

# The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network

*Network and Distributed System  
Security Symposium  
February 25<sup>th</sup>, 2014*

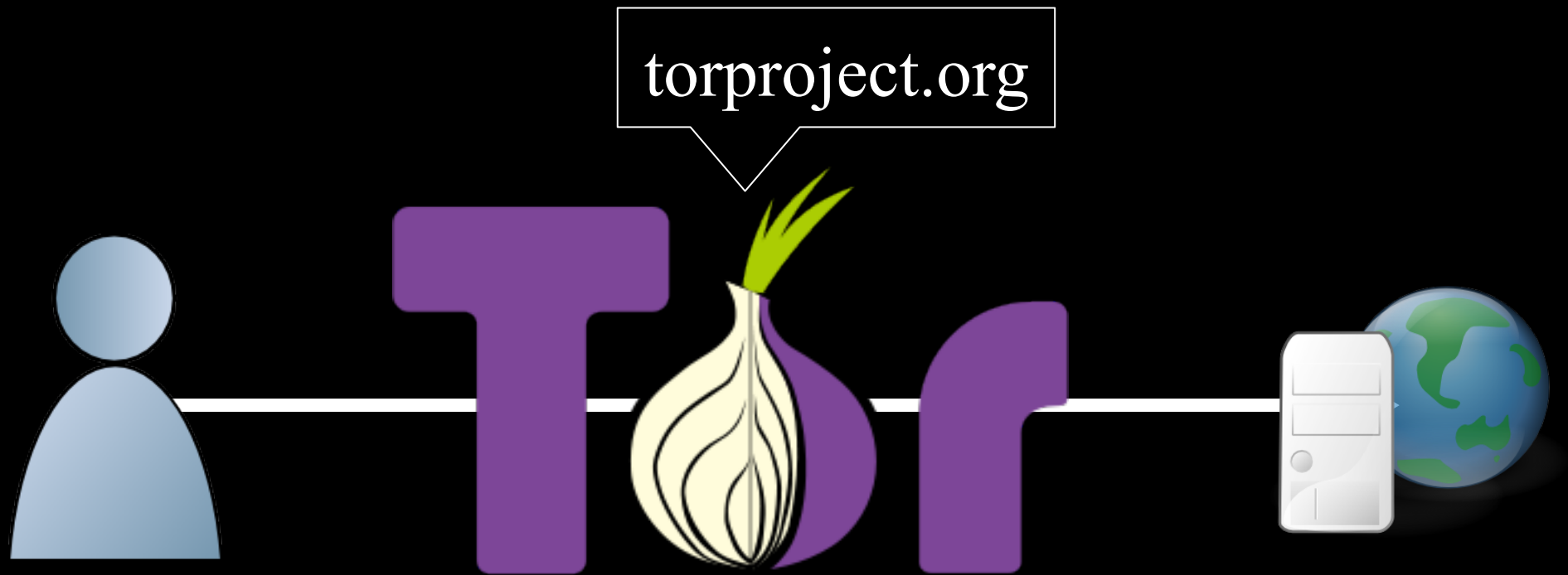


**Rob Jansen**<sup>1</sup>, Florian Tschorsch<sup>2</sup>,  
Aaron Johnson<sup>1</sup>, Björn Scheuermann<sup>2</sup>

<sup>1</sup>U.S. Naval Research Laboratory

<sup>2</sup>Humboldt University of Berlin

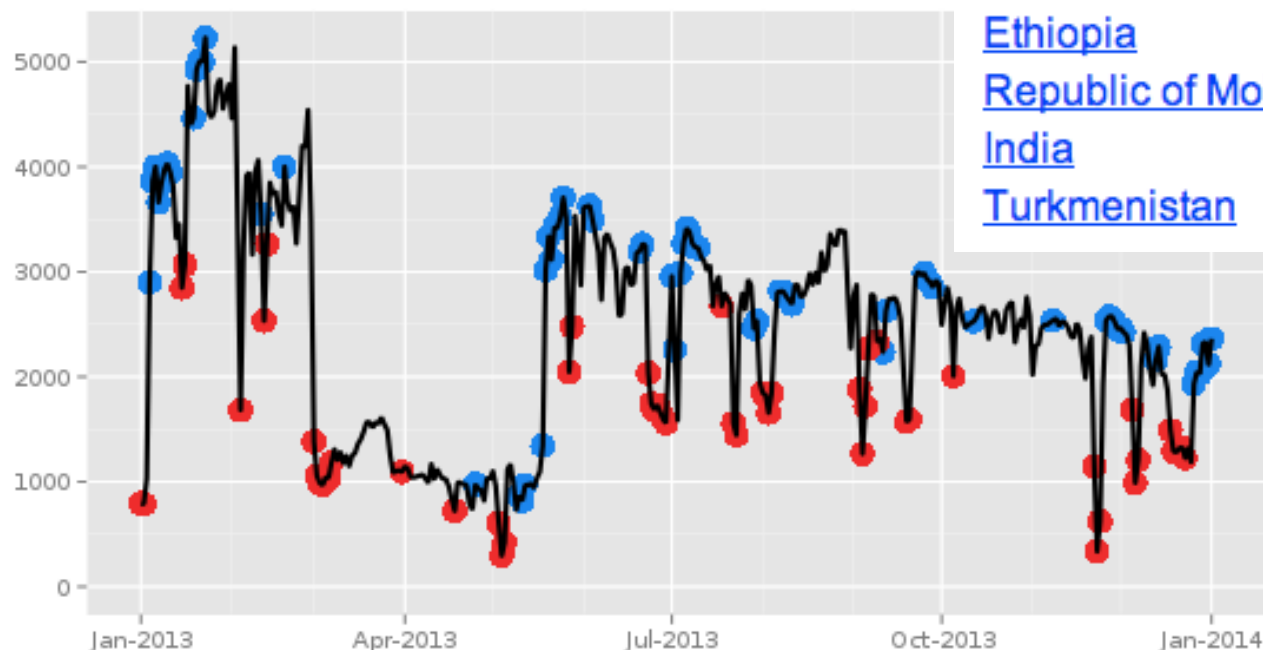
# The Tor Anonymity Network



# Censorship Arms Race

Country	Downturns	Upturns
<a href="#">China</a>	55	69
<a href="#">South Africa</a>	53	50
<a href="#">Iran</a>	47	33
<a href="#">Syrian Arab Republic</a>	28	46
<a href="#">United Republic of Tanzania</a>	27	42
<a href="#">no-man's-land</a>	20	26
<a href="#">Ethiopia</a>	14	7
<a href="#">Republic of Moldova</a>	12	17
<a href="#">India</a>	11	14
<a href="#">Turkmenistan</a>	11	5

Directly connecting users from China



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

# Censorship Arms Race

This screenshot shows a Google Scholar search for 'censorship circumvention' in 2013. The search bar contains the text 'censorship circumvention'. Below the search bar, the word 'Scholar' is visible on the left, and the text 'About 929 results (0.05 sec)' is displayed on the right. A black callout box with the year '2013' in yellow text points to the search results area.

Google

censorship circumvention

Scholar

About 929 results (0.05 sec)

2013

This screenshot shows a Google Scholar search for 'censorship circumvention' in 2014. The search bar contains the text 'censorship circumvention'. Below the search bar, the word 'Scholar' is visible on the left, and the text 'About 72 results (0.04 sec)' is displayed on the right. A black callout box with the year '2014' in yellow text points to the search results area.

Google

censorship circumvention

Scholar

About 72 results (0.04 sec)

2014

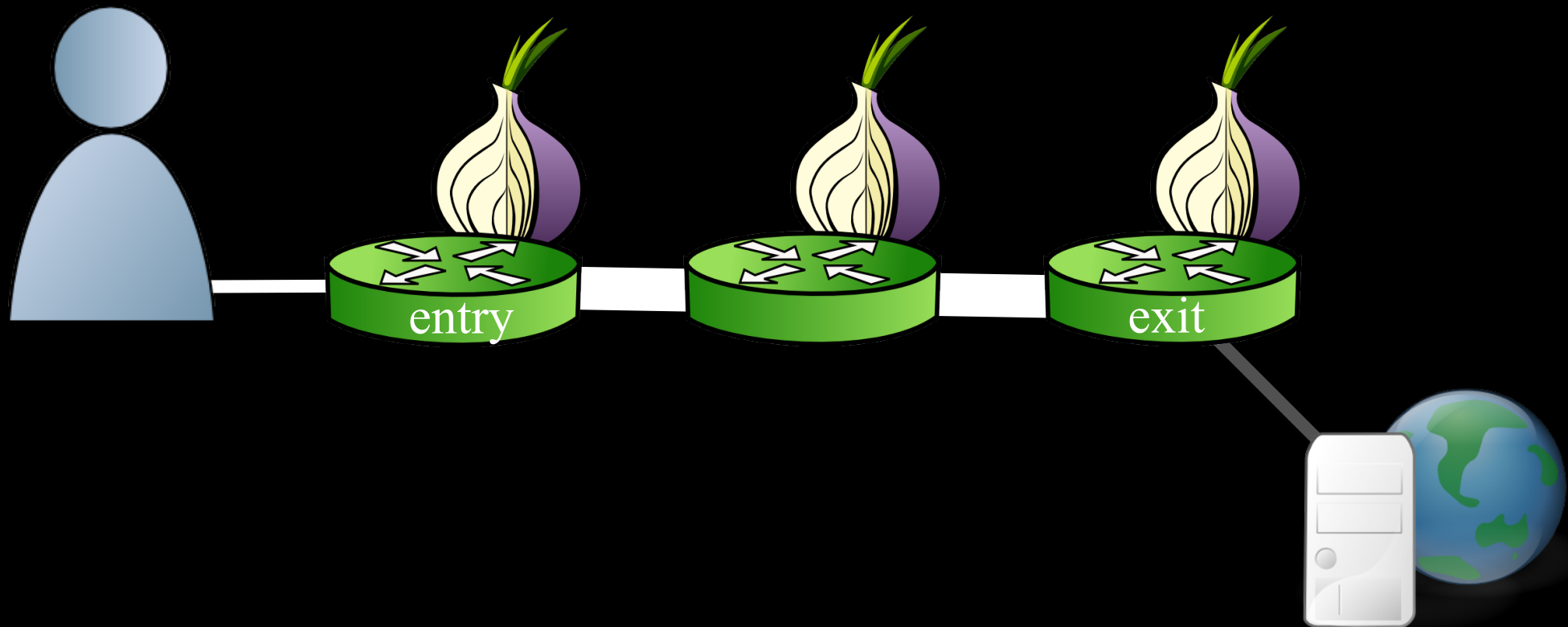
# Beyond the Finish Line

- As the **cost** to block access increases, a viable alternative is to **degrade service**
- **Active** attacks are increasingly pervasive
- Understanding the attack space and **how to defend** is vital to Tor's continued resilience:
  - As adversaries become increasingly **sophisticated**
  - When attacks **subvert explicit security goals**

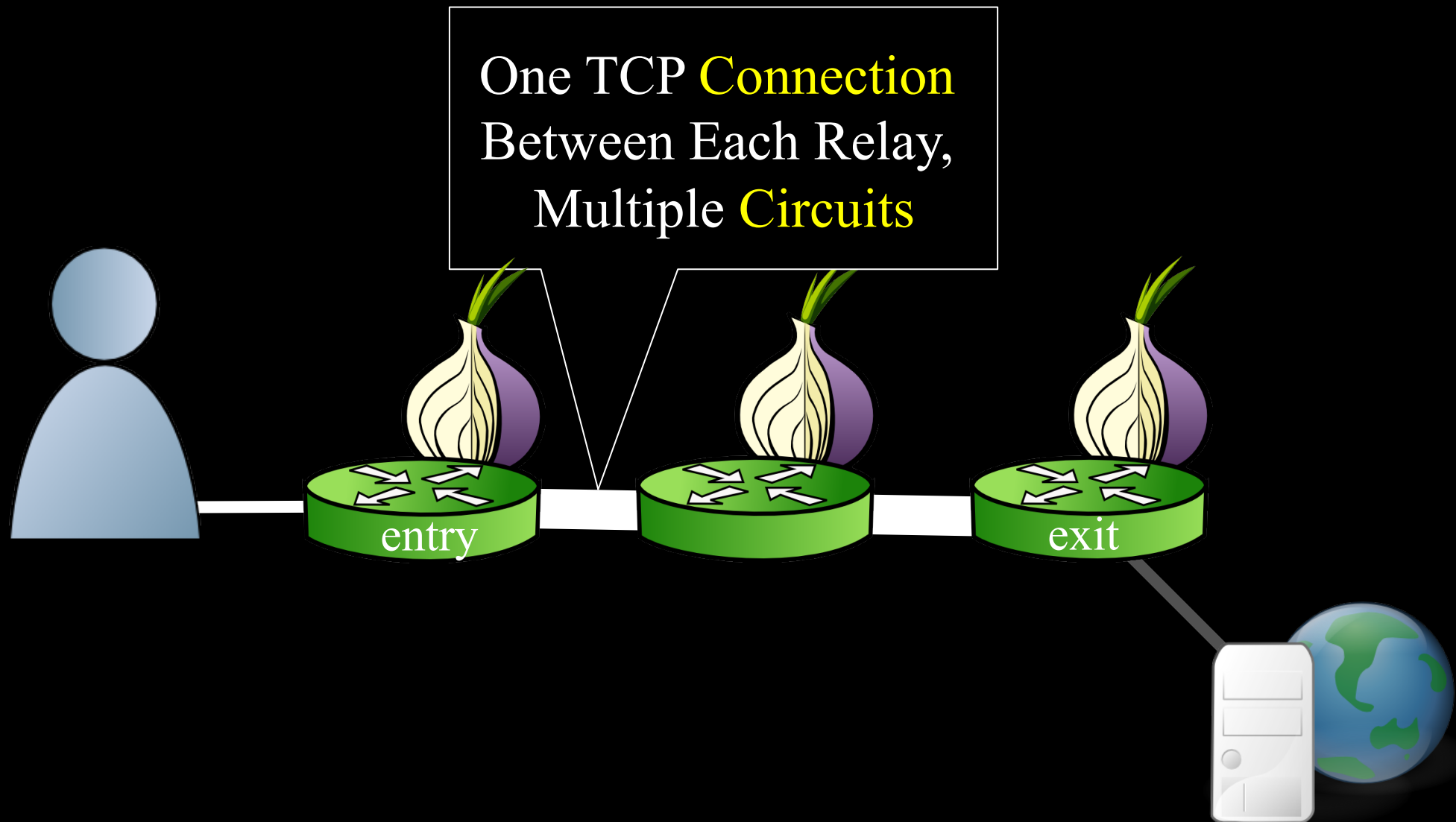
# Outline

- Background
- The Sniper DoS Attack Against Tor's Flow Control Protocol
- How DoS Leads to Hidden Service Deanonymization

# Tor Background

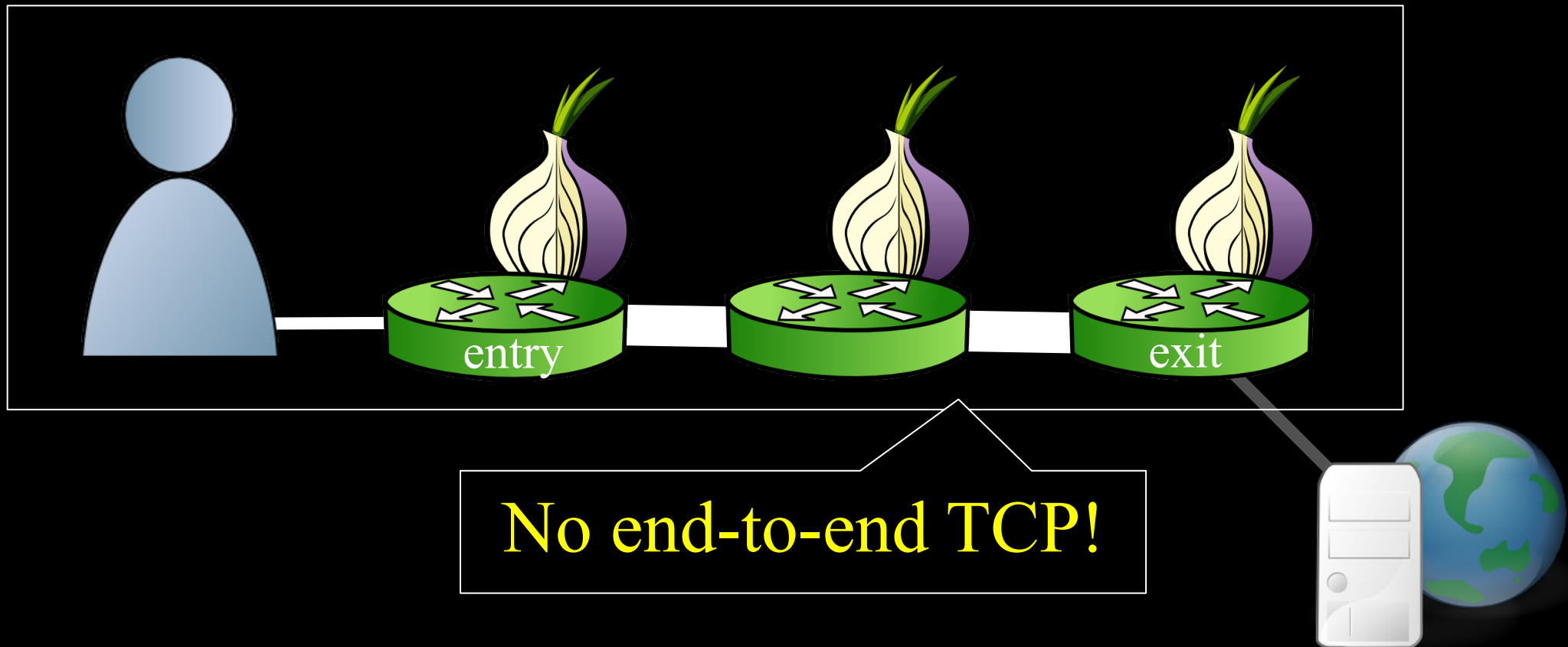


# Tor Background





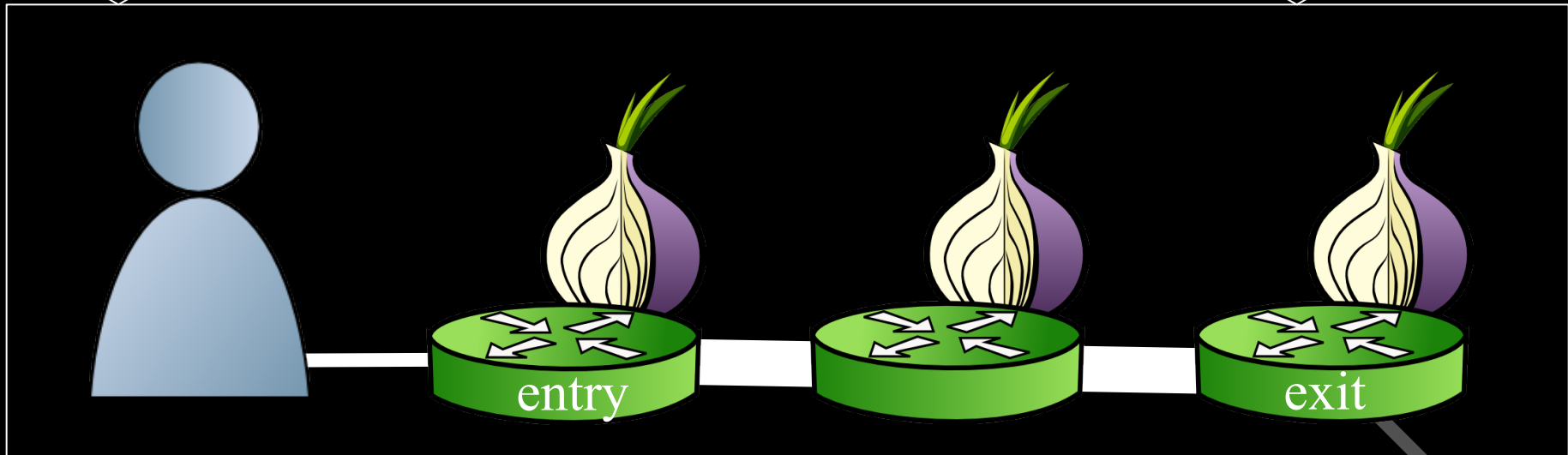
# Tor Background



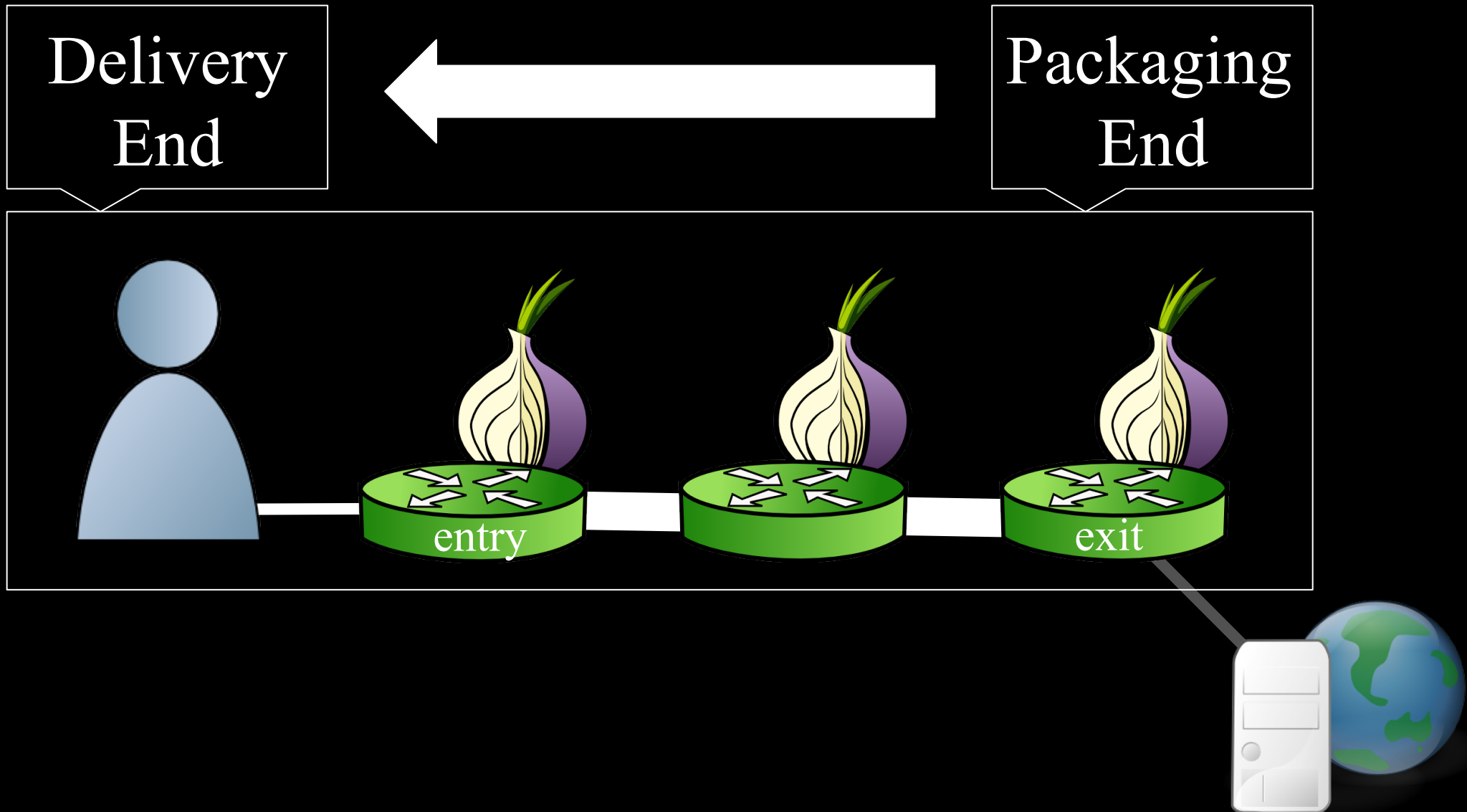
# Tor Flow Control

Delivery  
End

Packaging  
End



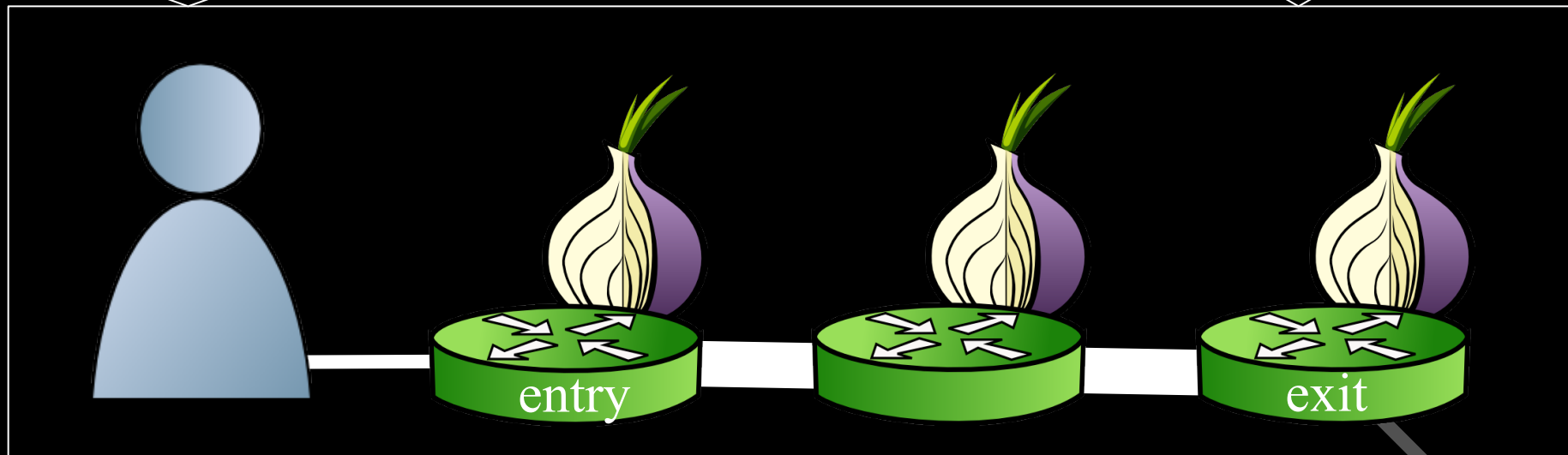
# Tor Flow Control



# Tor Flow Control

SENDME Signal  
Every 100 Cells

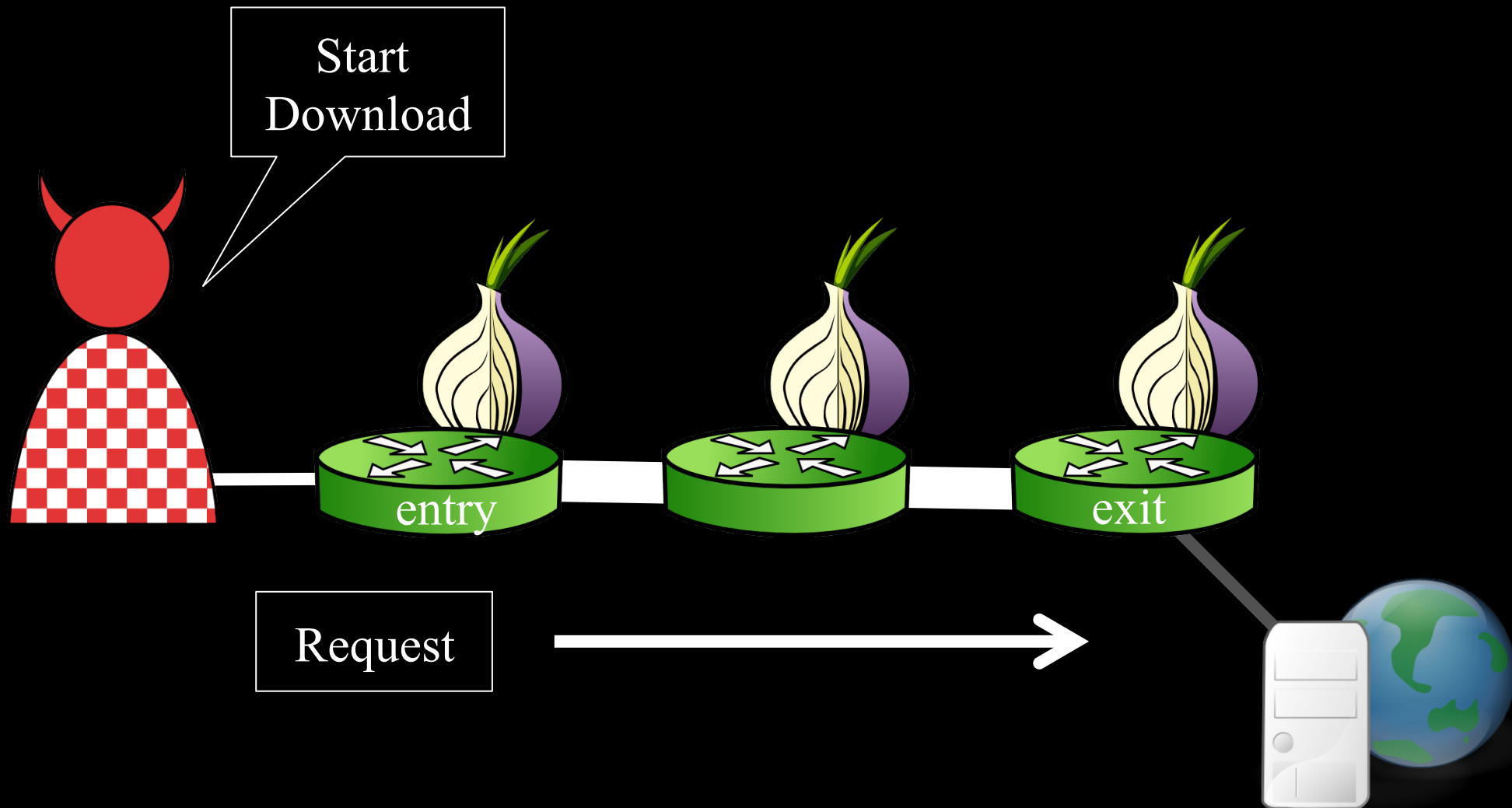
1000 Cell  
Limit



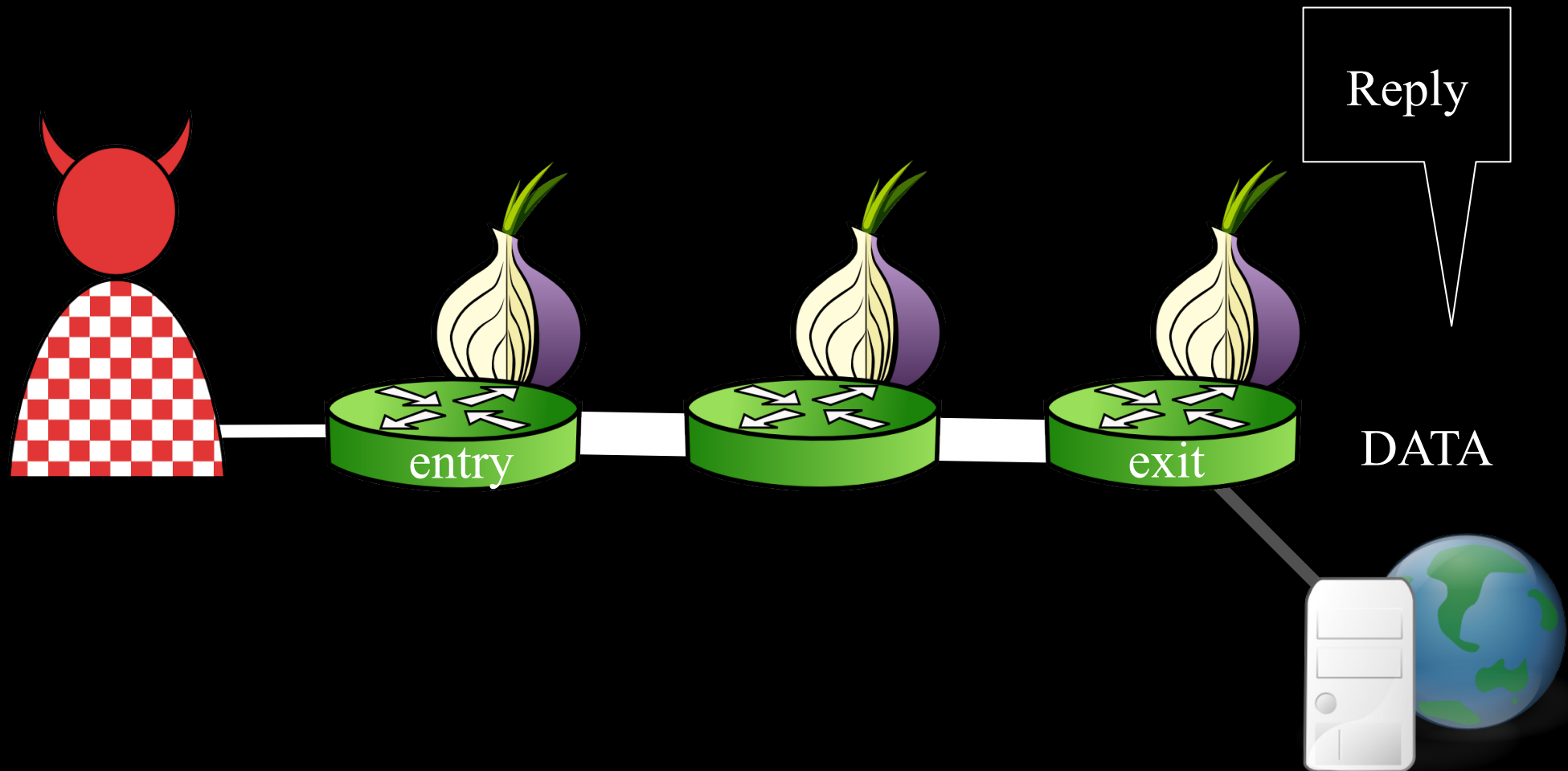
# The Sniper Attack

- Memory-based **denial of service** (DoS) attack
- Exploits vulnerabilities in Tor's **flow control** protocol
- Can be used to **disable** arbitrary Tor relays

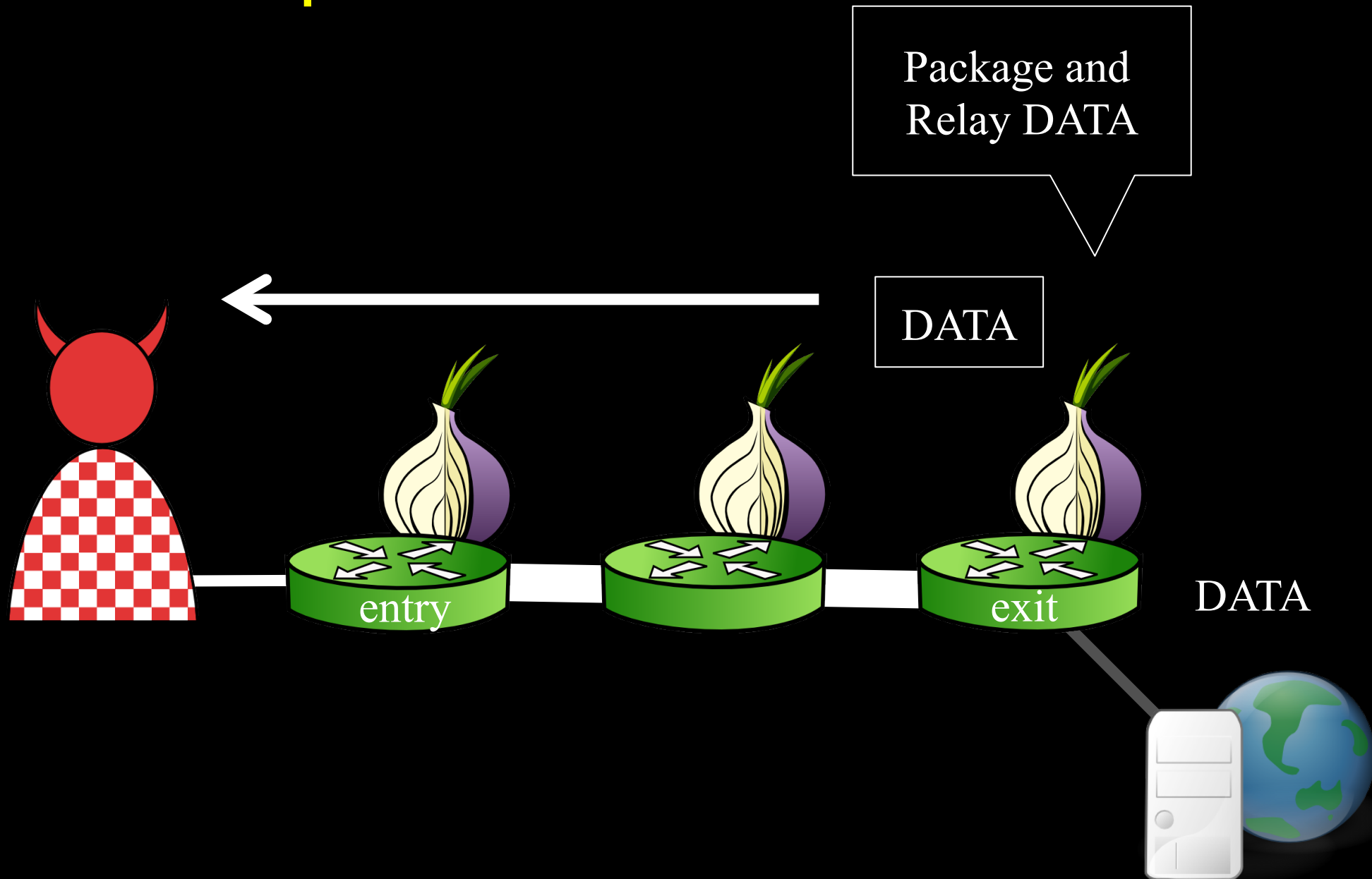
# The Sniper Attack



# The Sniper Attack

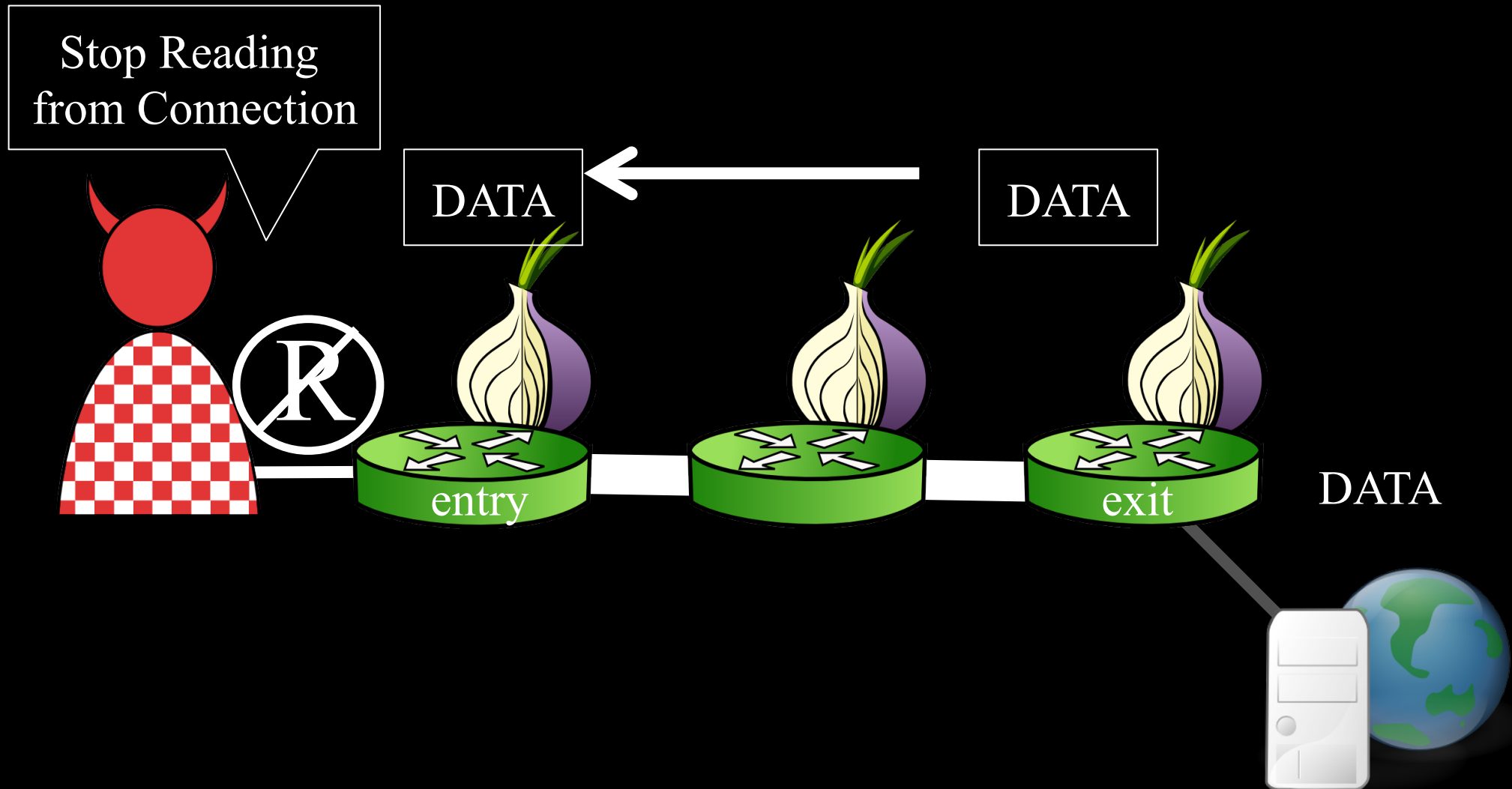


# The Sniper Attack

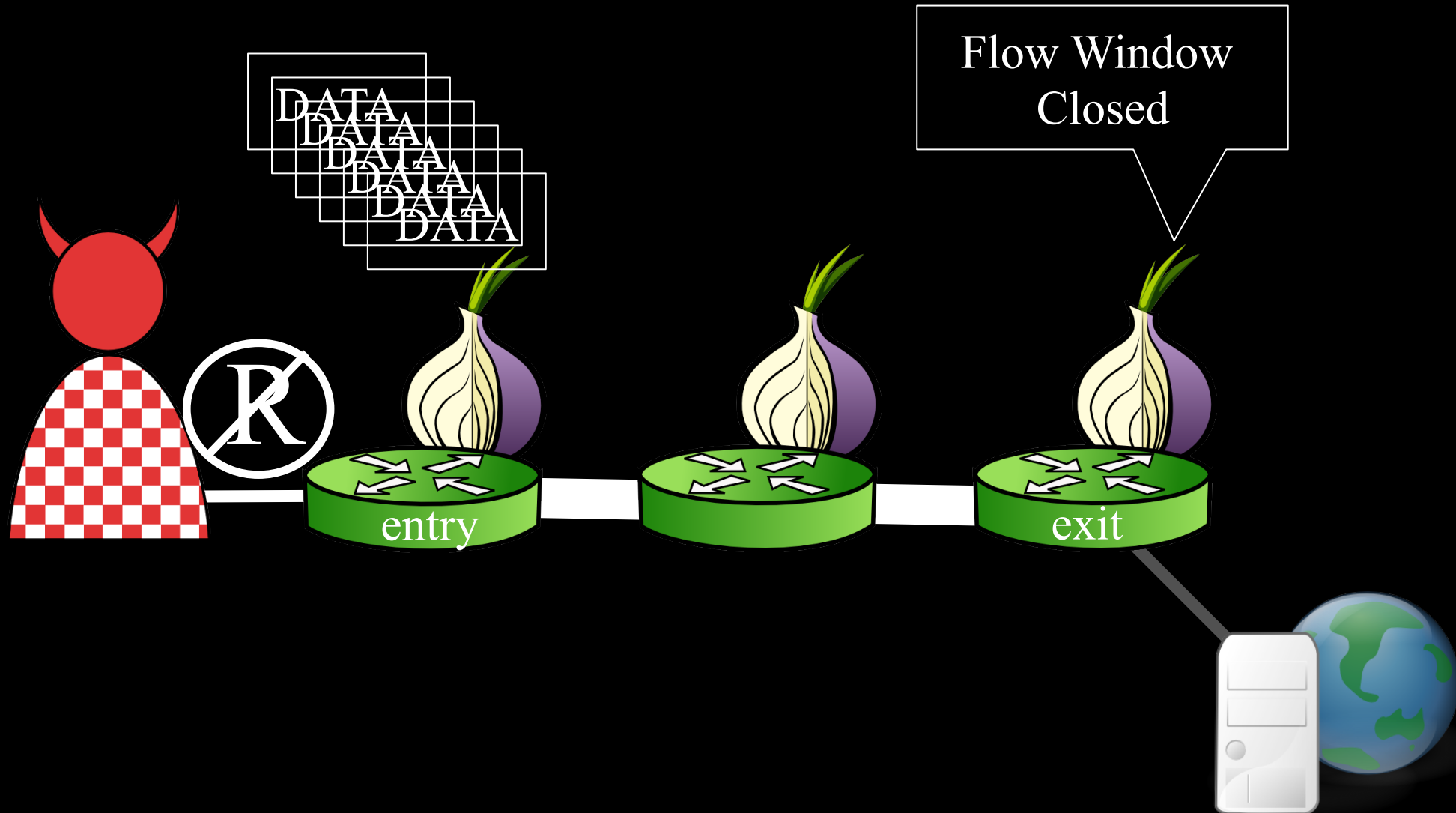




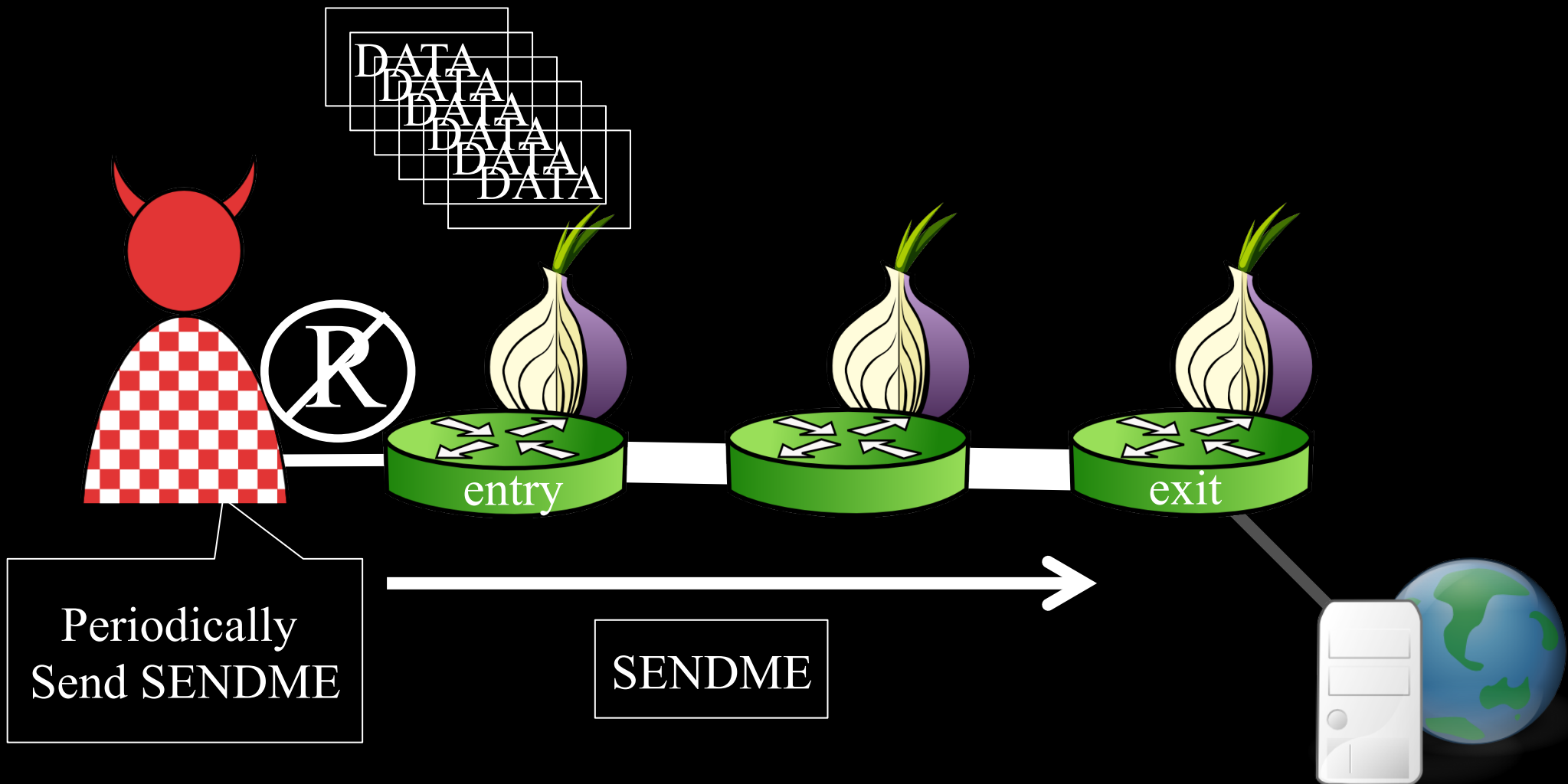
# The Sniper Attack



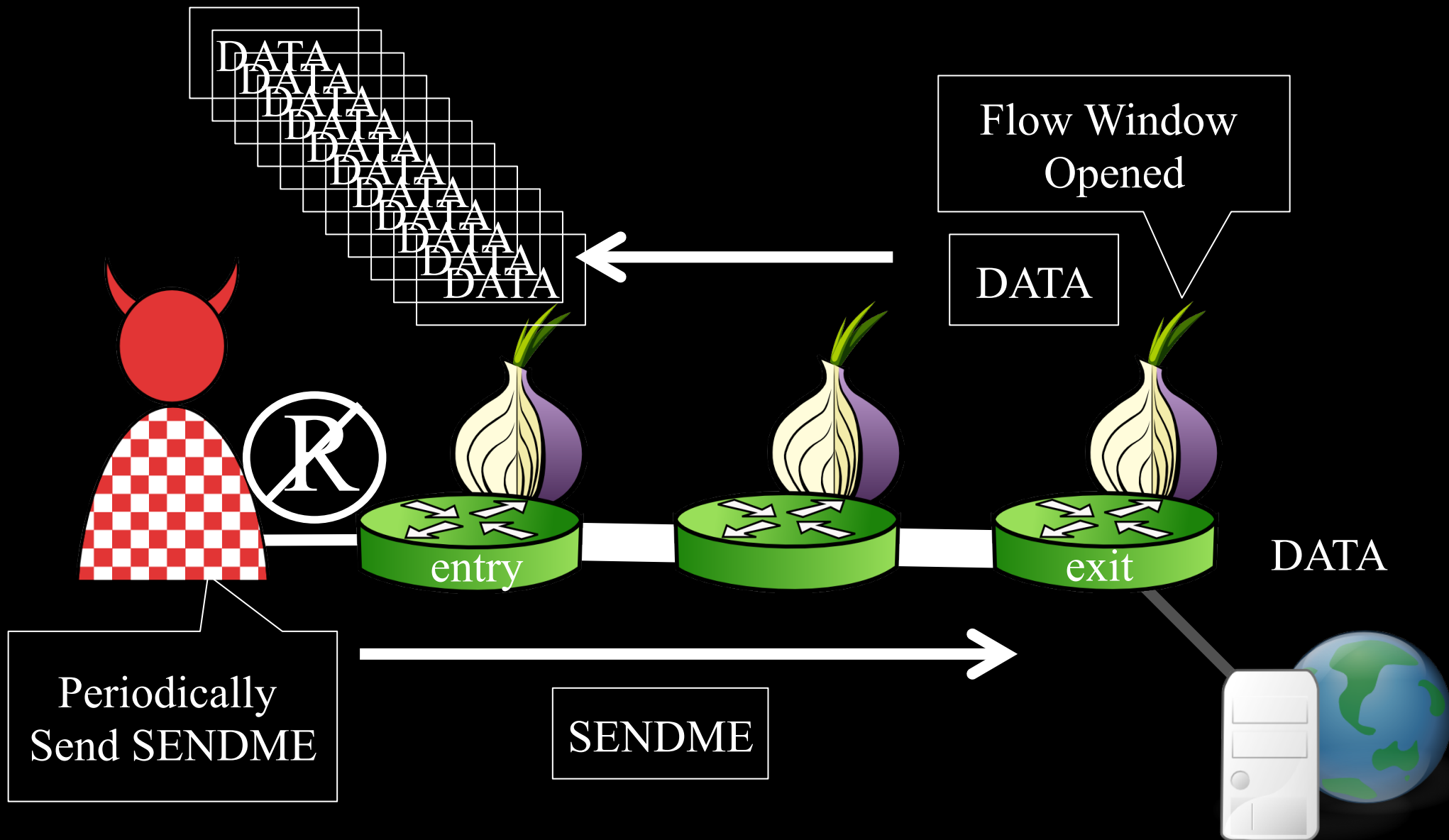
# The Sniper Attack



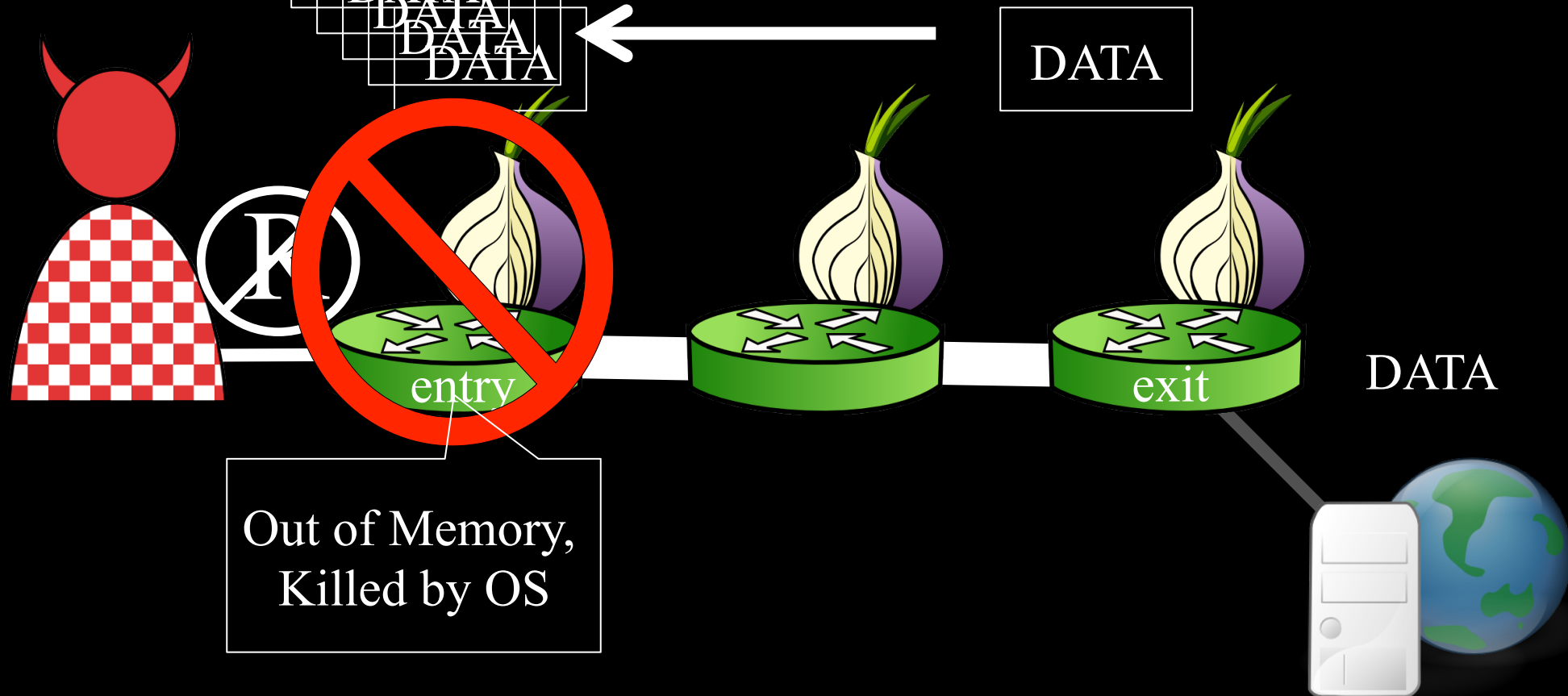
# The Sniper Attack



# The Sniper Attack



# The Sniper Attack

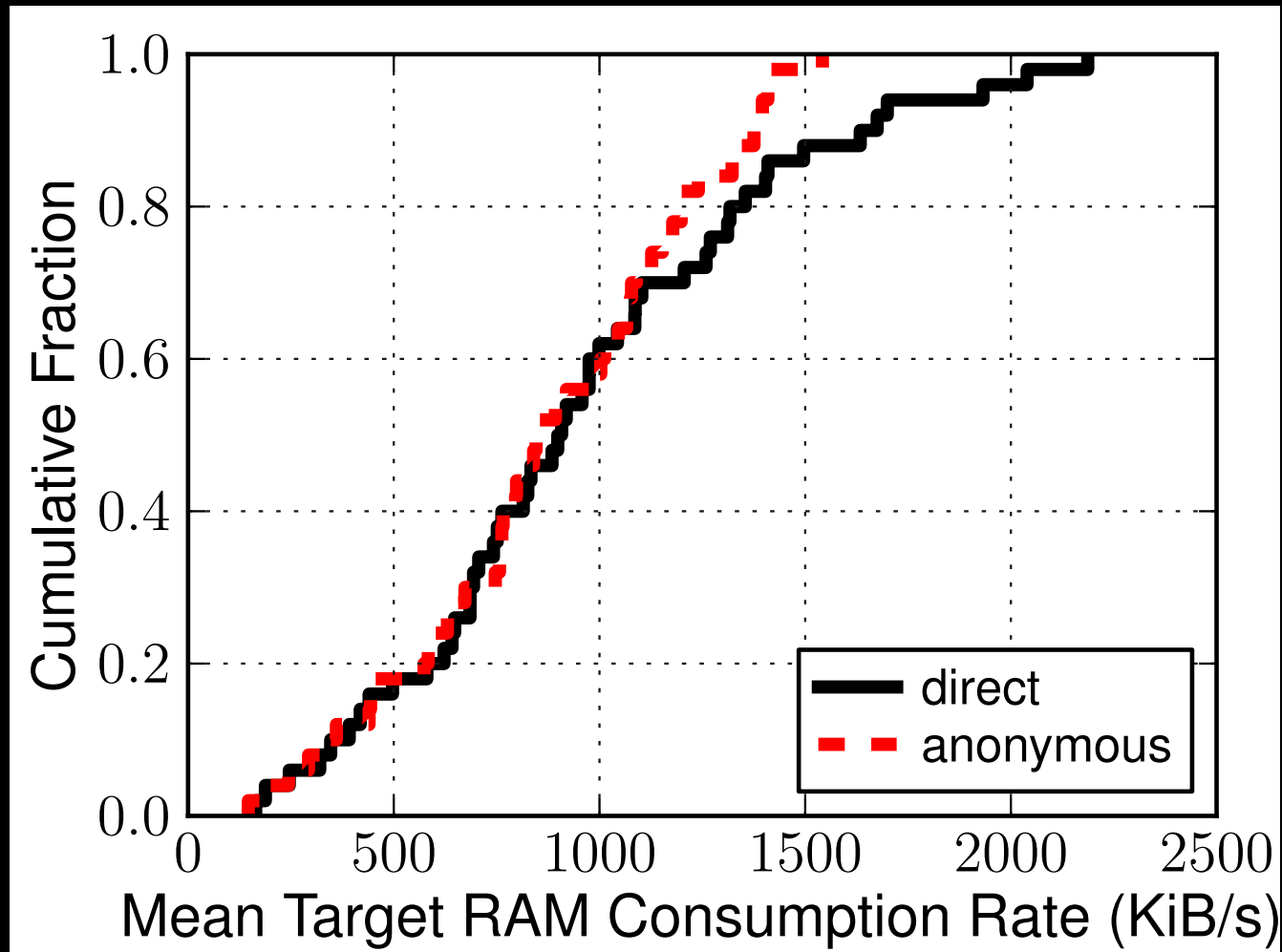




# The Sniper Attack: Results

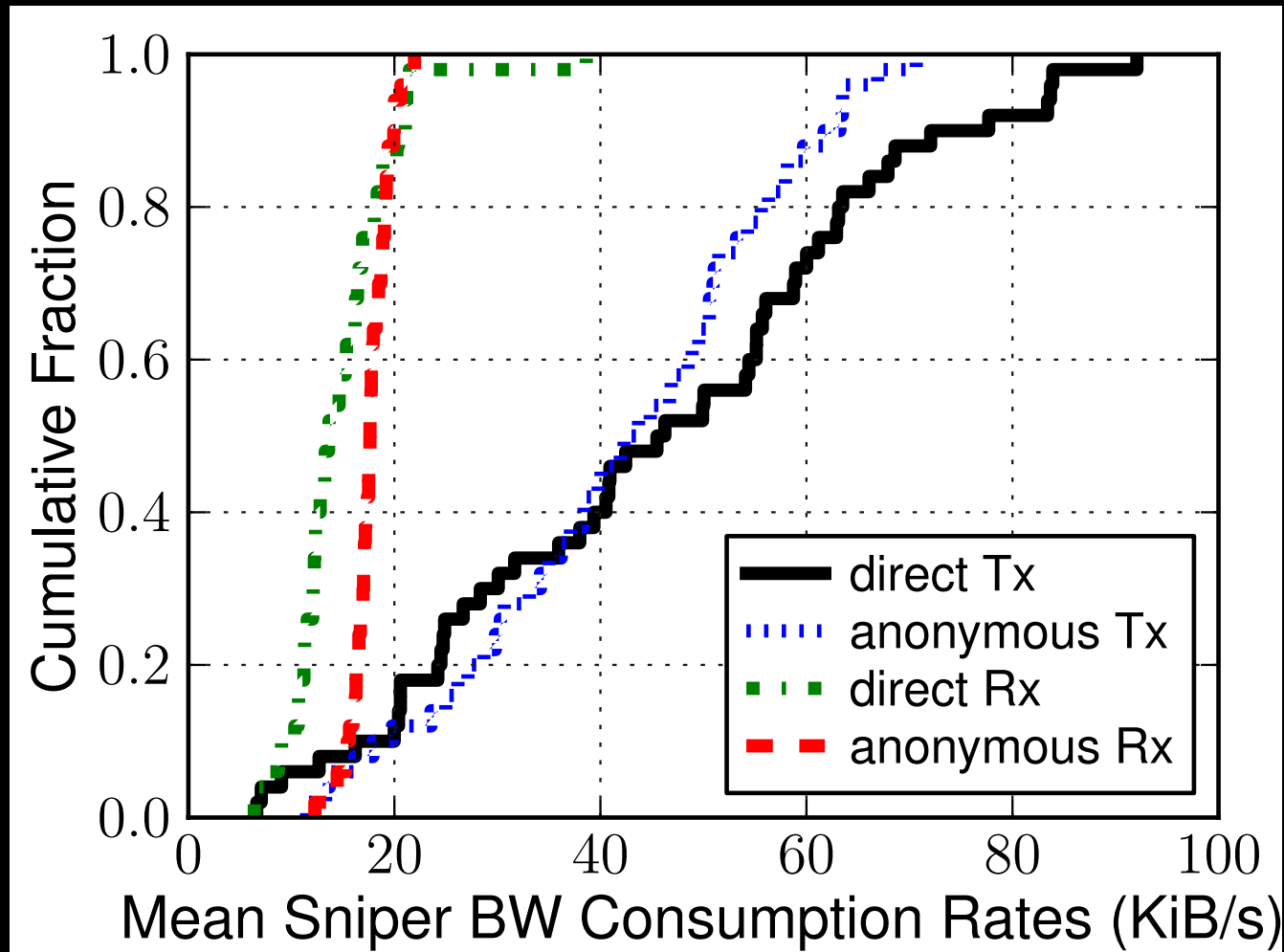
- Implemented Sniper Attack **Prototype**
  - Control Sybils via Tor Control Protocol
- Tested in **Shadow** ([shadow.github.io](https://shadow.github.io))
- Measured:
  - Victim Memory Consumption Rate
  - Adversary Bandwidth Usage

# Mean RAM Consumed at Victim





# Mean BW Consumed at Adversary



# Speed of Sniper Attack

		Direct		Anonymous	
<u>Relay Groups</u>	<u>Select %</u>	<u>1 GiB</u>	<u>8 GiB</u>	<u>1 GiB</u>	<u>8 GiB</u>
Top Guard	1.7				
Top 5 Guards	6.5				
Top 20 Guards	19				
Top Exit	3.2				
Top 5 Exits	13				
Top 20 Exits	35				

Path Selection Probability  
 $\approx$  Network Capacity

# Speed of Sniper Attack

		Direct		Anonymous	
<u>Relay Groups</u>	<u>Select %</u>	<u>1 GiB</u>	<u>8 GiB</u>	<u>1 GiB</u>	<u>8 GiB</u>
Top Guard	1.7	0:01	0:18	0:02	0:14
Top 5 Guards	6.5	0:08	1:03	0:12	1:37
Top 20 Guards	19	0:45	5:58	1:07	8:56
Top Exit	3.2	0:01	0:08	0:01	0:12
Top 5 Exits	13	0:05	0:37	0:07	0:57
Top 20 Exits	35	0:29	3:50	0:44	5:52

Time (hours:minutes) to  
Consume RAM

# Speed of Sniper Attack

		Direct		Anonymous	
<u>Relay Groups</u>	<u>Select %</u>	<u>1 GiB</u>	<u>8 GiB</u>	<u>1 GiB</u>	<u>8 GiB</u>
Top Guard	1.7	0:01	0:18	0:02	0:14
Top 5 Guards	6.5	0:08	1:03	0:12	1:37
Top 20 Guards	19	0:45	5:58	1:07	8:56
Top Exit	3.2	0:01	0:08	0:01	0:12
Top 5 Exits	13	0:05	0:37	0:07	0:57
Top 20 Exits	35	0:29	3:50	0:44	5:52

Time (hours:minutes) to  
Consume RAM

# Speed of Sniper Attack

		Direct		Anonymous	
<u>Relay Groups</u>	<u>Select %</u>	<u>1 GiB</u>	<u>8 GiB</u>	<u>1 GiB</u>	<u>8 GiB</u>
Top Guard	1.7	0:01	0:18	0:02	0:14
Top 5 Guards	6.5	0:08	1:03	0:12	1:37
Top 20 Guards	19	0:45	5:58	1:07	8:56
Top Exit	3.2	0:01	0:08	0:01	0:12
Top 5 Exits	13	0:05	0:37	0:07	0:57
Top 20 Exits	35	0:29	3:50	0:44	5:52

Time (hours:minutes) to  
Consume RAM

# Speed of Sniper Attack

		Direct		Anonymous	
<u>Relay Groups</u>	<u>Select %</u>	<u>1 GiB</u>	<u>8 GiB</u>	<u>1 GiB</u>	<u>8 GiB</u>
Top Guard	1.7	0:01	0:18	0:02	0:14
Top 5 Guards	6.5	0:08	1:03	0:12	1:37
Top 20 Guards	19	0:45	5:58	1:07	8:56
Top Exit	3.2	0:01	0:08	0:01	0:12
Top 5 Exits	13	0:05	0:37	0:07	0:57
Top 20 Exits	35	0:29	3:50	0:44	5:52

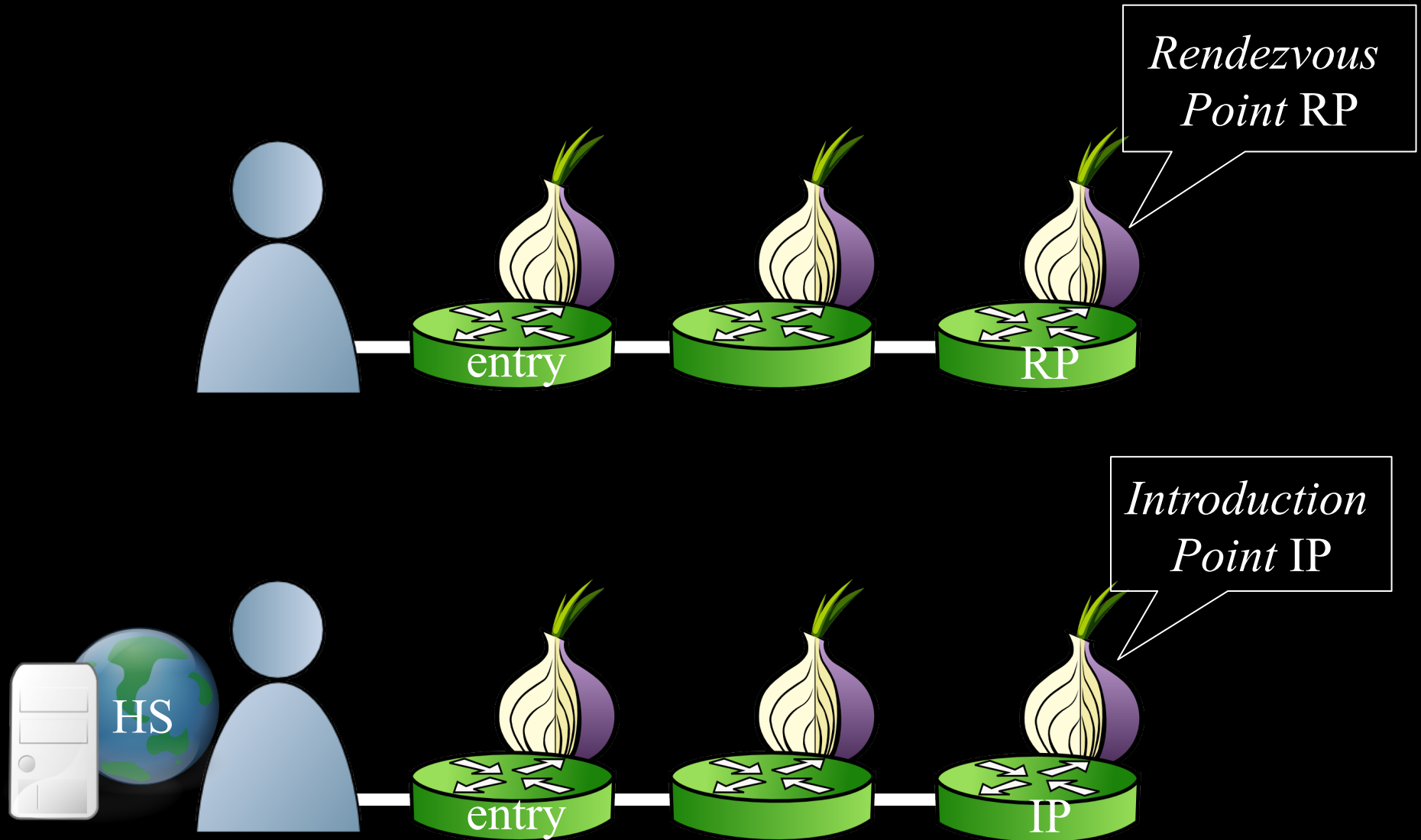
< 1 GiB RAM  
< 50 KiB/s Downstream BW  
< 100 KiB/s Upstream BW

Time (hours:minutes) to  
Consume RAM

# Deanonymizing Hidden Services

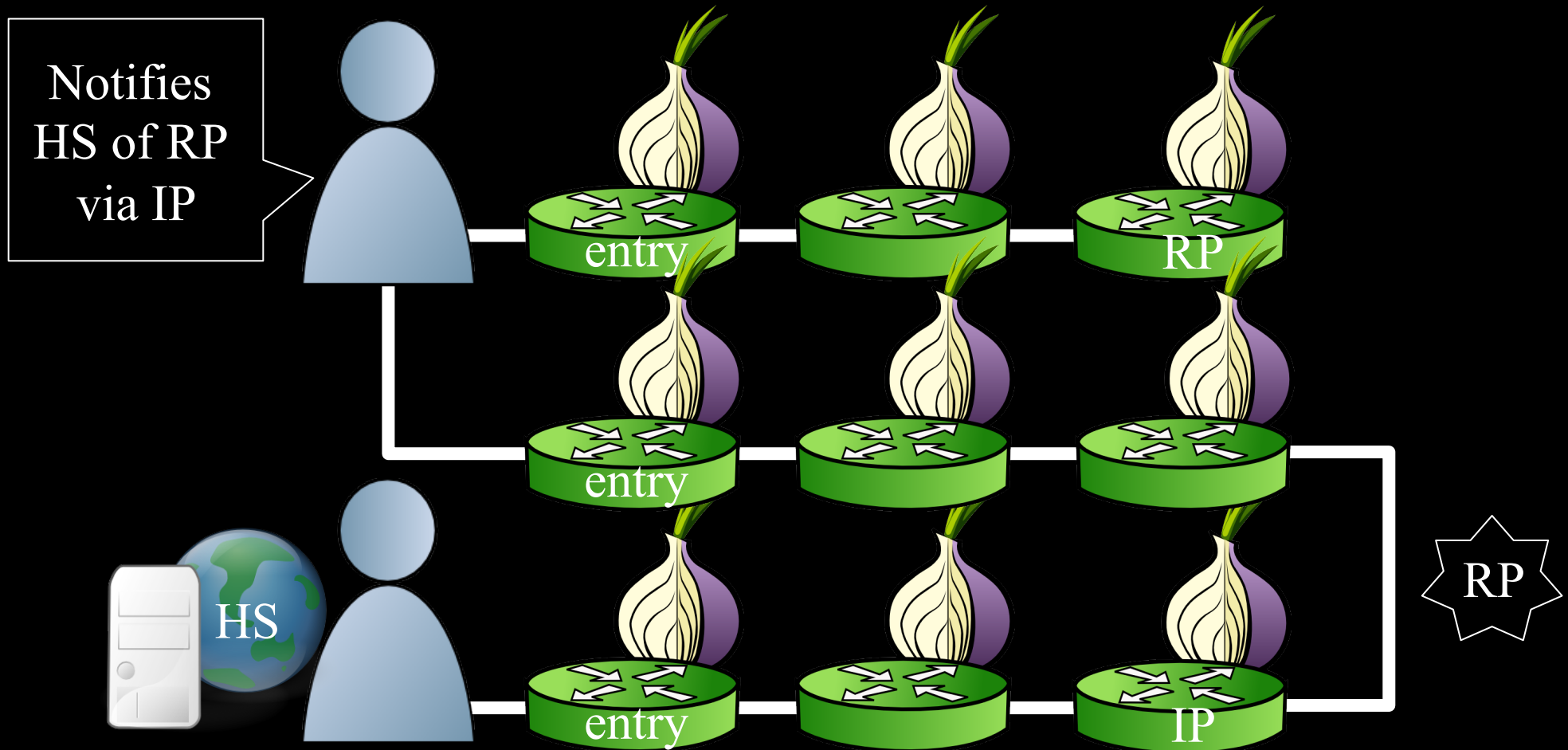
1. Cause HS to build **new** rendezvous circuits to learn its guard
2. Snipe HS guard to force **reselection**
3. Repeat until HS chooses **adversarial** guard

# Hidden Services

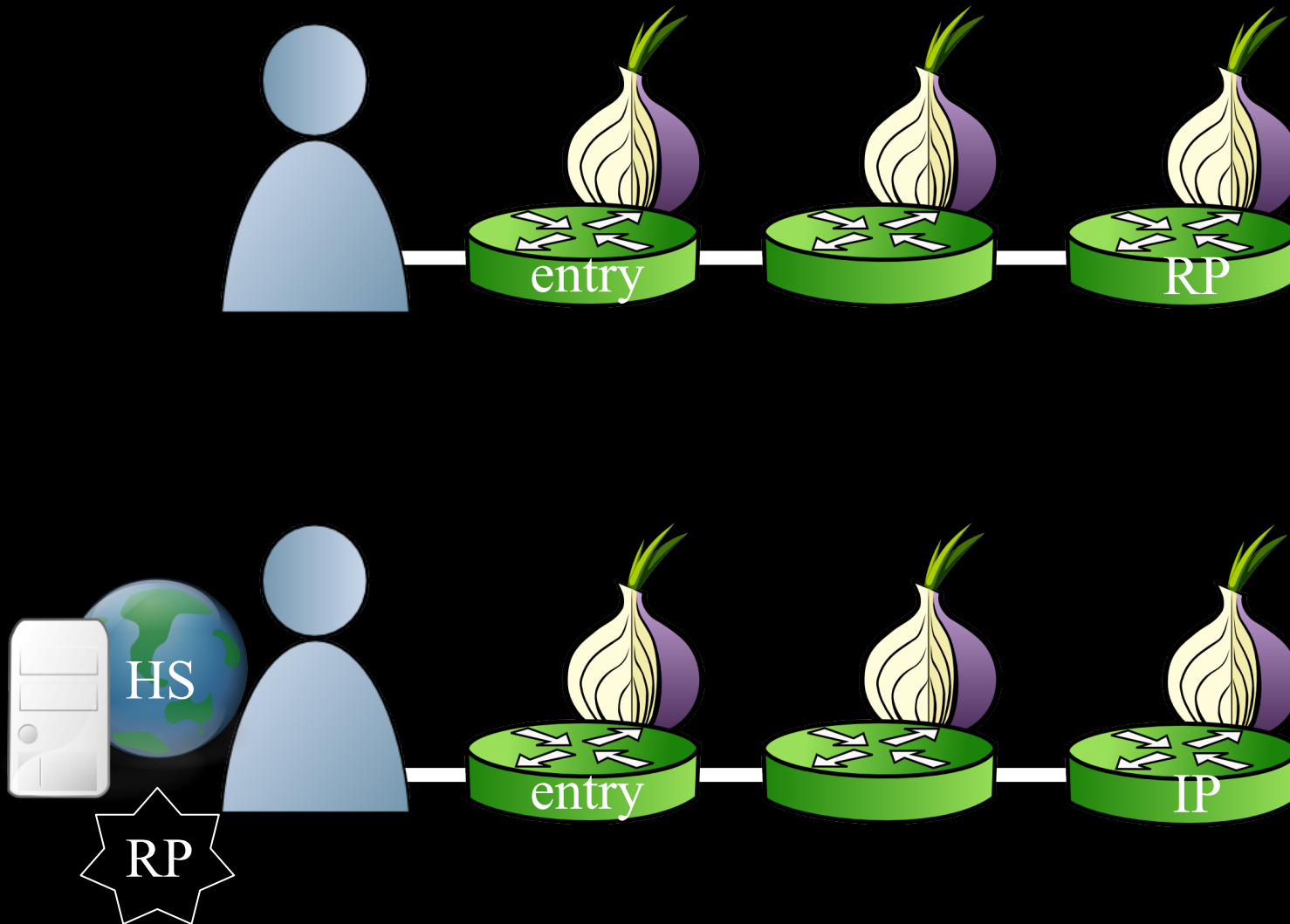




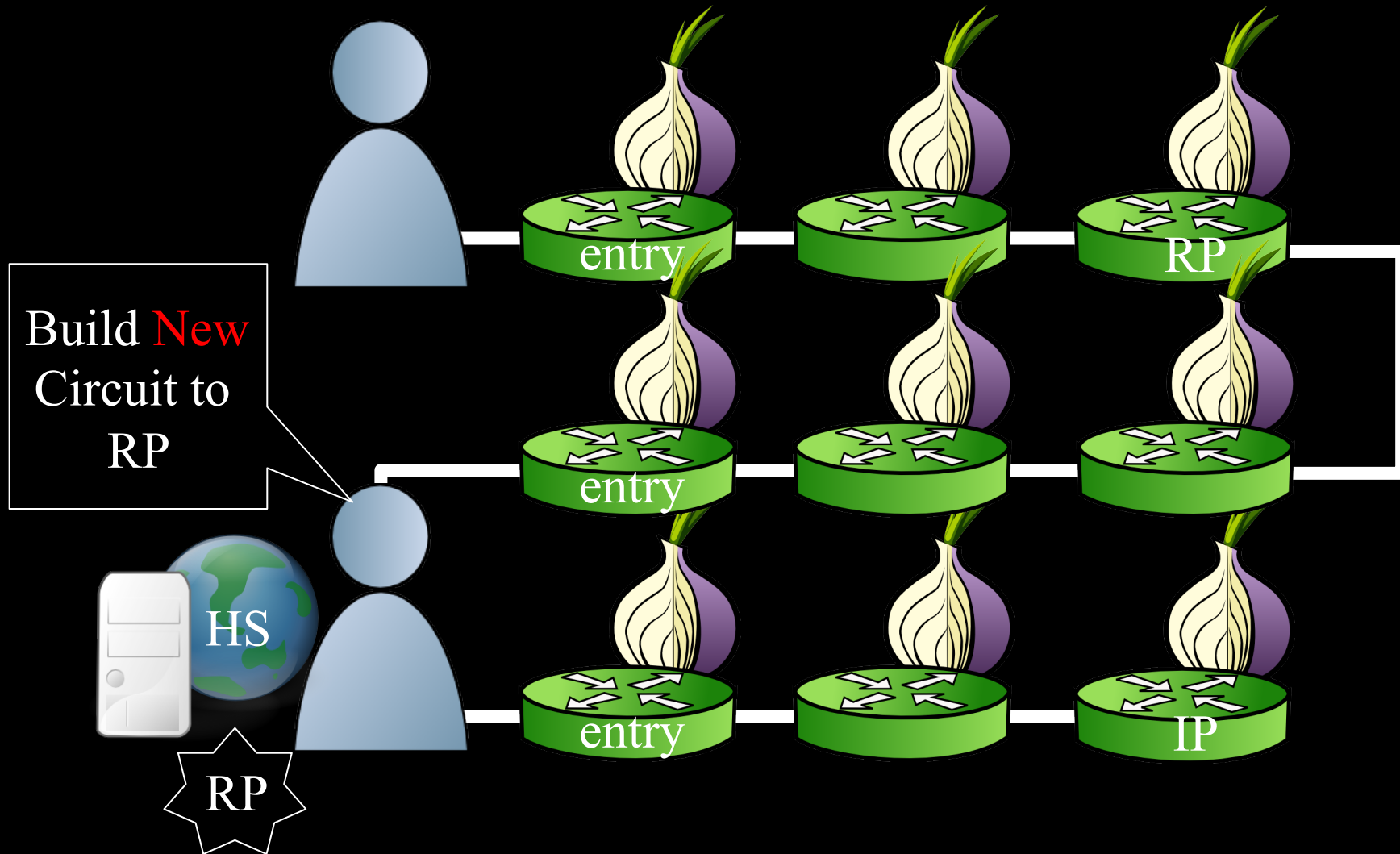
# Hidden Services



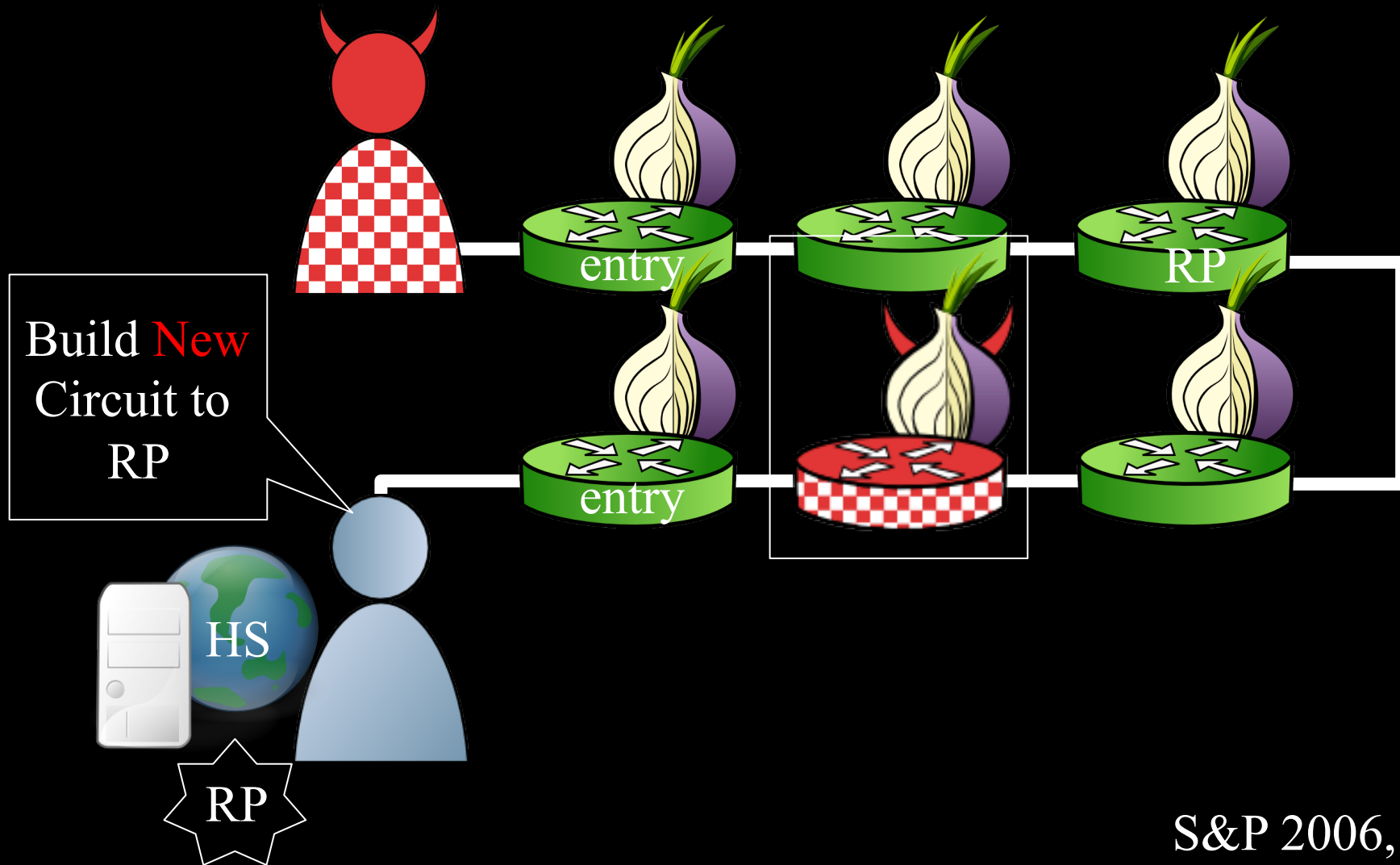
# Hidden Services



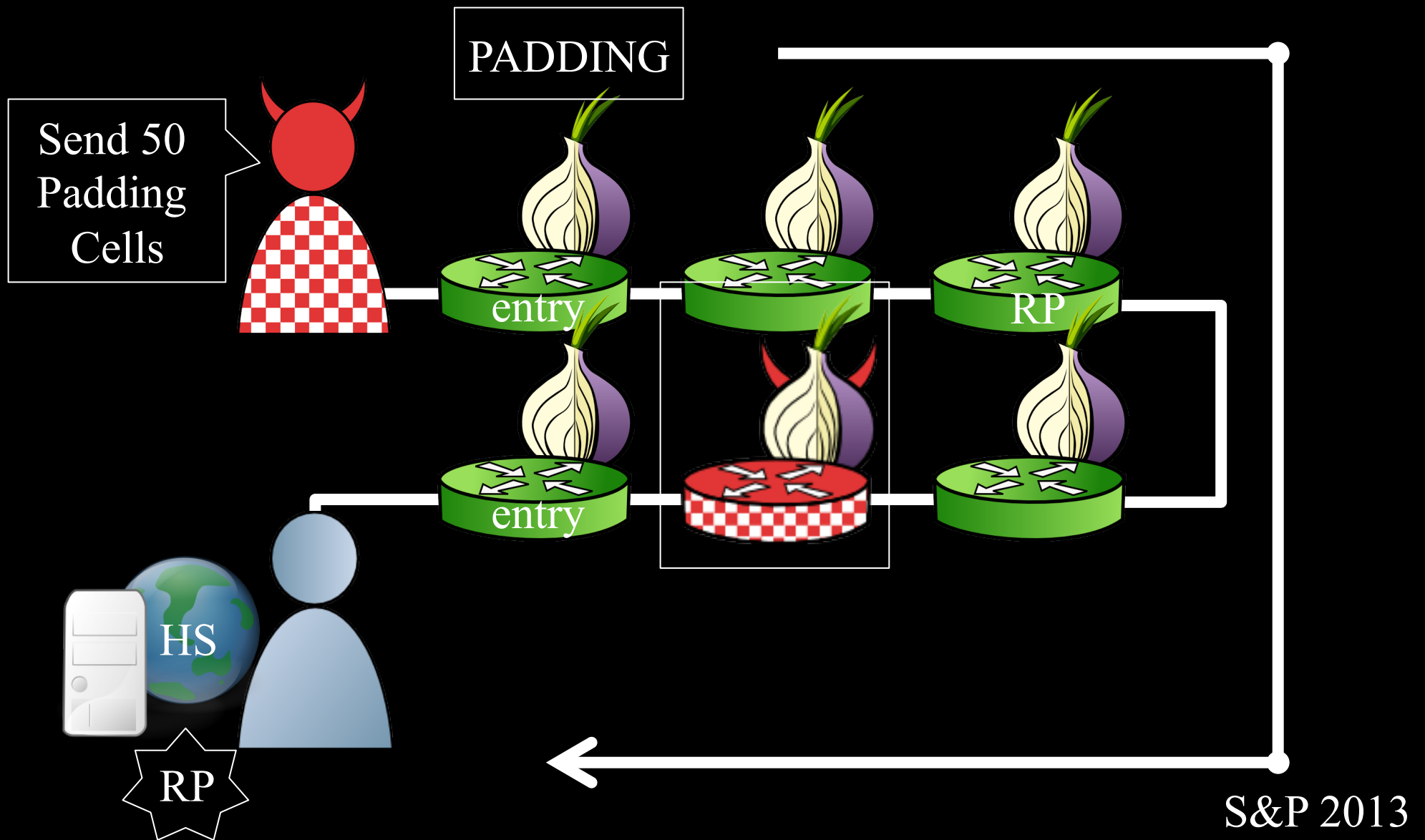
# Hidden Services



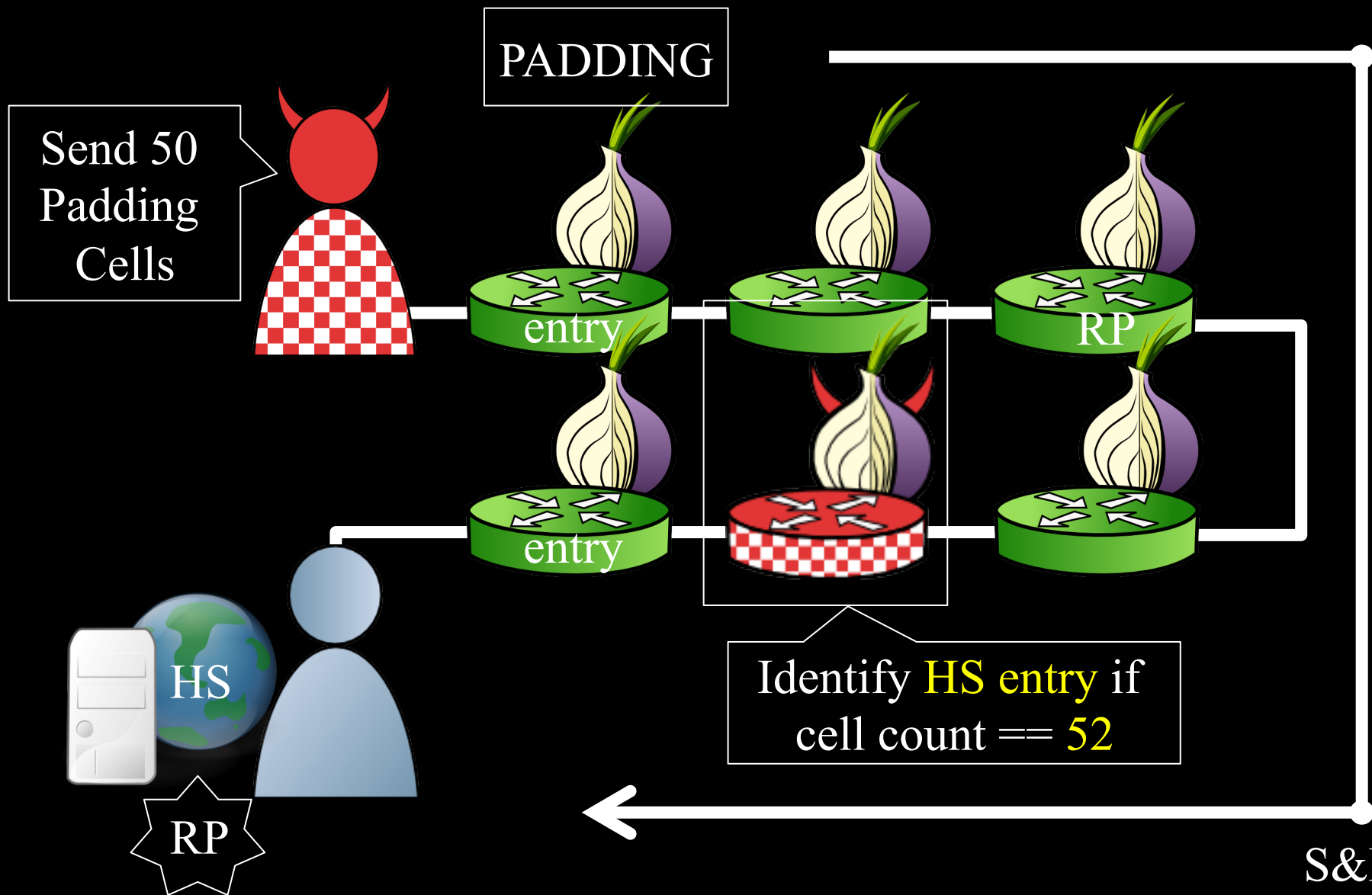
# Deanonymizing Hidden Services



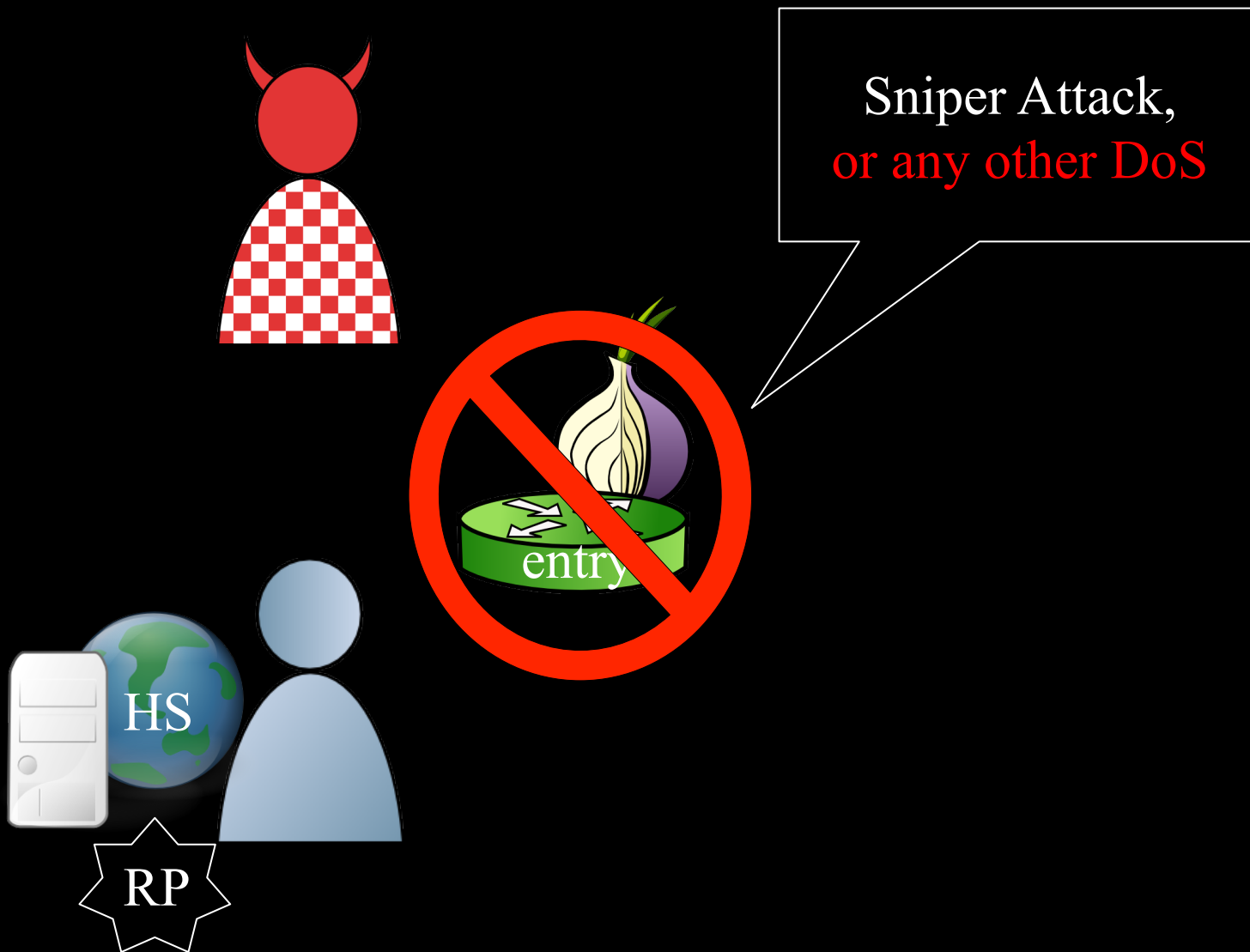
# Deanonymizing Hidden Services



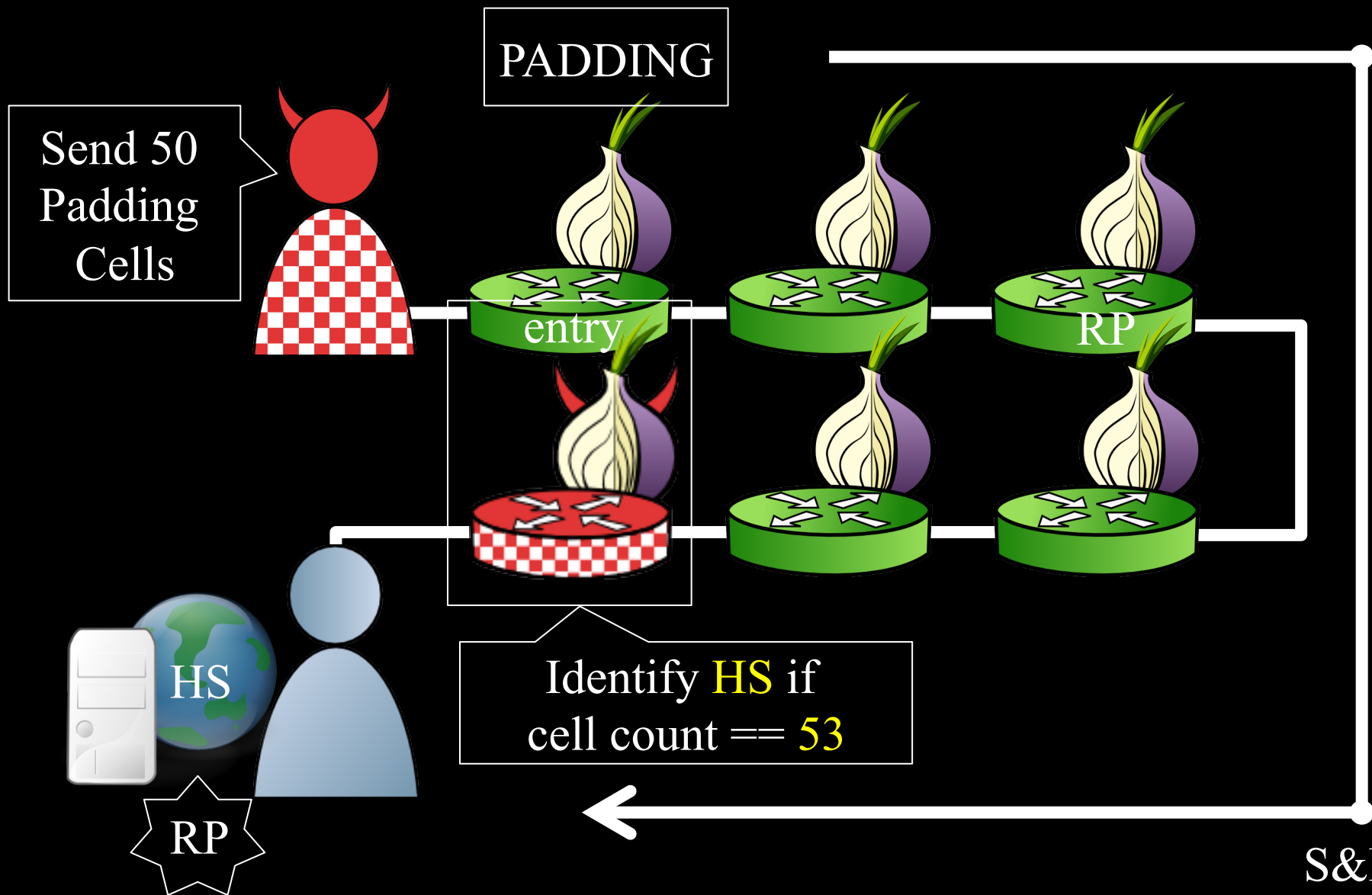
# Deanonymizing Hidden Services



# Deanonymizing Hidden Services



# Deanonymizing Hidden Services





# Speed of Deanononymization

Guard BW (MiB/s)	Guard Probability (%)	Average # Rounds	Average # Sniped	Average Time (h) 1 GiB	Average Time (h) 8 GiB
8.41	0.48				
16.65	0.97				
31.65	1.9				
66.04	3.8				
96.61	5.4				

# Speed of Deanononymization

Guard BW (MiB/s)	Guard Probability (%)	Average # Rounds	Average # Sniped	Average Time (h) 1 GiB	Average Time (h) 8 GiB
8.41	0.48	66	133	46	279
16.65	0.97	39	79	23	149
31.65	1.9	24	48	13	84
66.04	3.8	13	26	6	44
96.61	5.4	9	19	5	31

# Speed of Deanonymization


Guard BW (MiB/s)	Guard Probability (%)	Average # Rounds	Average # Sniped	Average Time (h) 1 GiB	Average Time (h) 8 GiB
8.41	0.48	66	133	46	279
16.65	0.97	39	79	23	149
31.65	1.9	24	48	13	84
66.04	3.8	13	26	6	44
96.61	5.4	9	19	5	31

1 GiB/s Relay Can  
Deanonymize HS in  
about a day

# Countermeasures

- Sniper Attack Defenses

- Authenticated SENDMEs
- Queue Length Limit
- Adaptive Circuit Killer



Countermeasure  
deployed in Tor!

- Deanonymization Defenses

- Entry-guard Rate-limiting
- Middle Guards

# Questions?

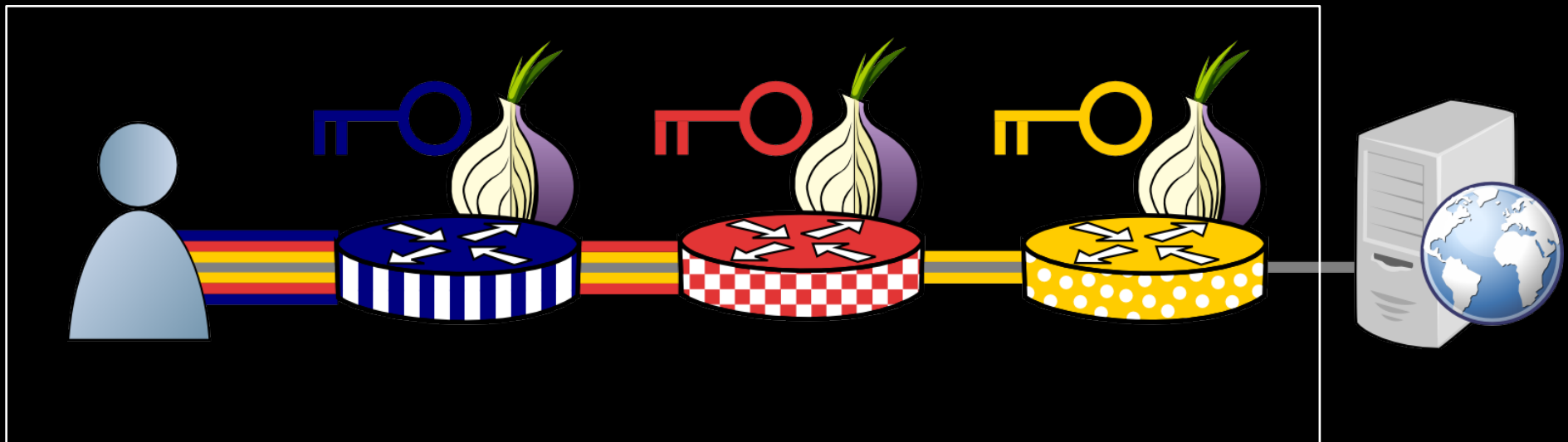
[cs.umn.edu/~jansen](http://cs.umn.edu/~jansen)  
[rob.g.jansen@nrl.navy.mil](mailto:rob.g.jansen@nrl.navy.mil)

*think like an adversary*



# How Tor Works

Tor protocol aware



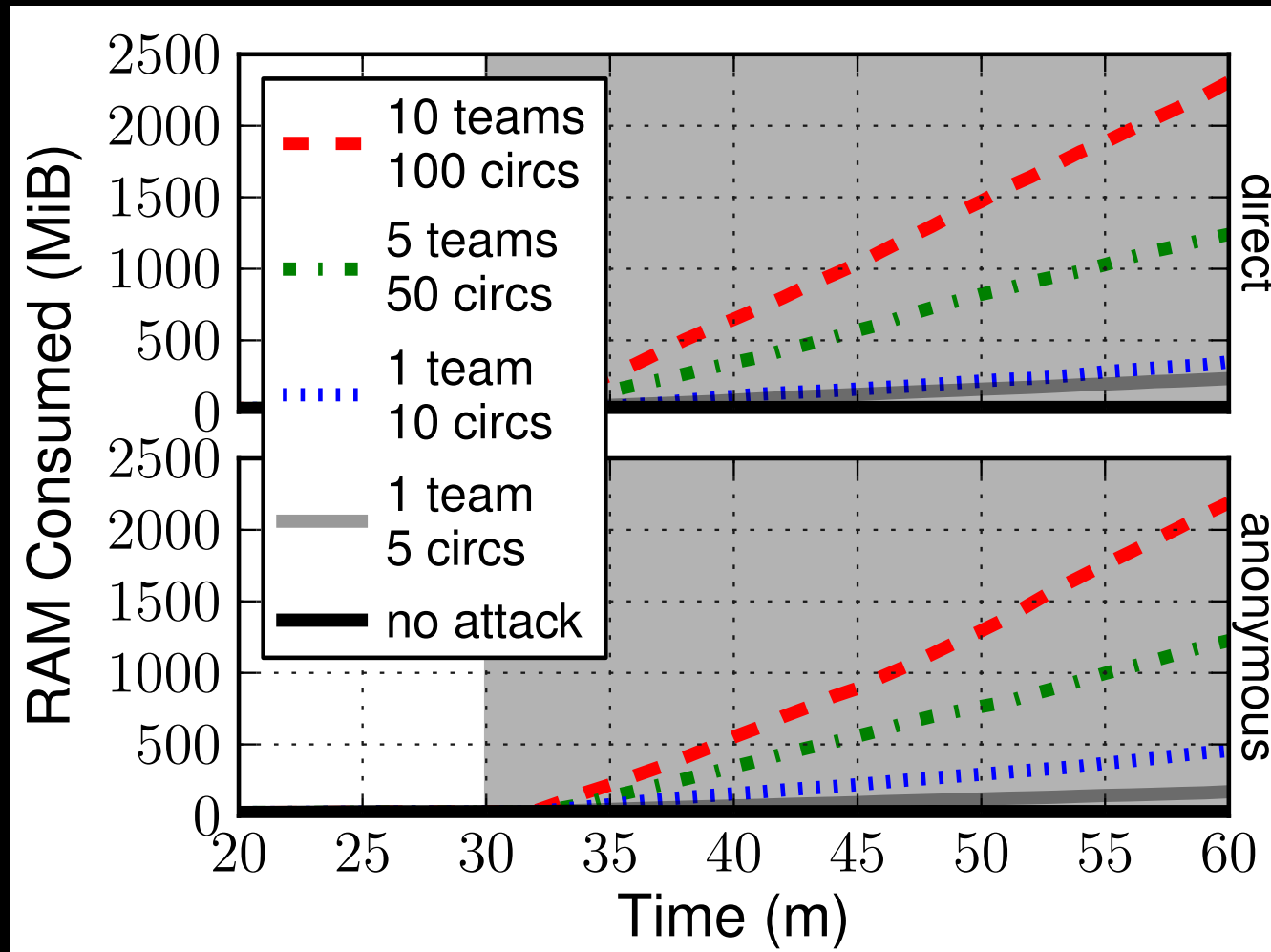
# Sniper Attack Experimental Results

# Sniper Resource Usage

	Direct			Anonymous		
<u>Config</u>	<u>RAM</u> (MiB)	<u>Tx</u> (KiB/s)	<u>Rx</u> (KiB/s)	<u>RAM</u> (MiB)	<u>Tx</u> (KiB/s)	<u>Rx</u> (KiB/s)
<b>1 team, 5 circuits</b>	28	4.0	2.3	56	3.6	1.8
<b>1 team, 10 circuits</b>	28	6.1	2.6	57	9.4	2.1
<b>5 teams, 50 circuits</b>	141	30.0	9.5	283	27.7	8.5
<b>10 teams, 100 circuits</b>	283	56.0	20.9	564	56.6	17.0

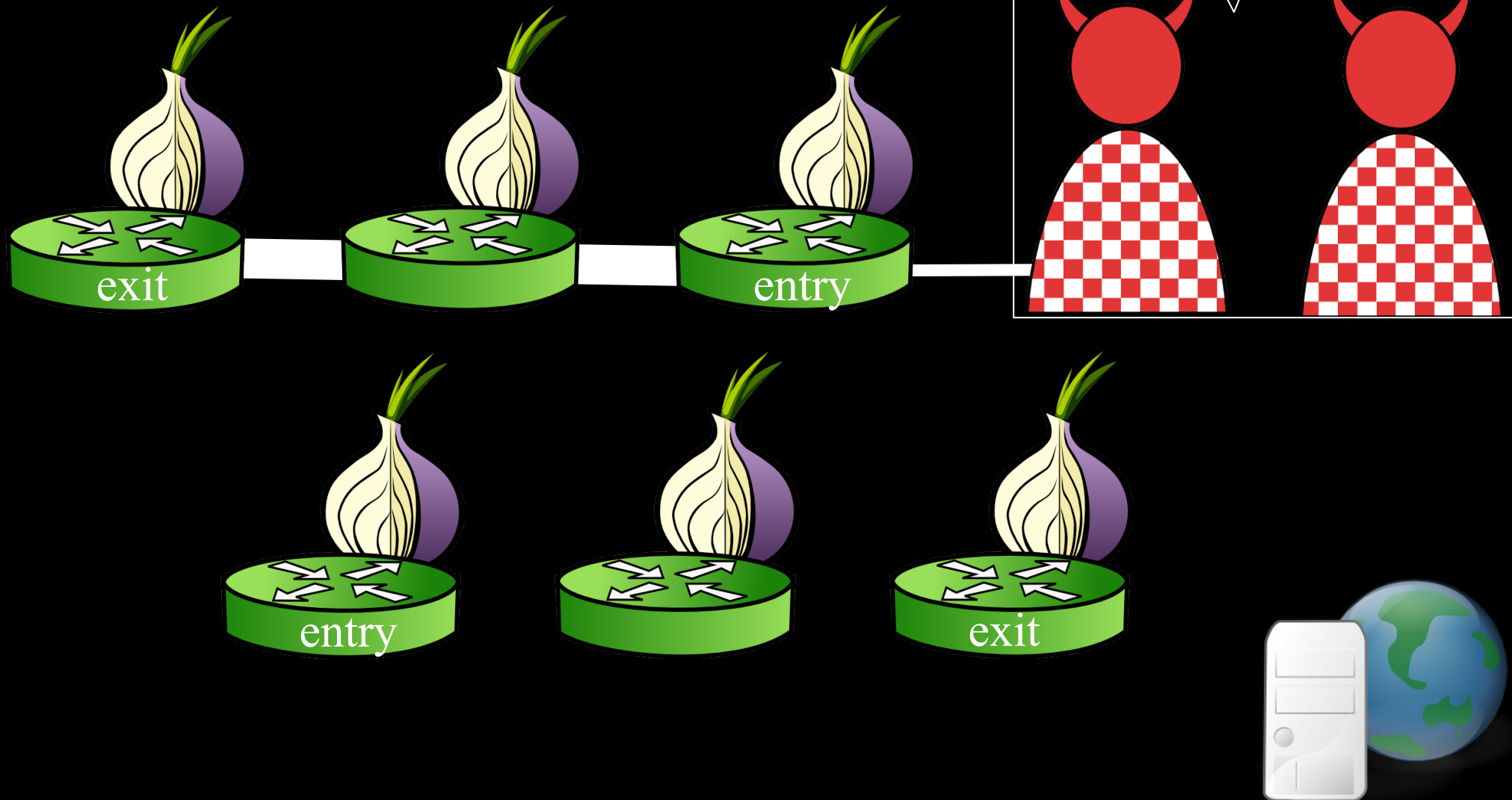


# Memory Consumed over Time



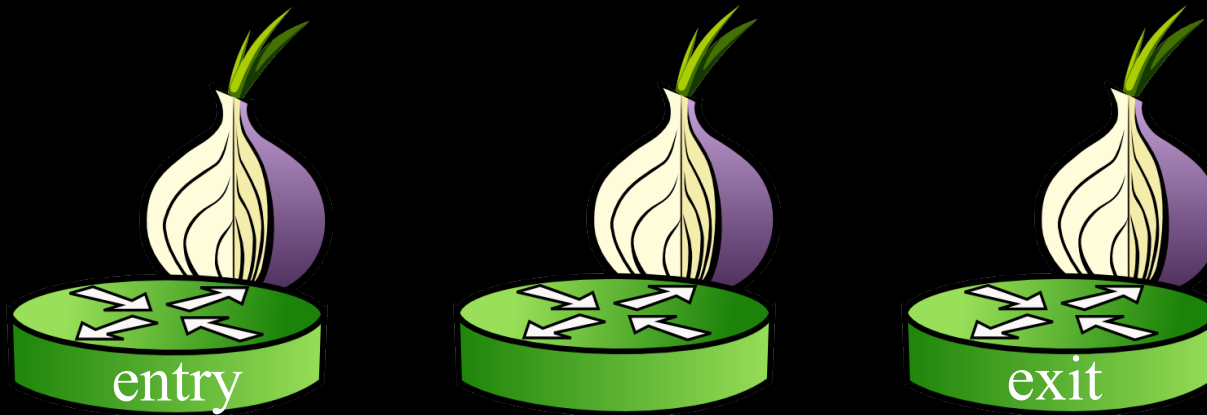
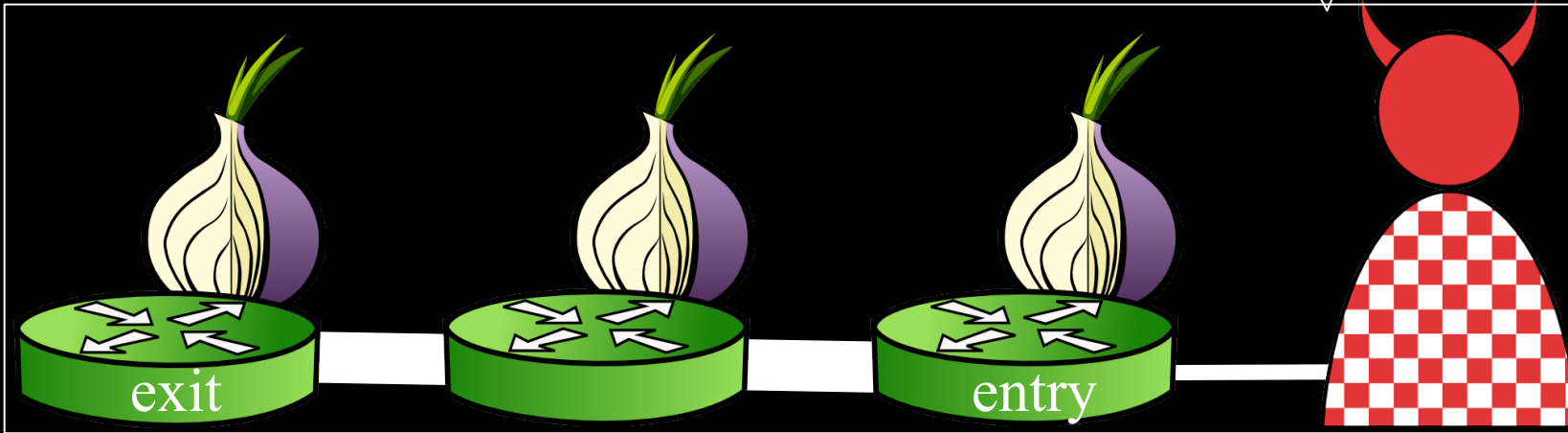
# Sniper Attack Through Tor

# The Sniper Attack

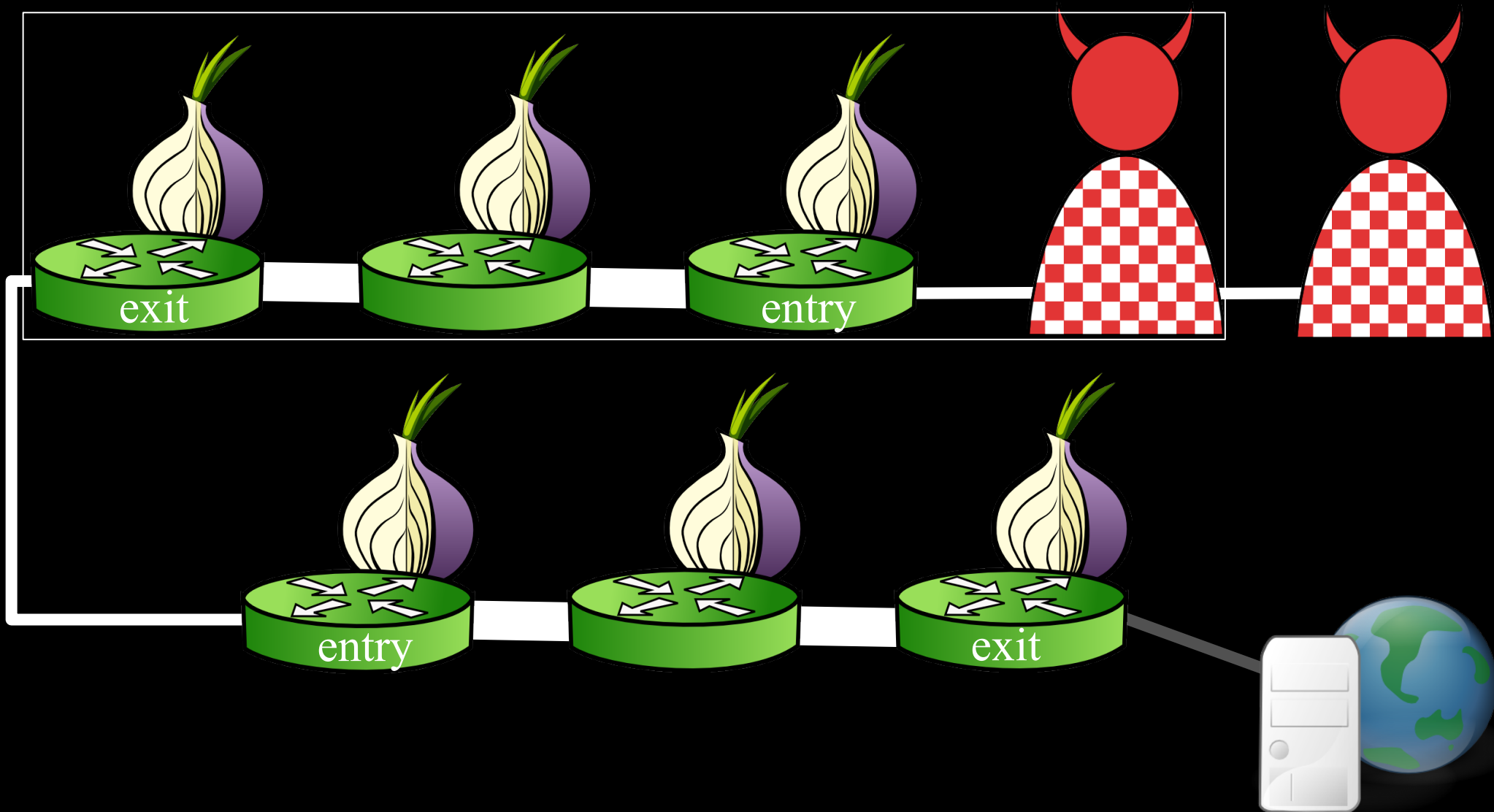


# The Sniper Attack

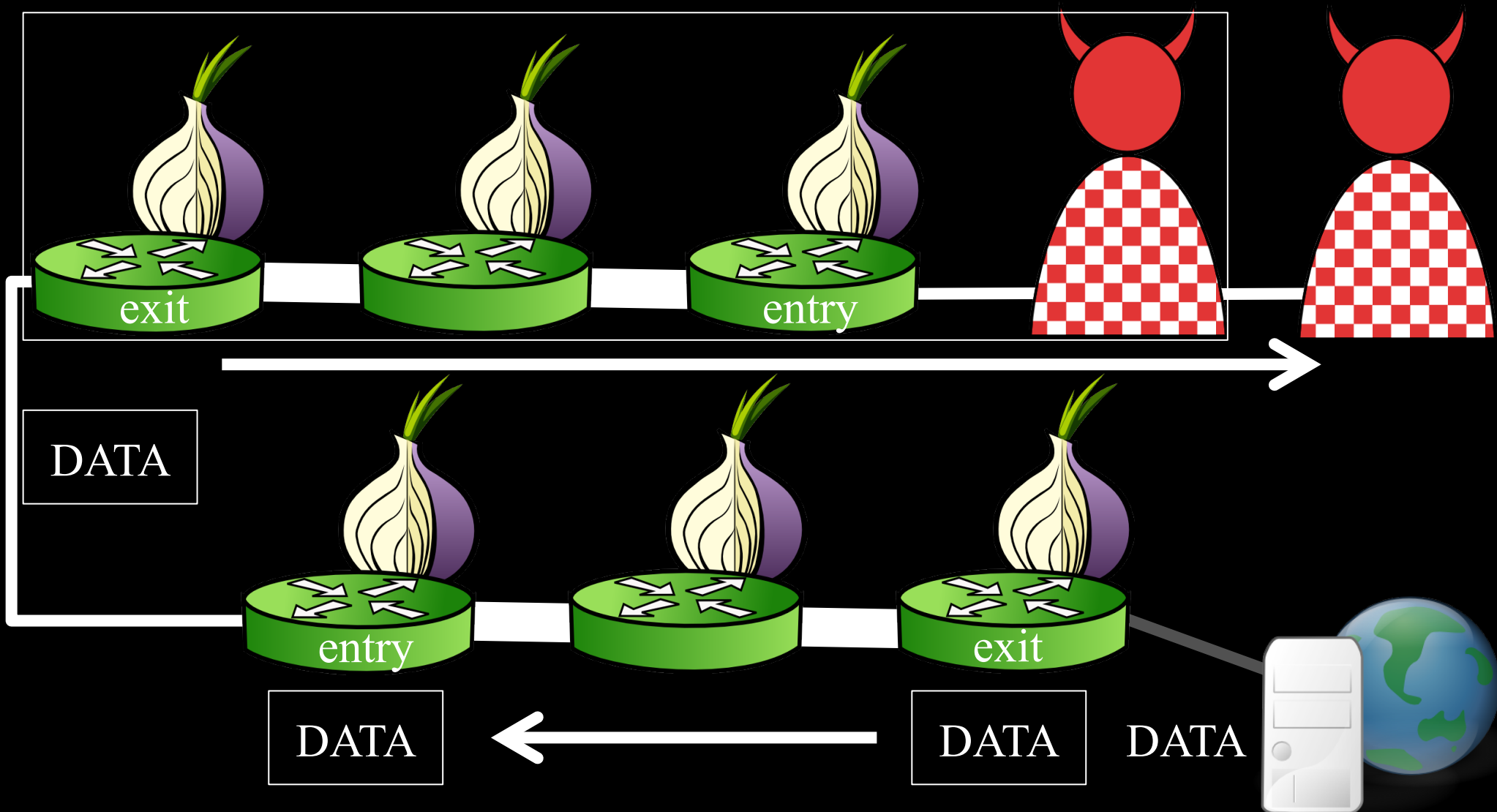
Anonymous  
Tunnel



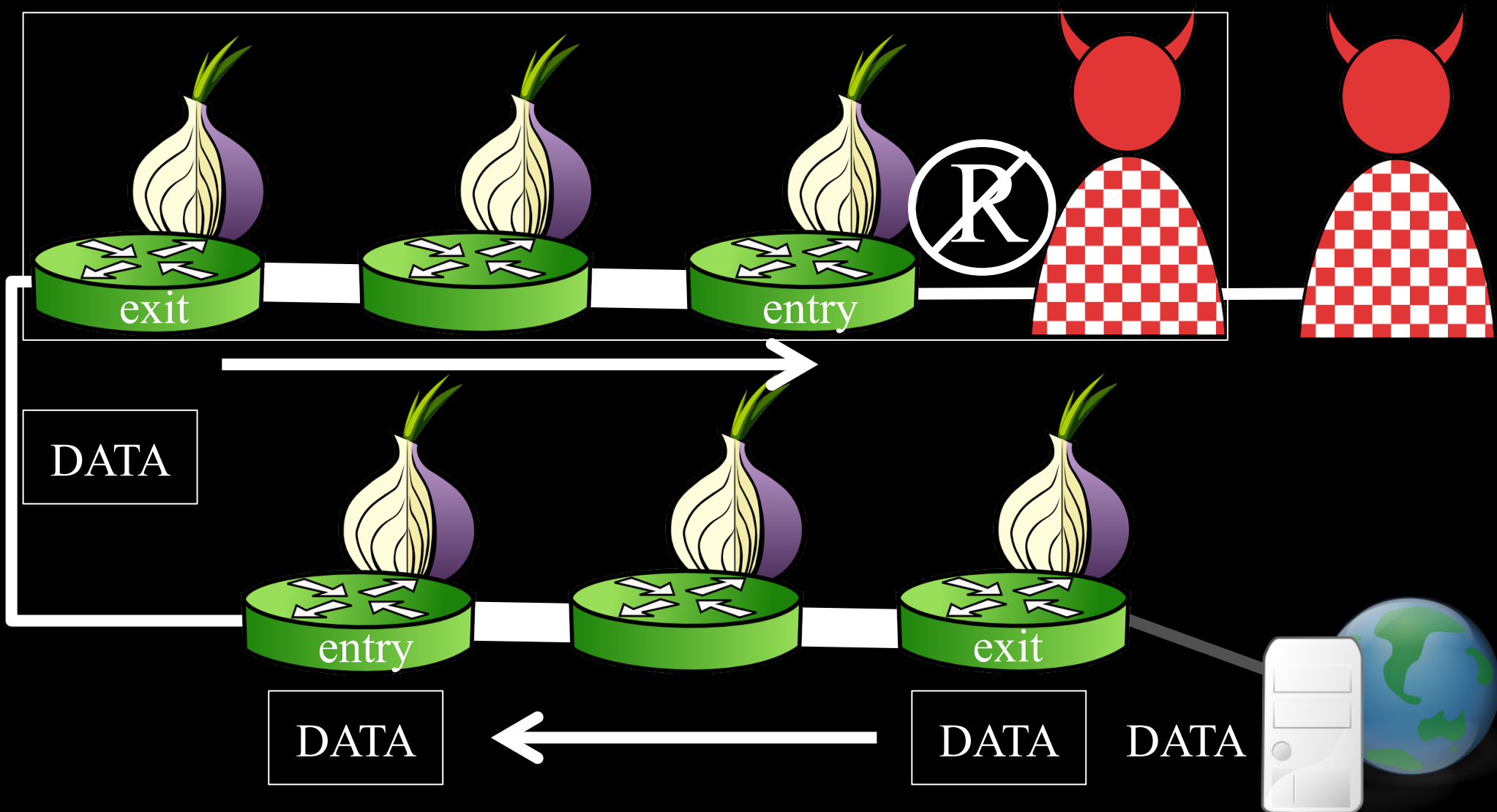
# The Sniper Attack



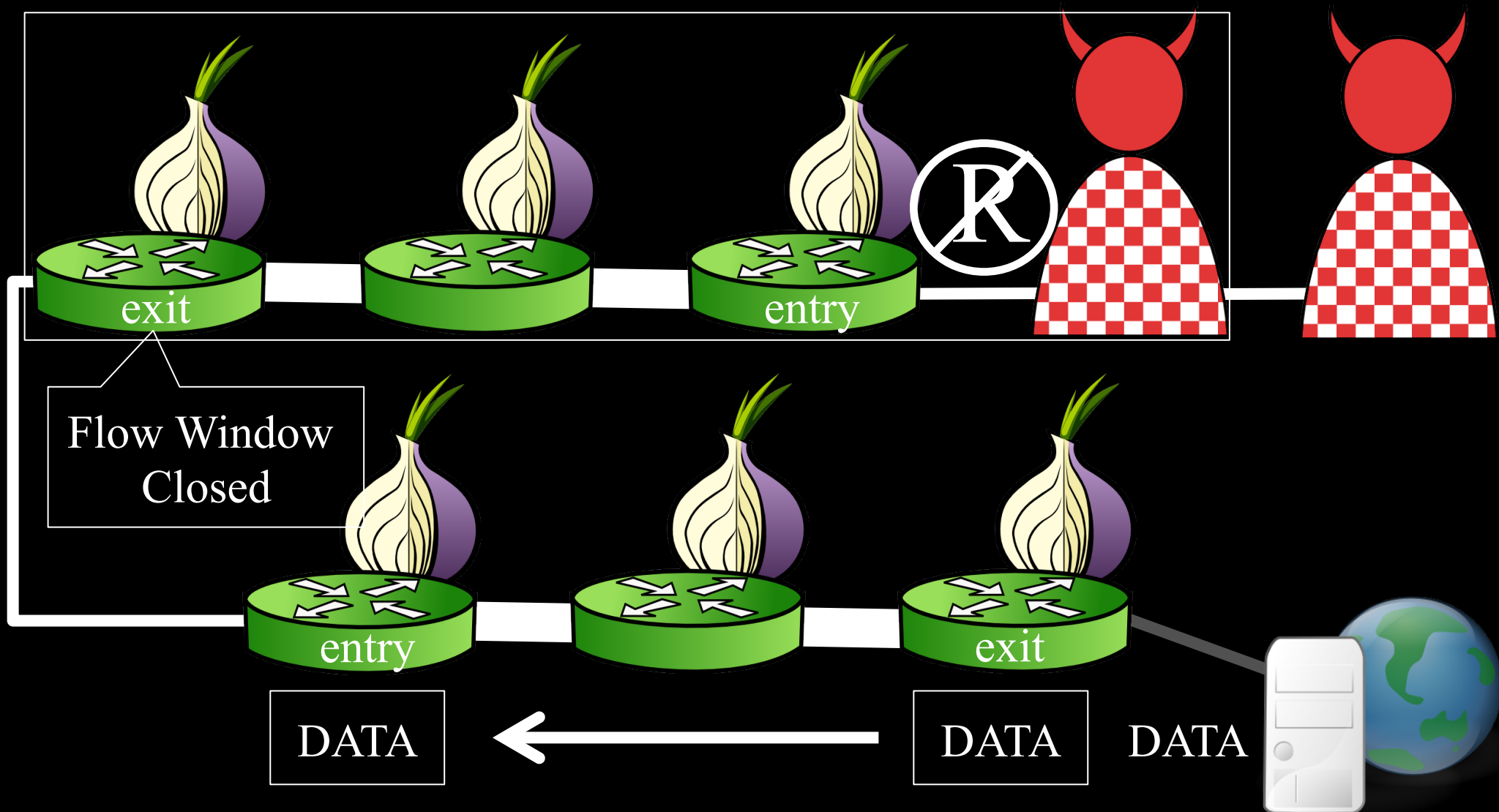
# The Sniper Attack



# The Sniper Attack

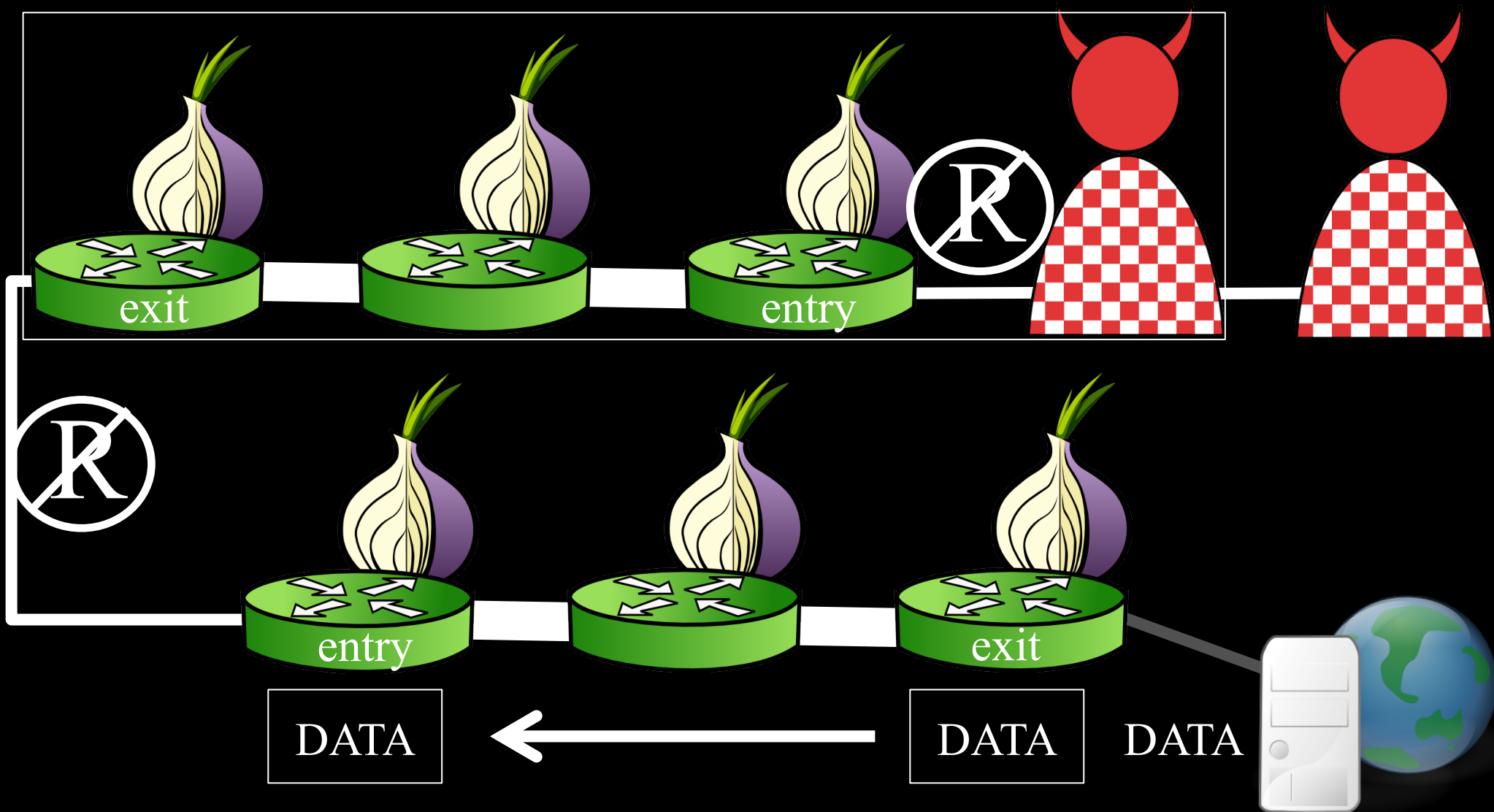


# The Sniper Attack

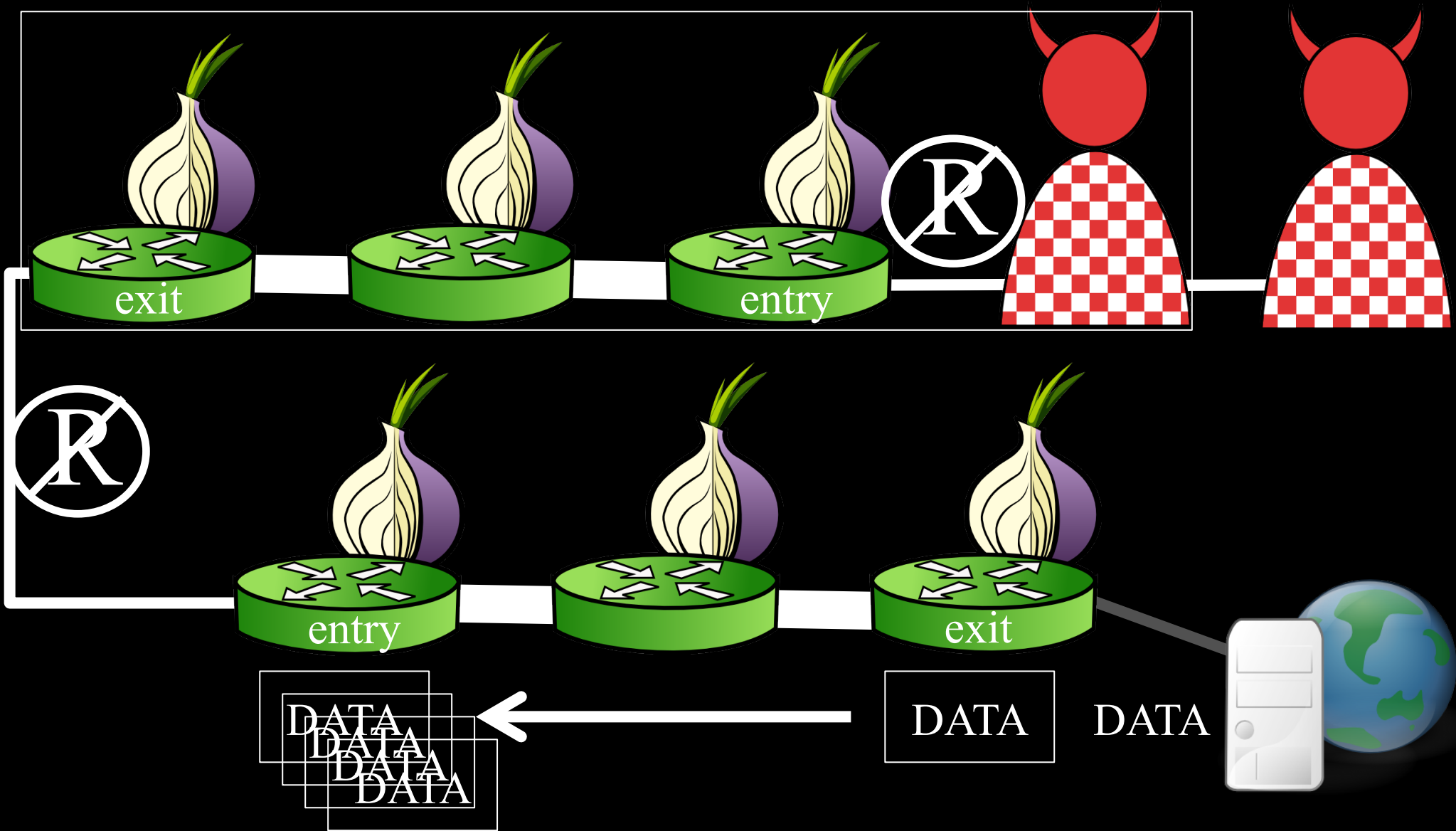




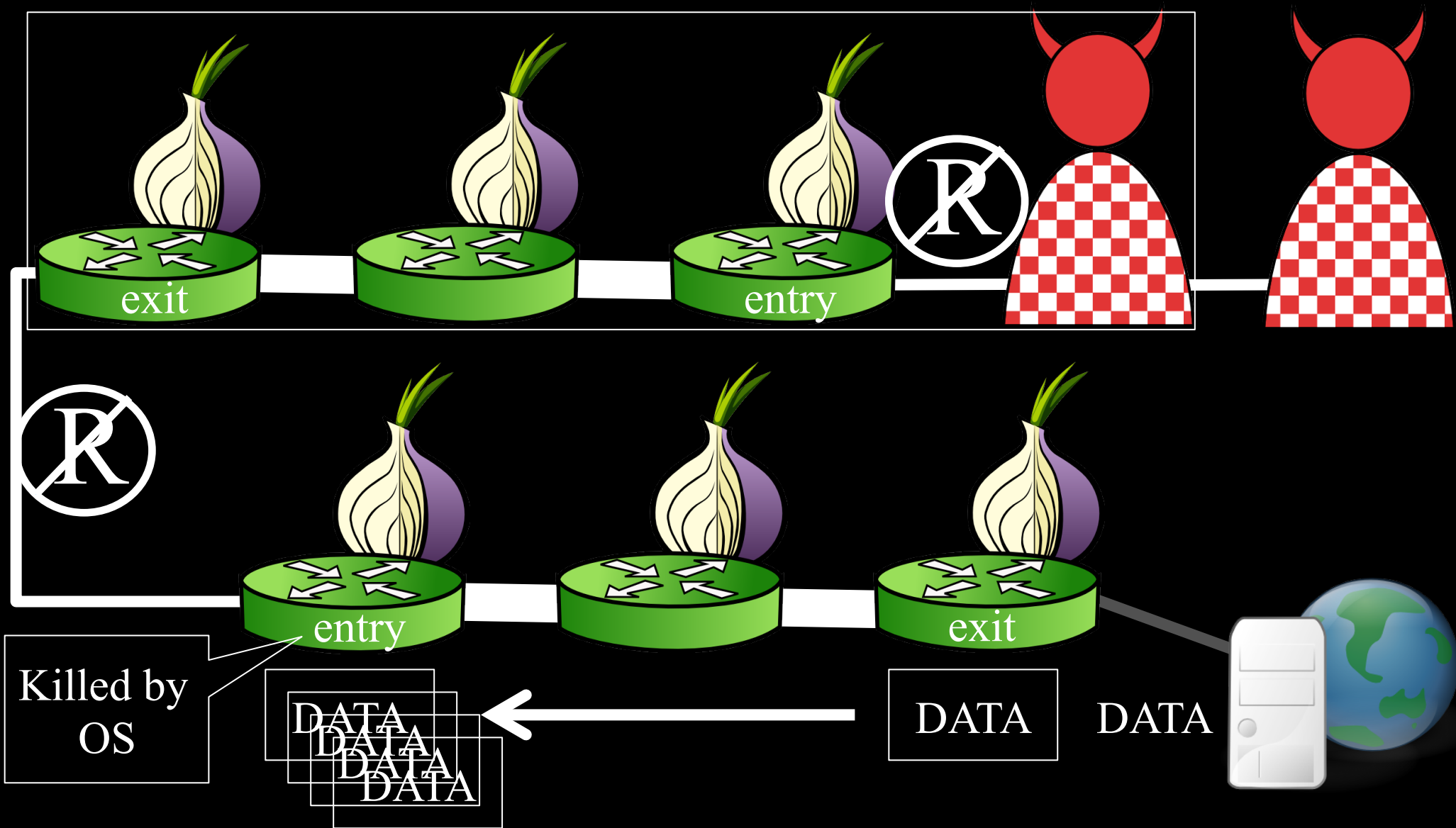
# The Sniper Attack



# The Sniper Attack



# The Sniper Attack

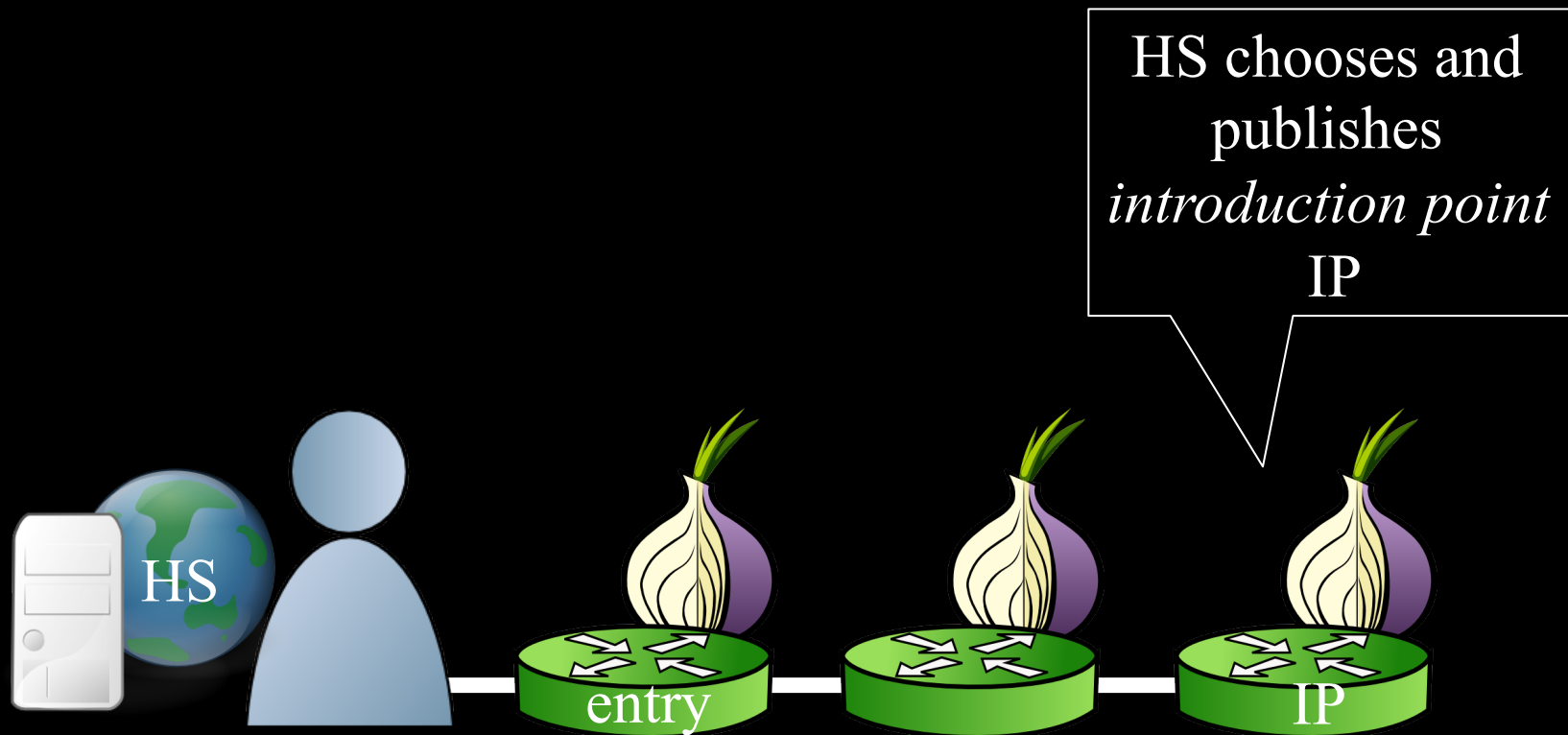


# Tor Hidden Services Background

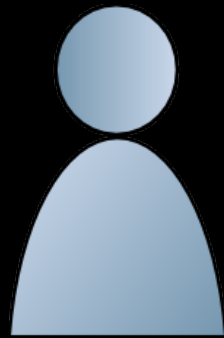
# Hidden Services



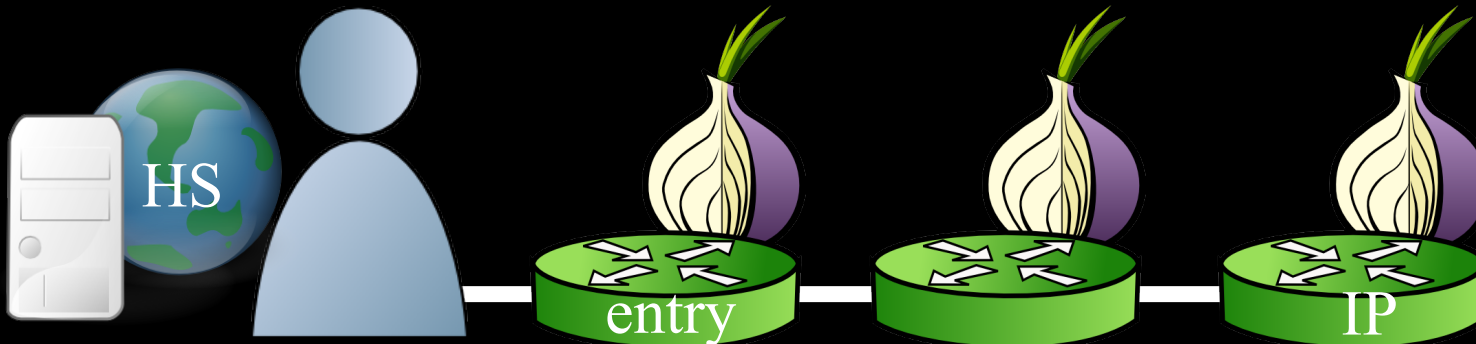
# Hidden Services



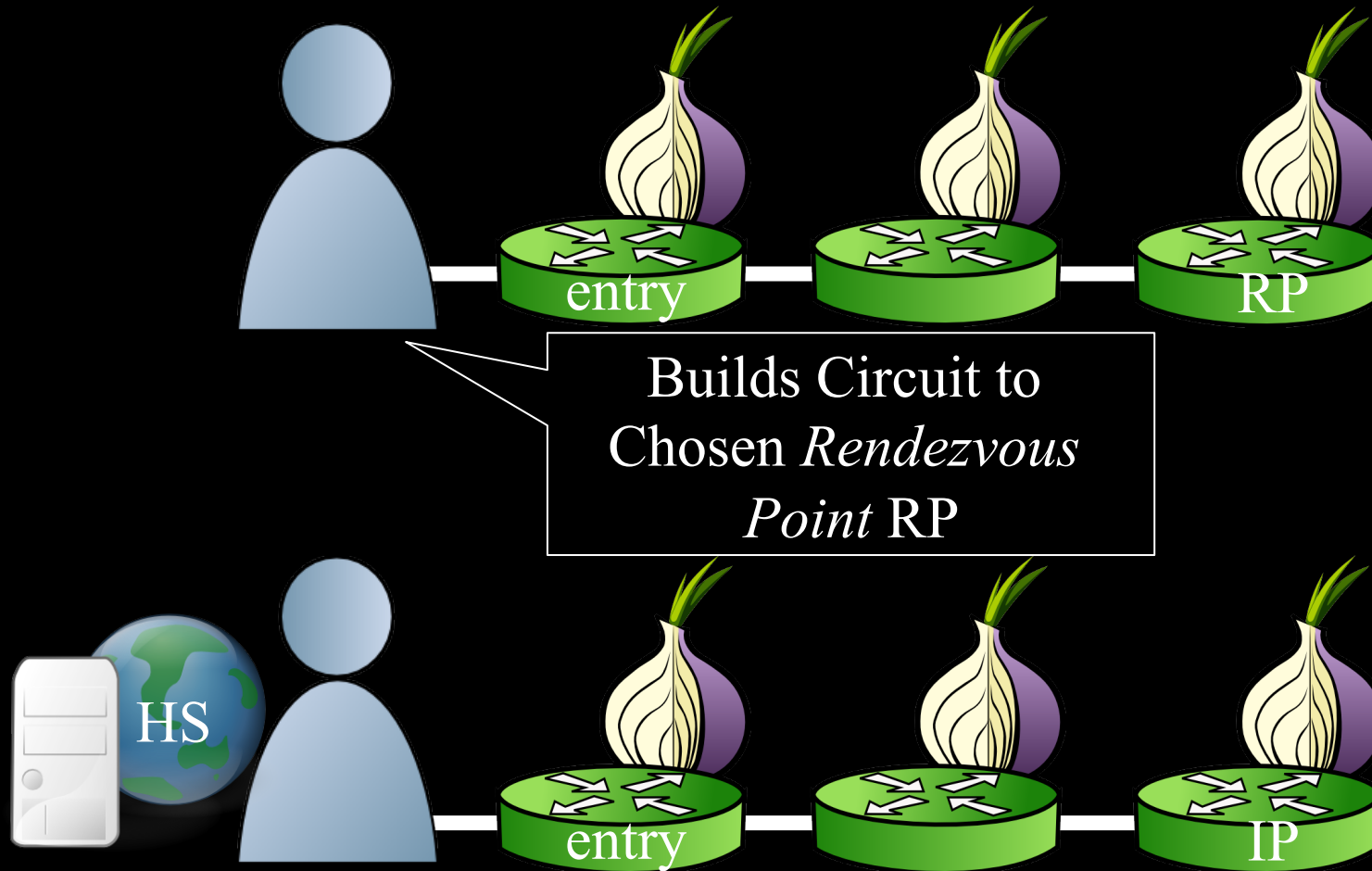
# Hidden Services



Learns about  
HS on web

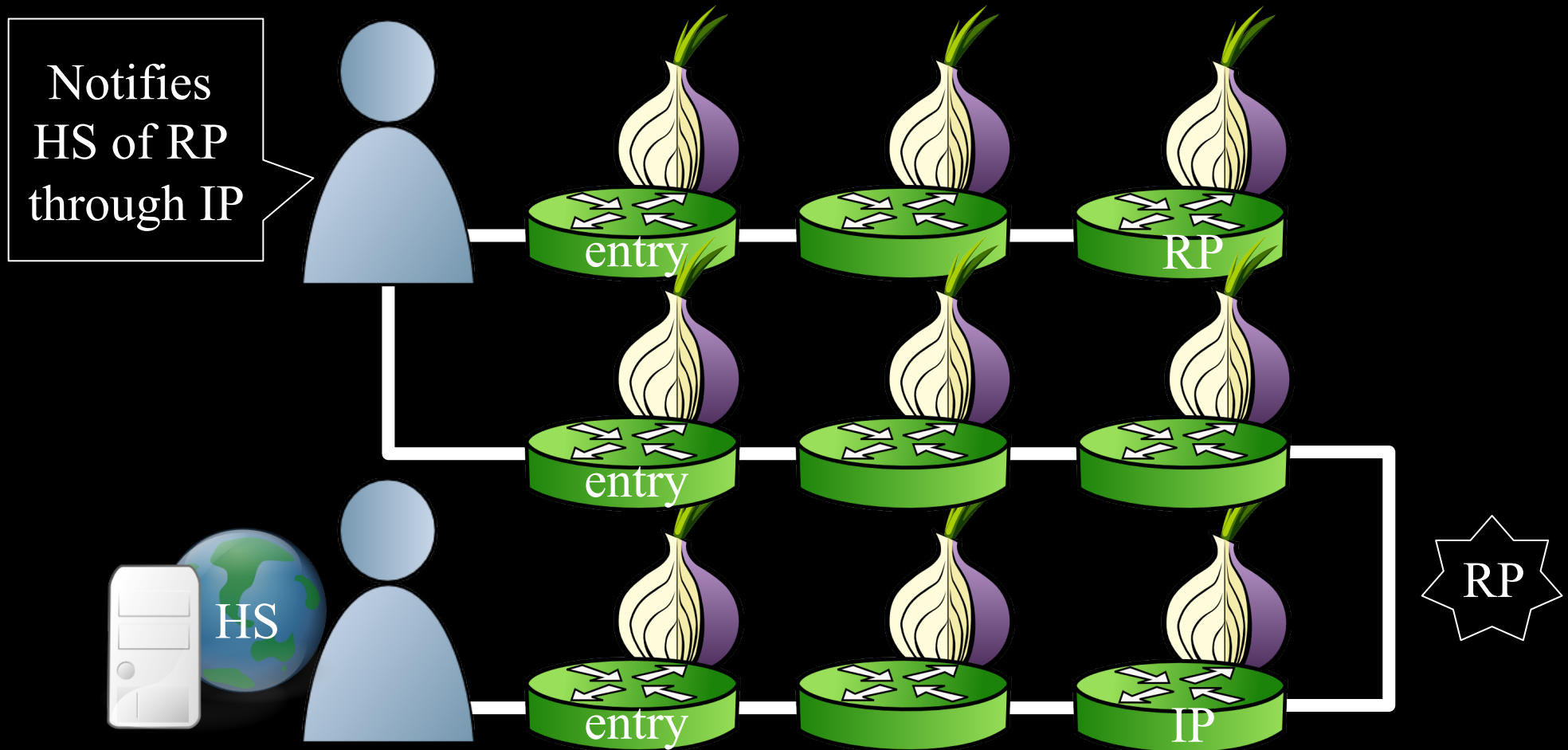


# Hidden Services

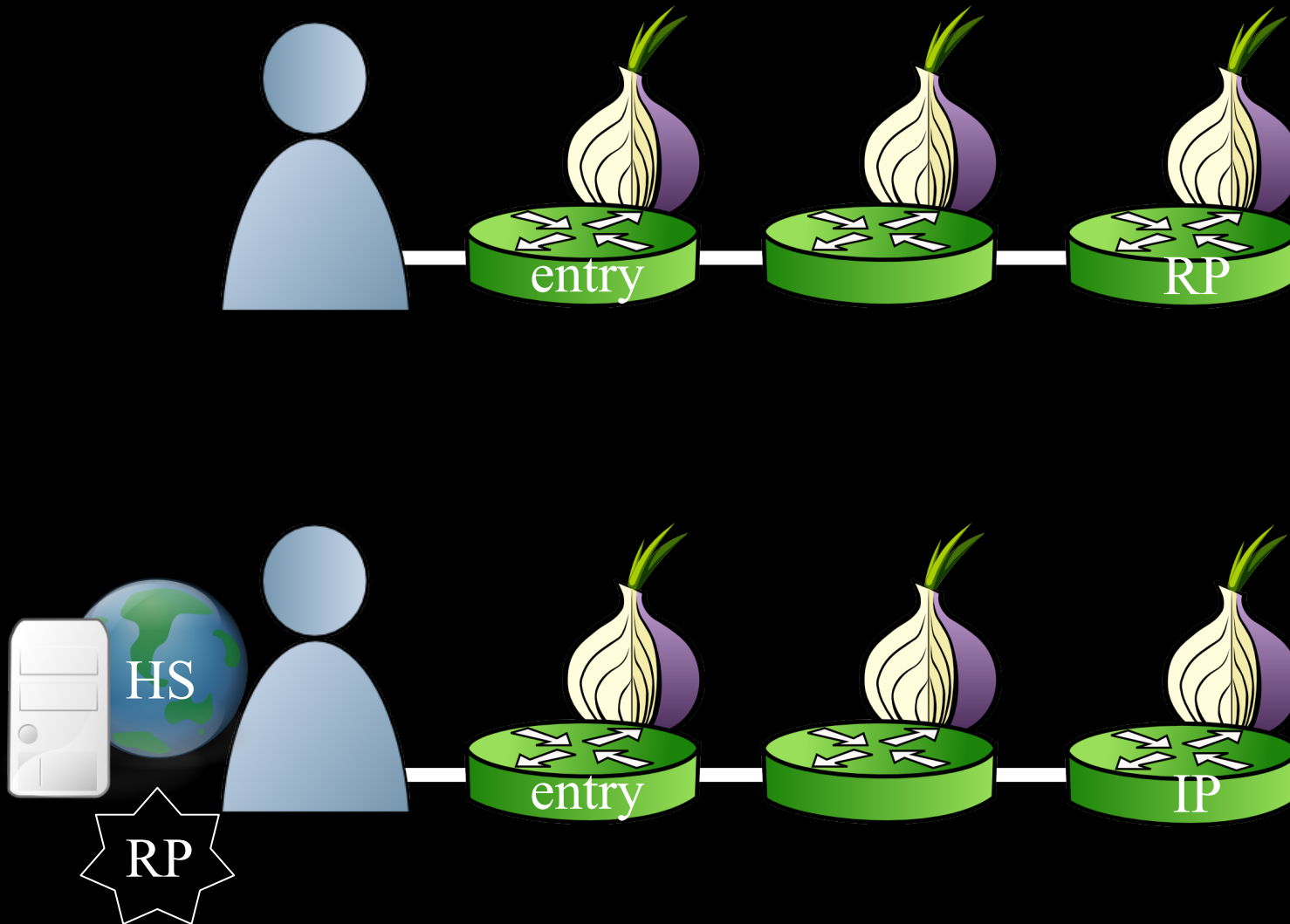




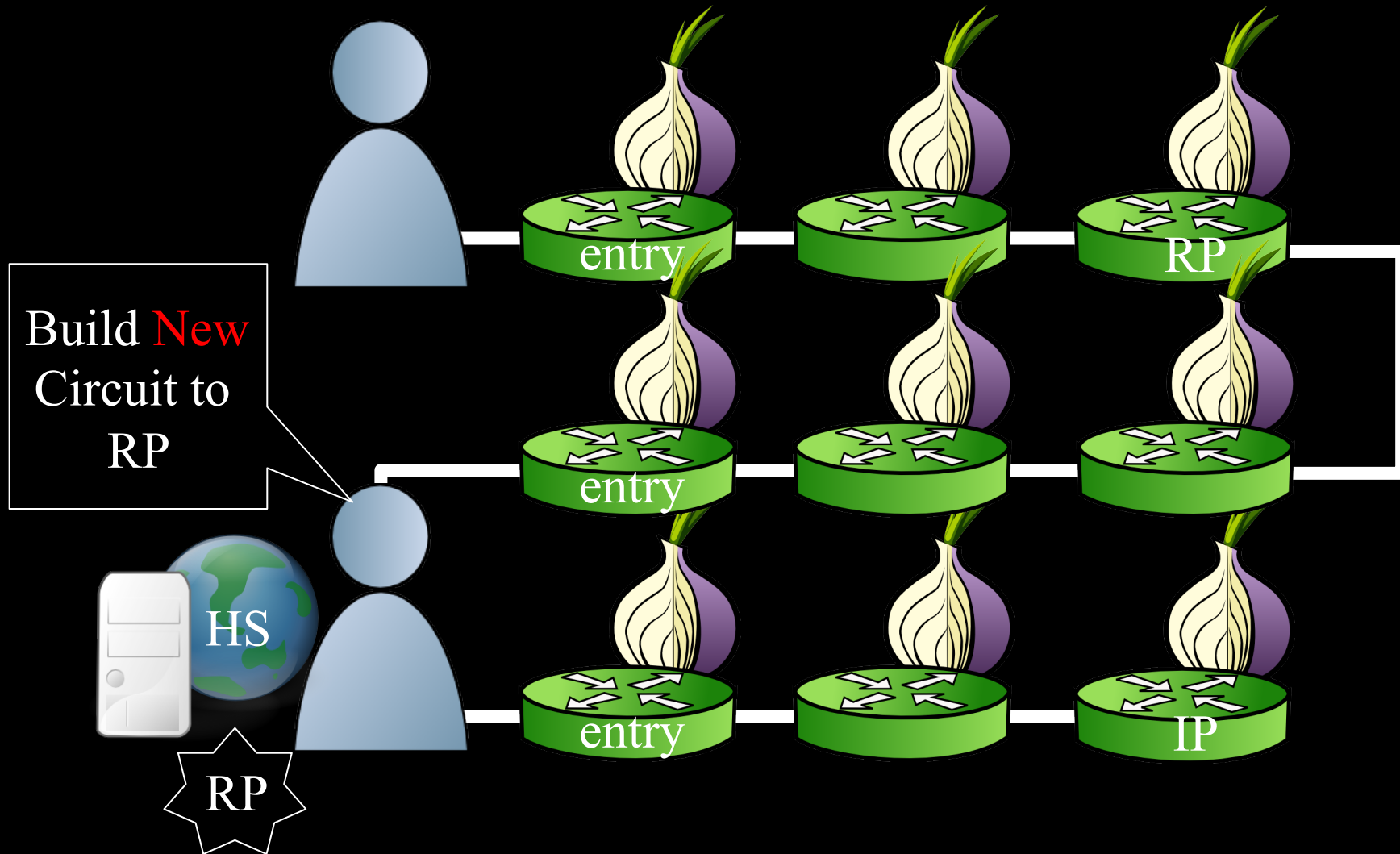
# Hidden Services



# Hidden Services



# Hidden Services



# Hidden Services

