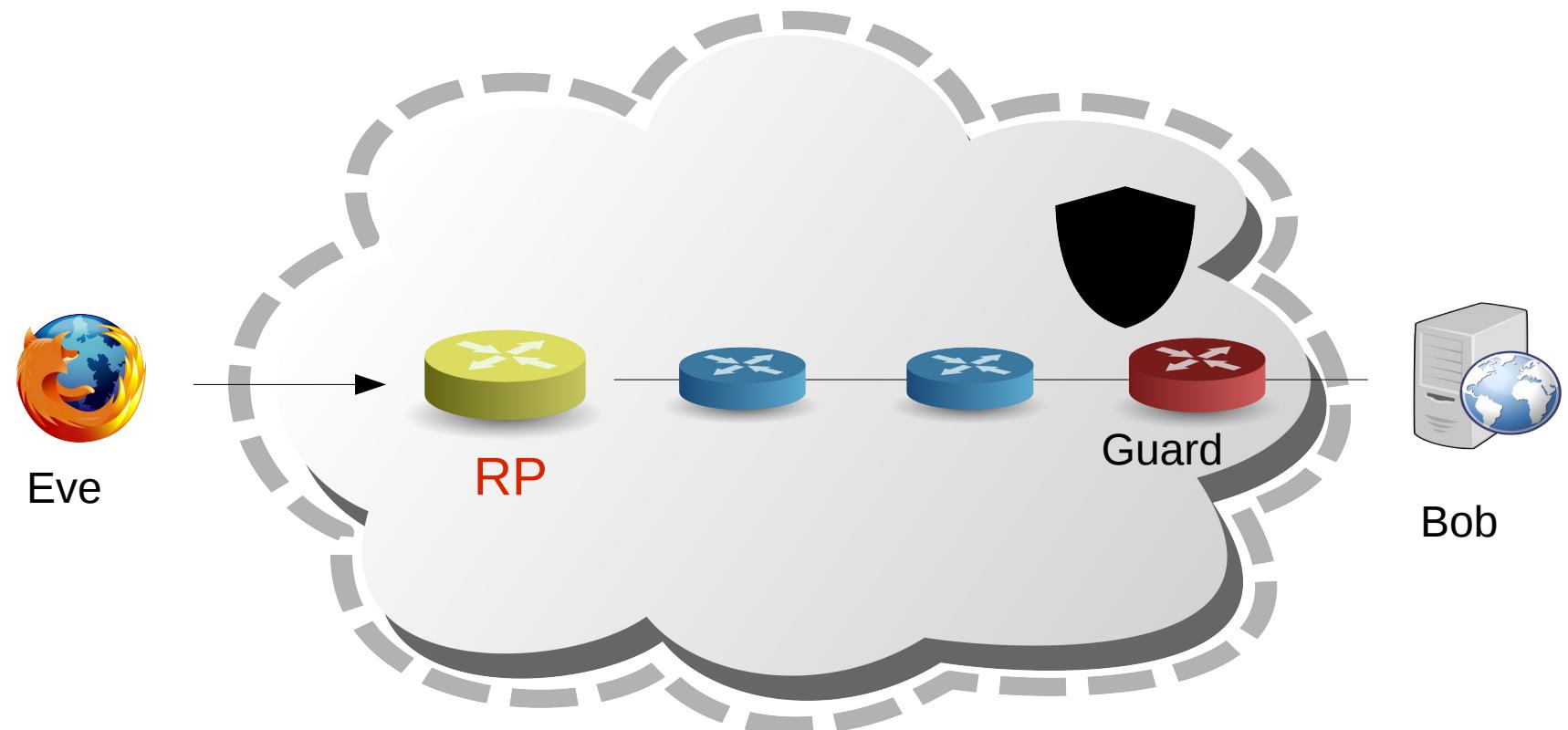


Revealing Guard Nodes

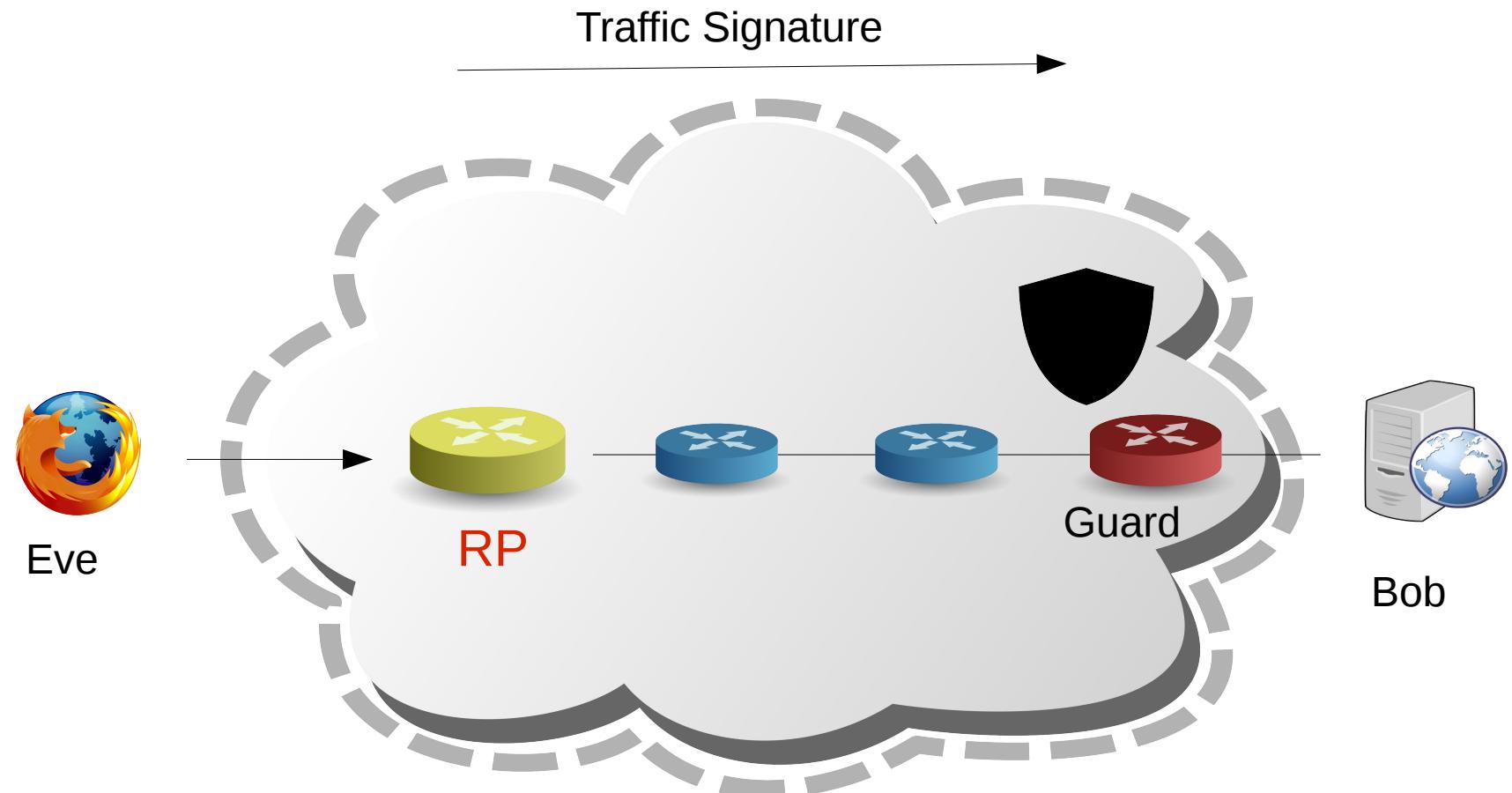


~40 minutes to reveal the guard nodes for a 5Mb/s node

Opportunistic deanonymisation



Opportunistic deanonymisation



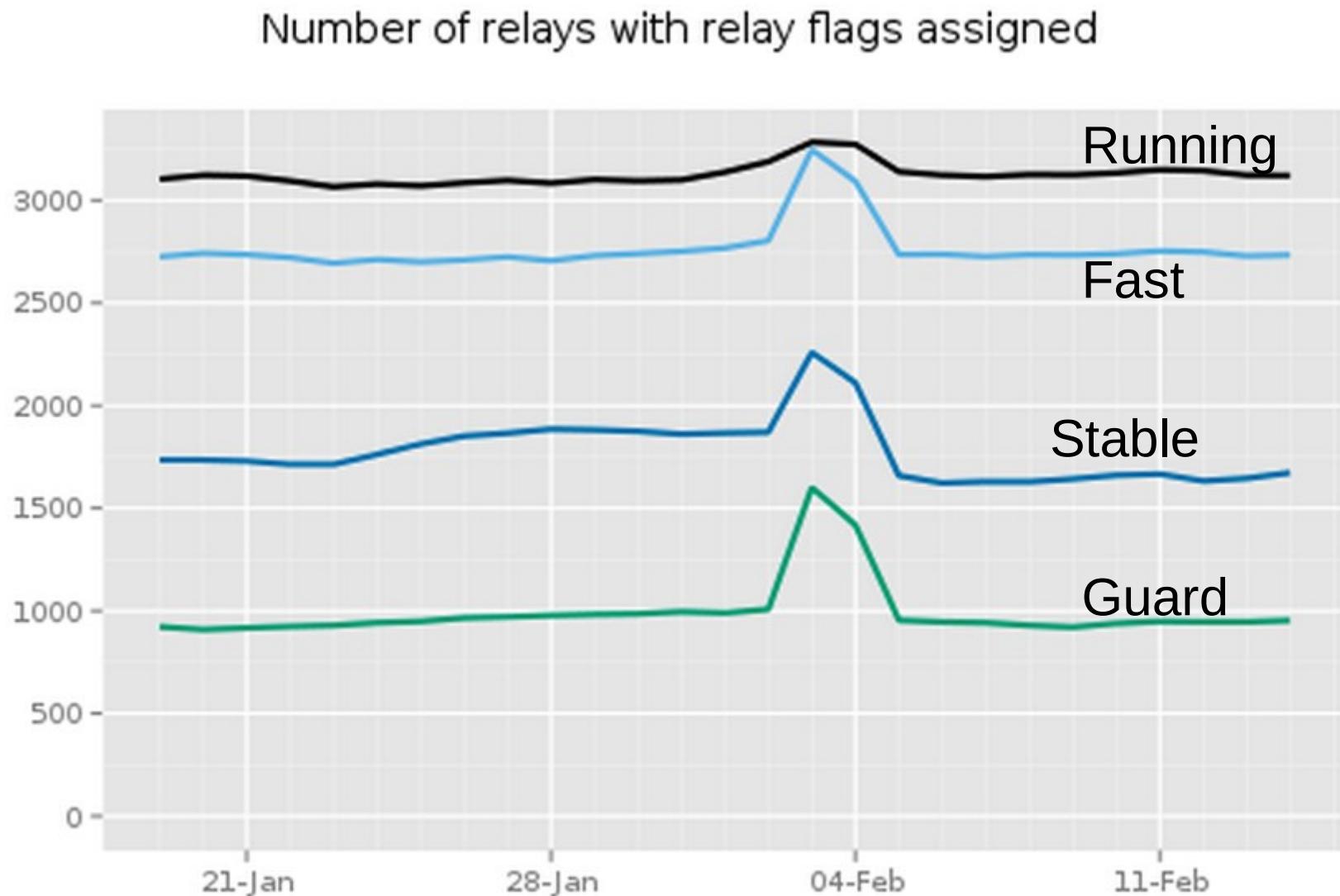
How long does it take to become
a Guard of a hidden service?

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