Memory-based DoS and Deanonymization Attacks on Tor

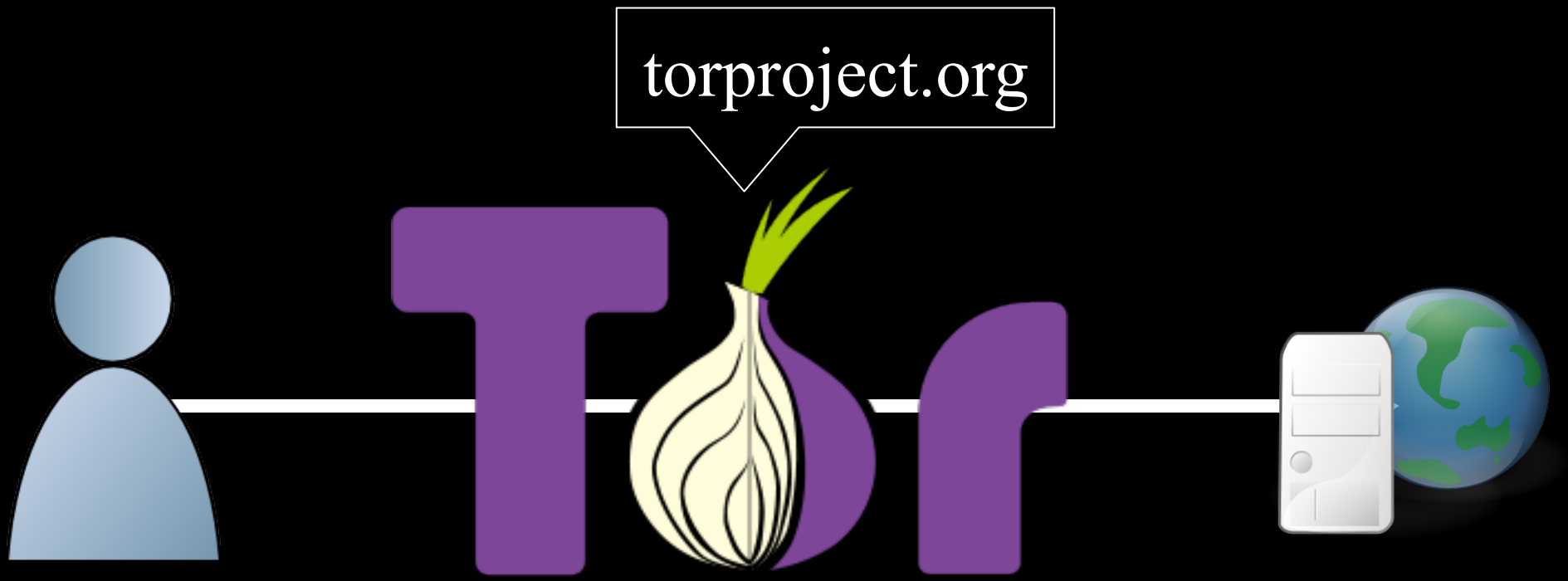
DCAPS Seminar

October 11th, 2013

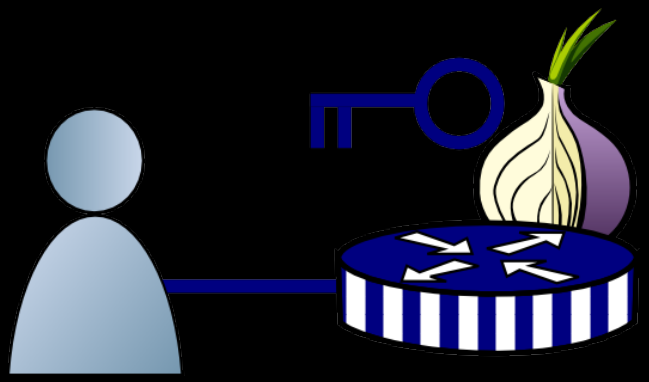
Rob Jansen
U.S. Naval Research Laboratory
rob.g.jansen@nrl.navy.mil

*Joint with Aaron Johnson, Florian Tschorsch, Björn Scheuermann

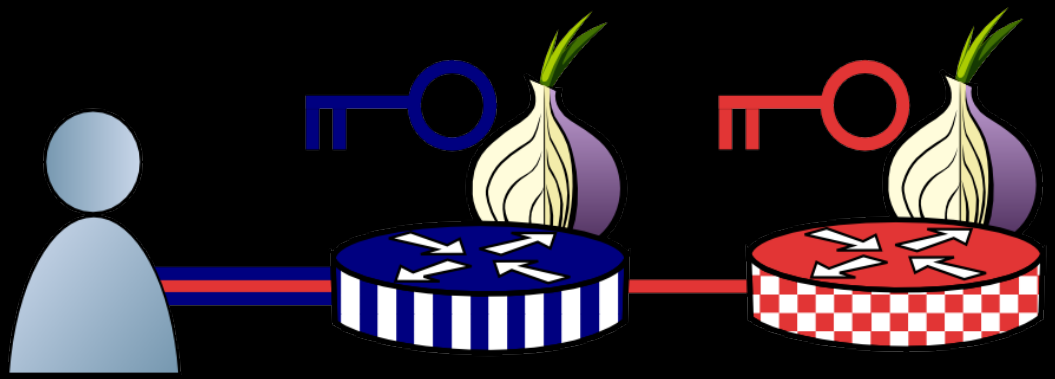
The Tor Anonymity Network



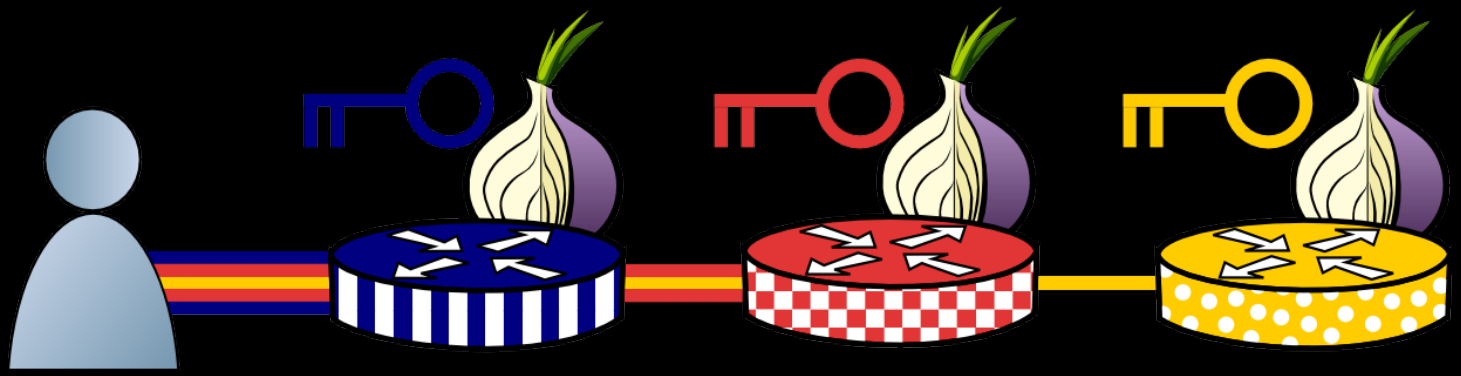
How Tor Works



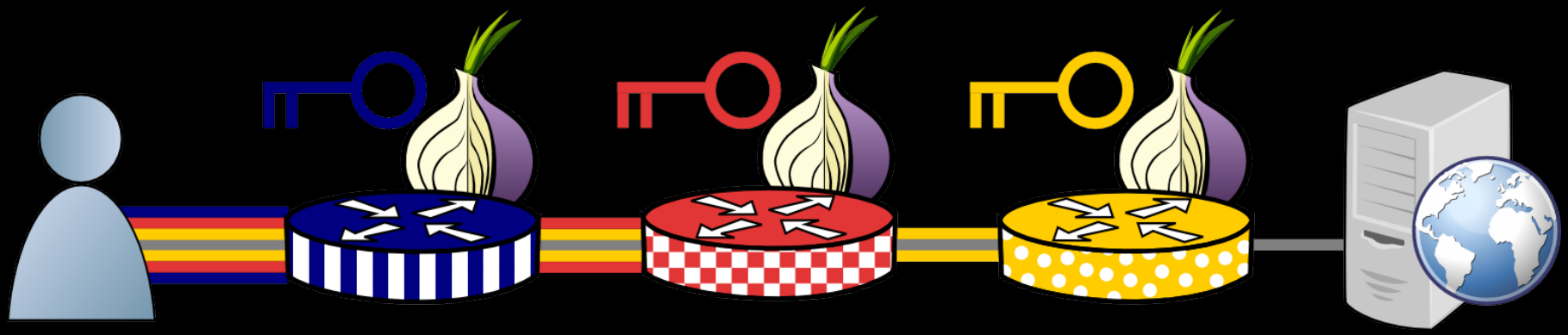
How Tor Works



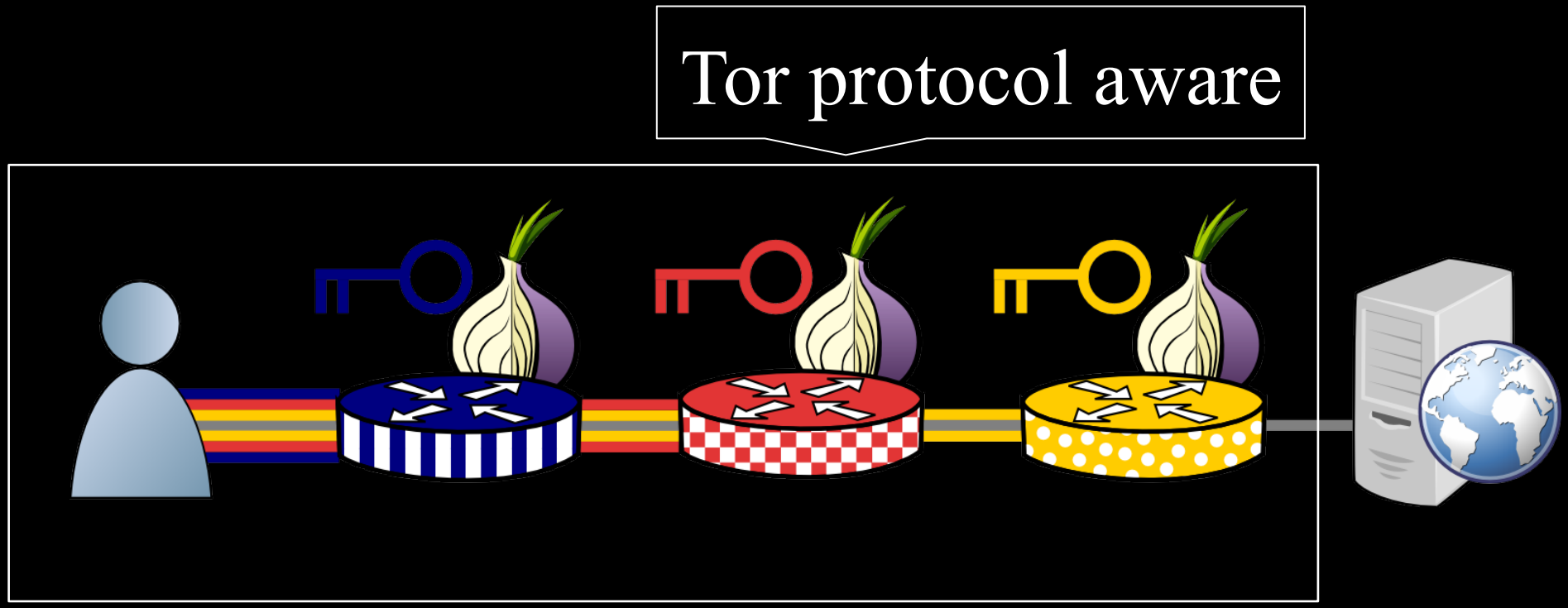
How Tor Works



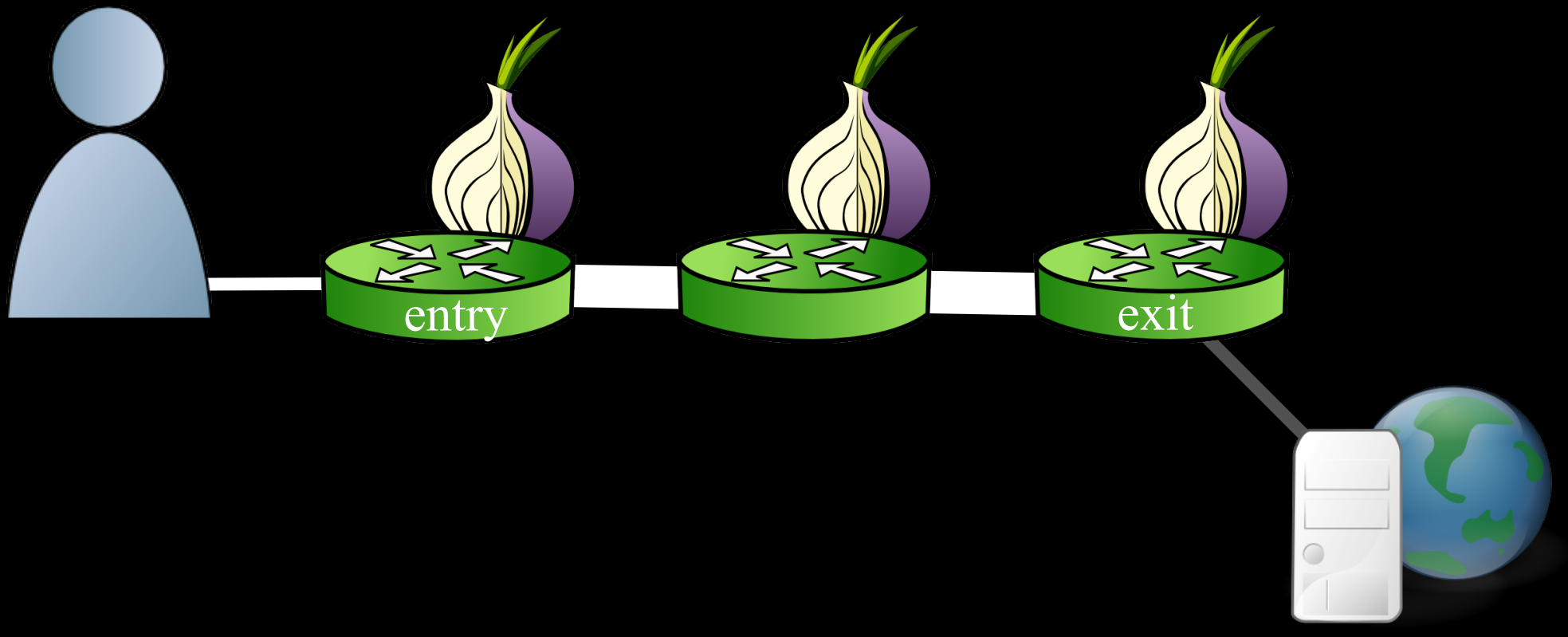
How Tor Works



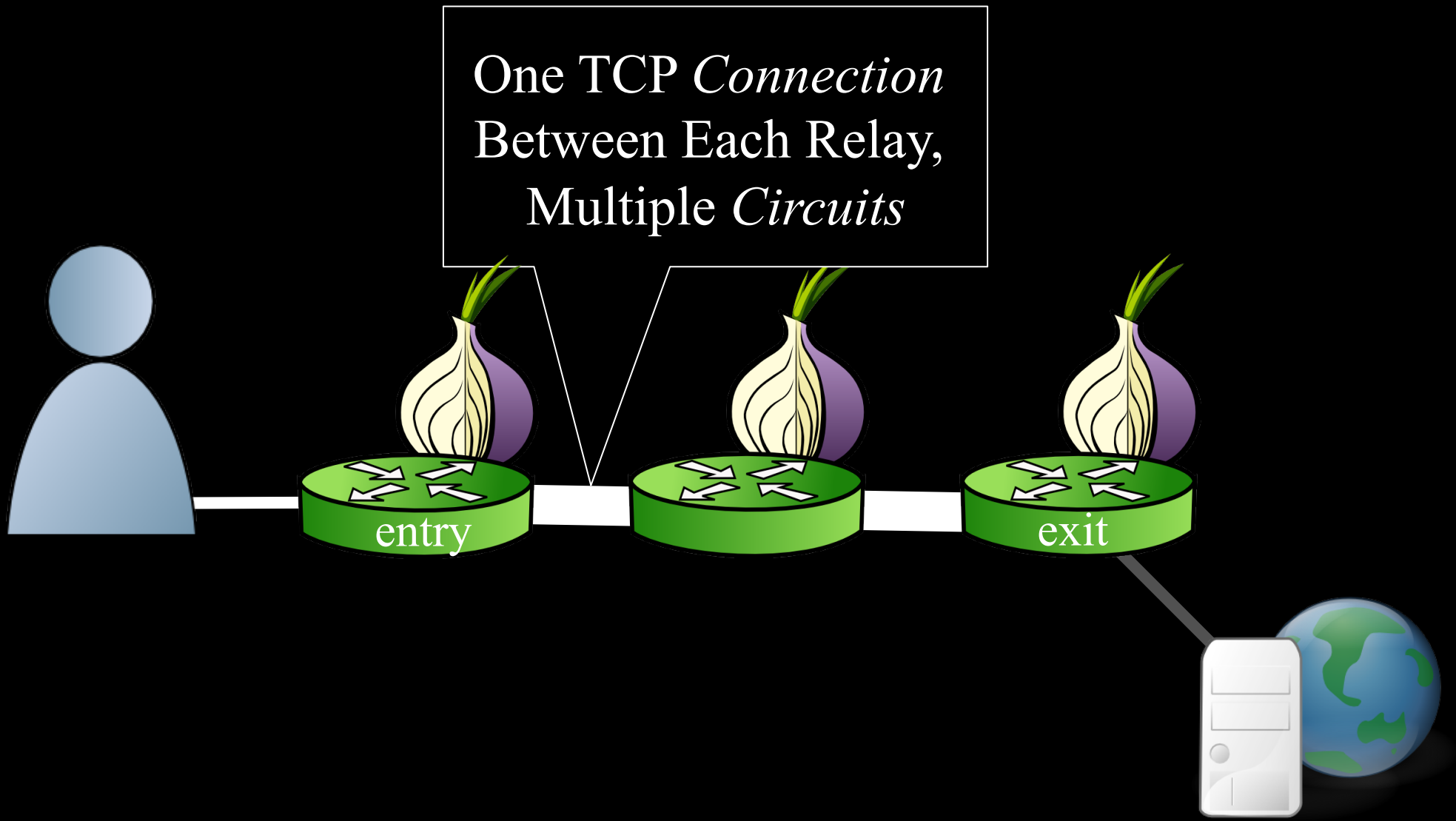
How Tor Works



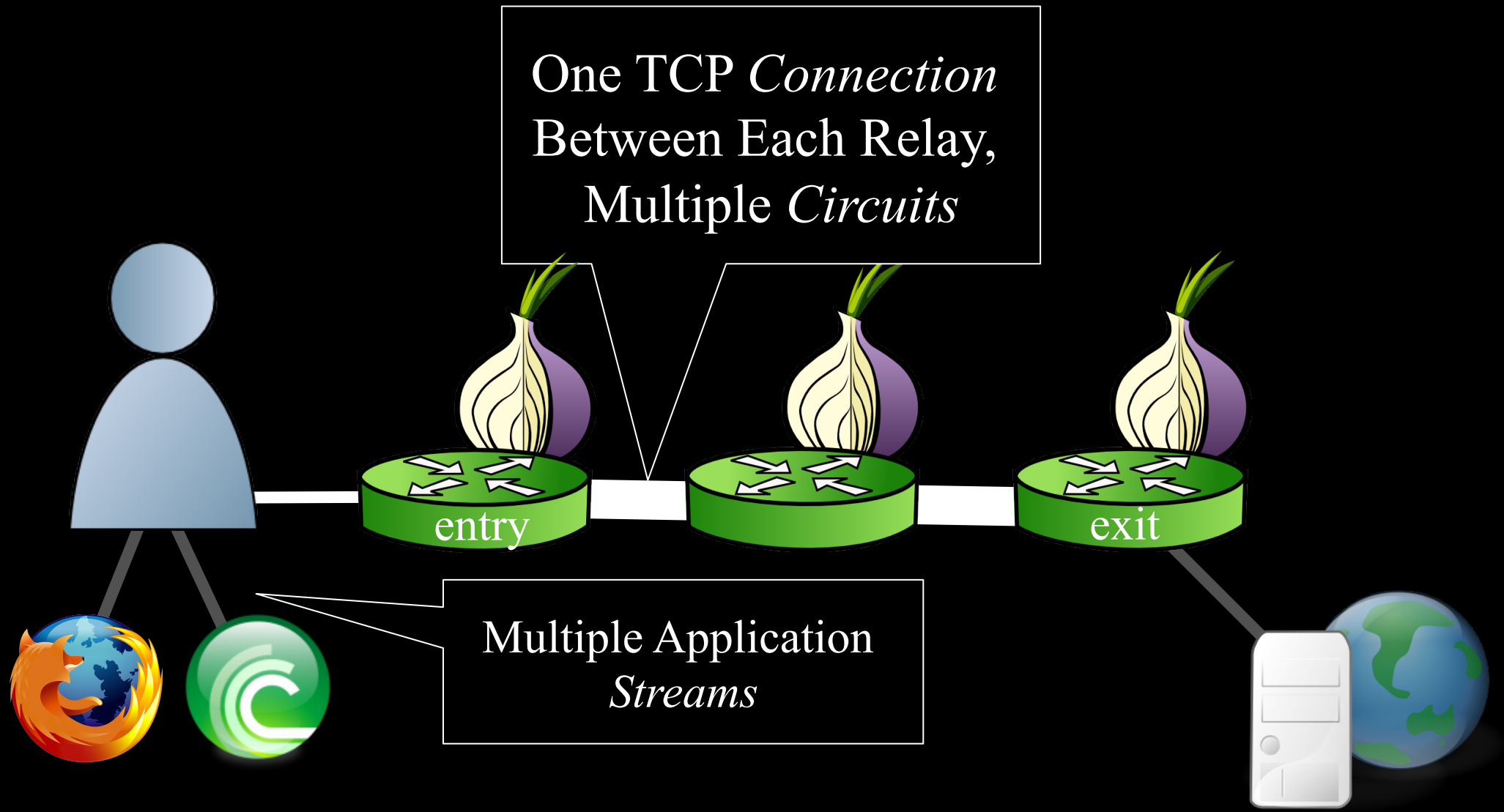
Tor Flow Control



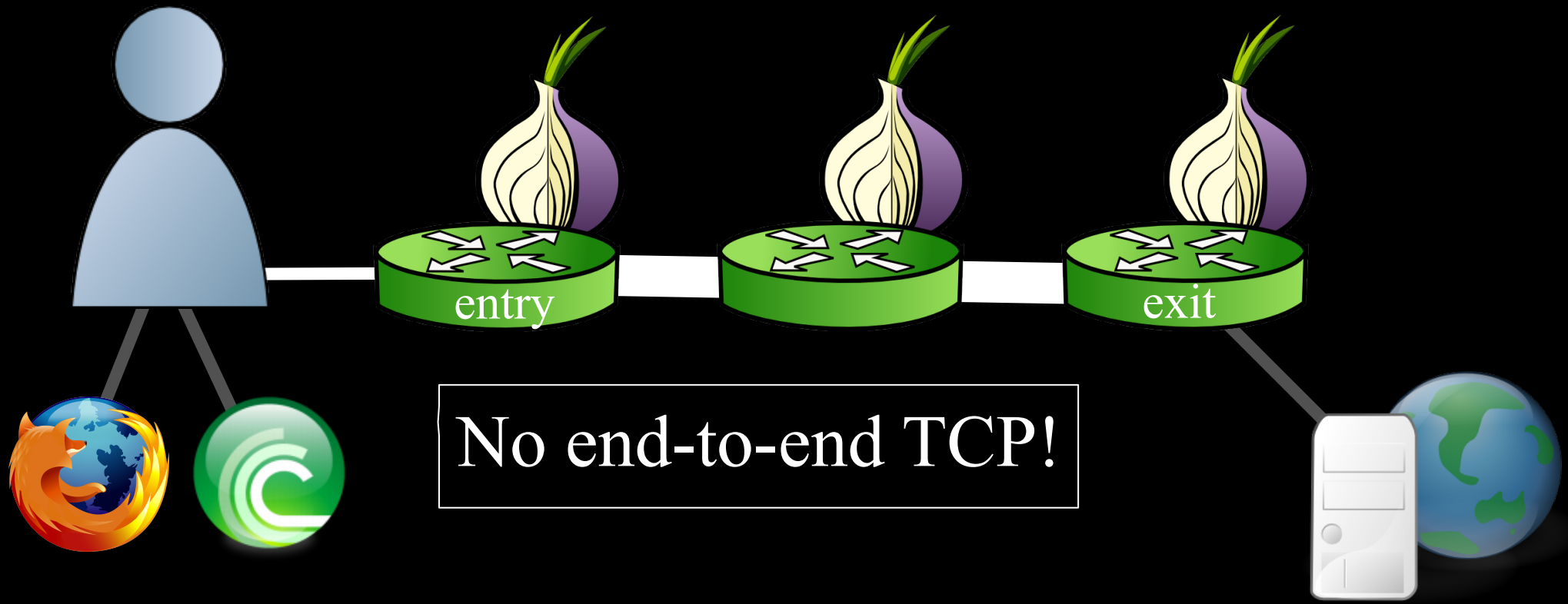
Tor Flow Control



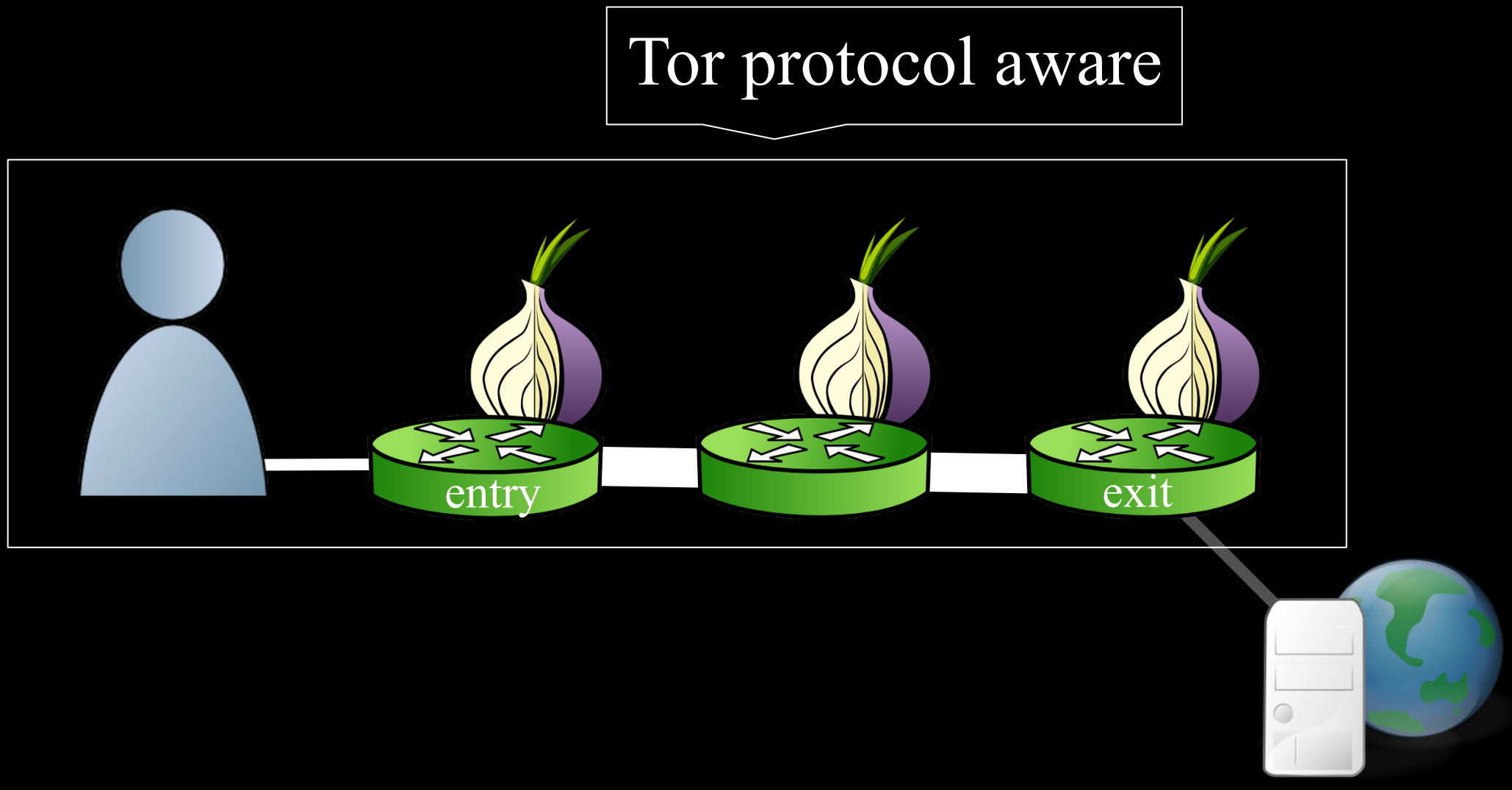
Tor Flow Control



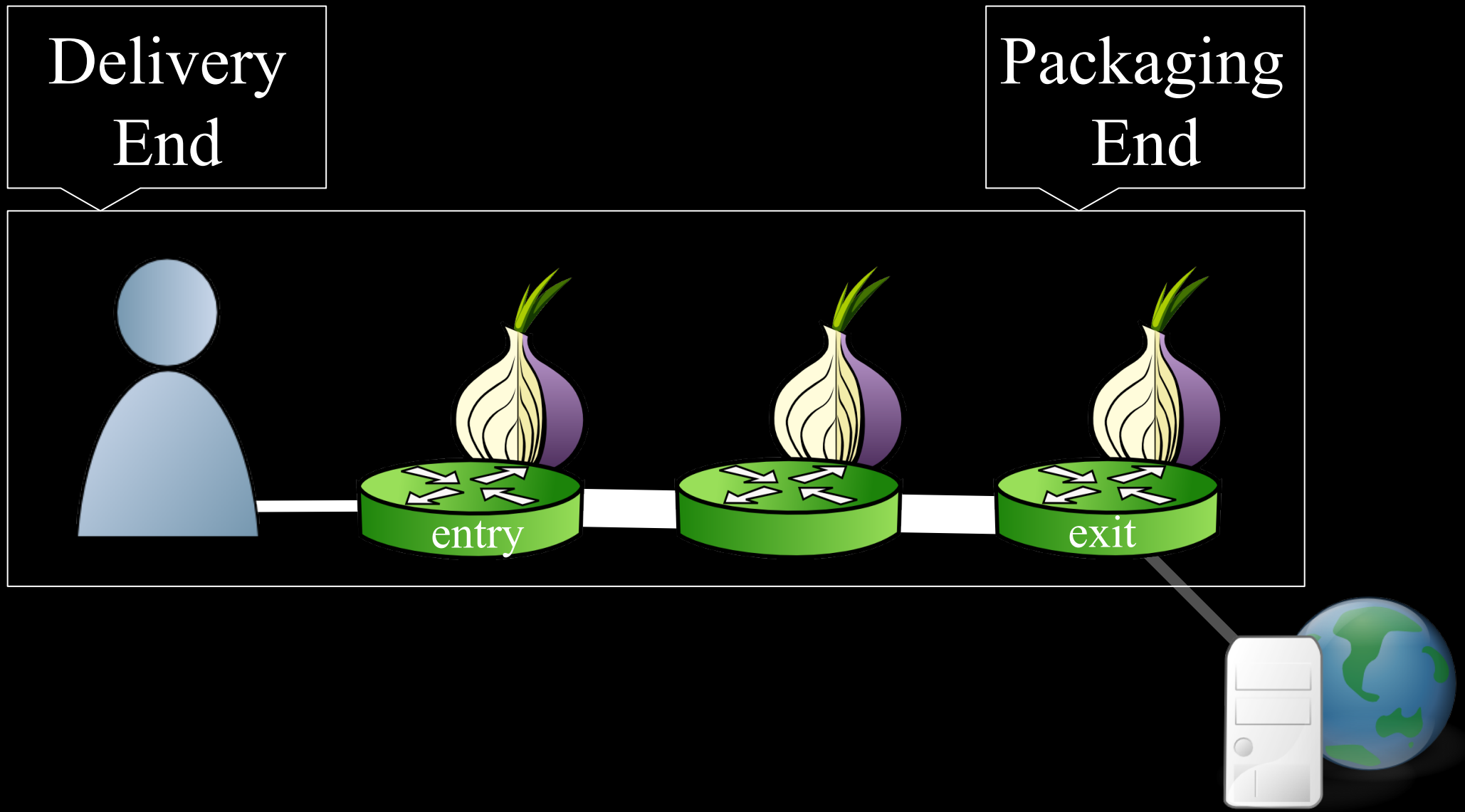
Tor Flow Control



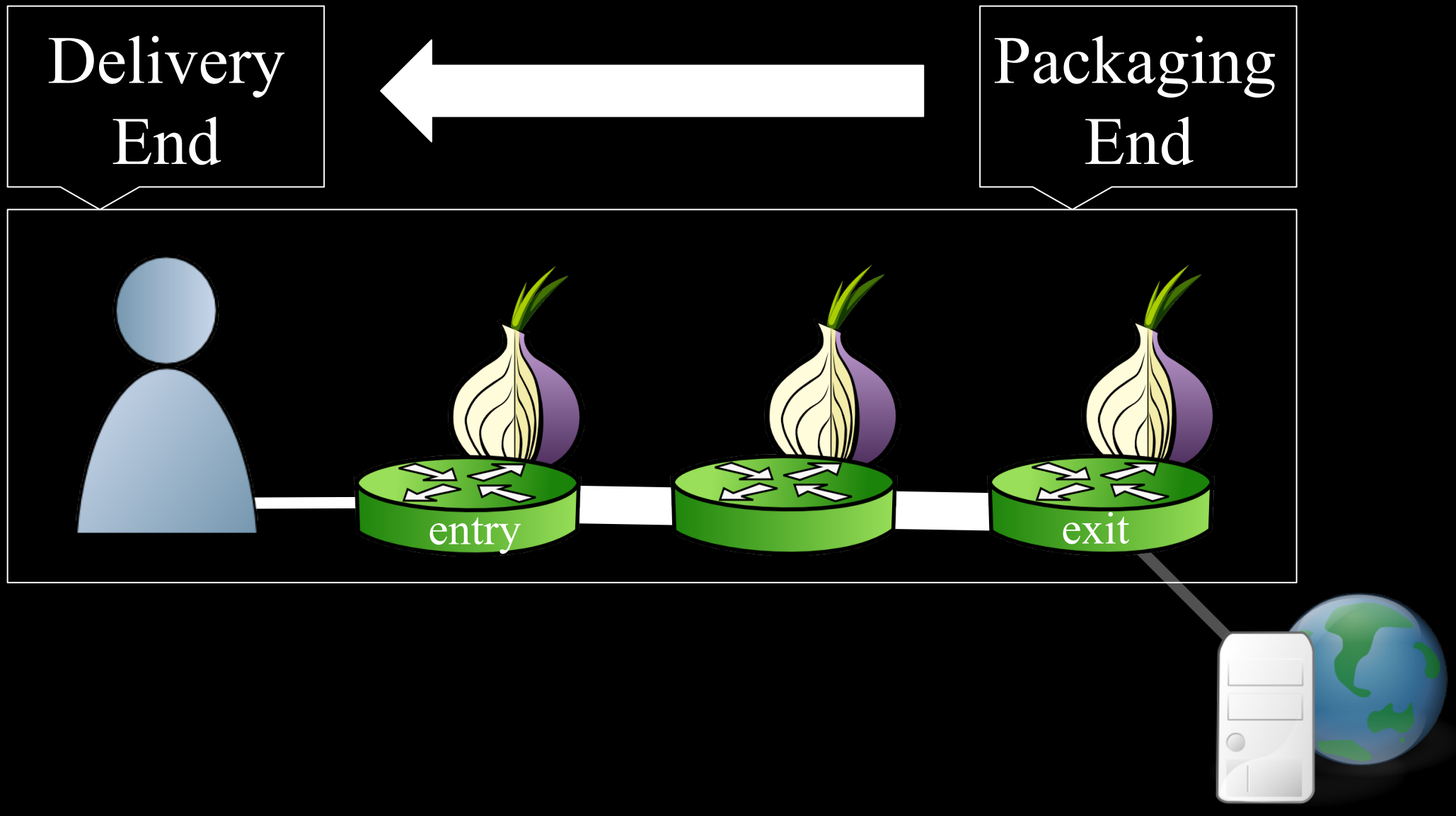
Tor Flow Control



Tor Flow Control



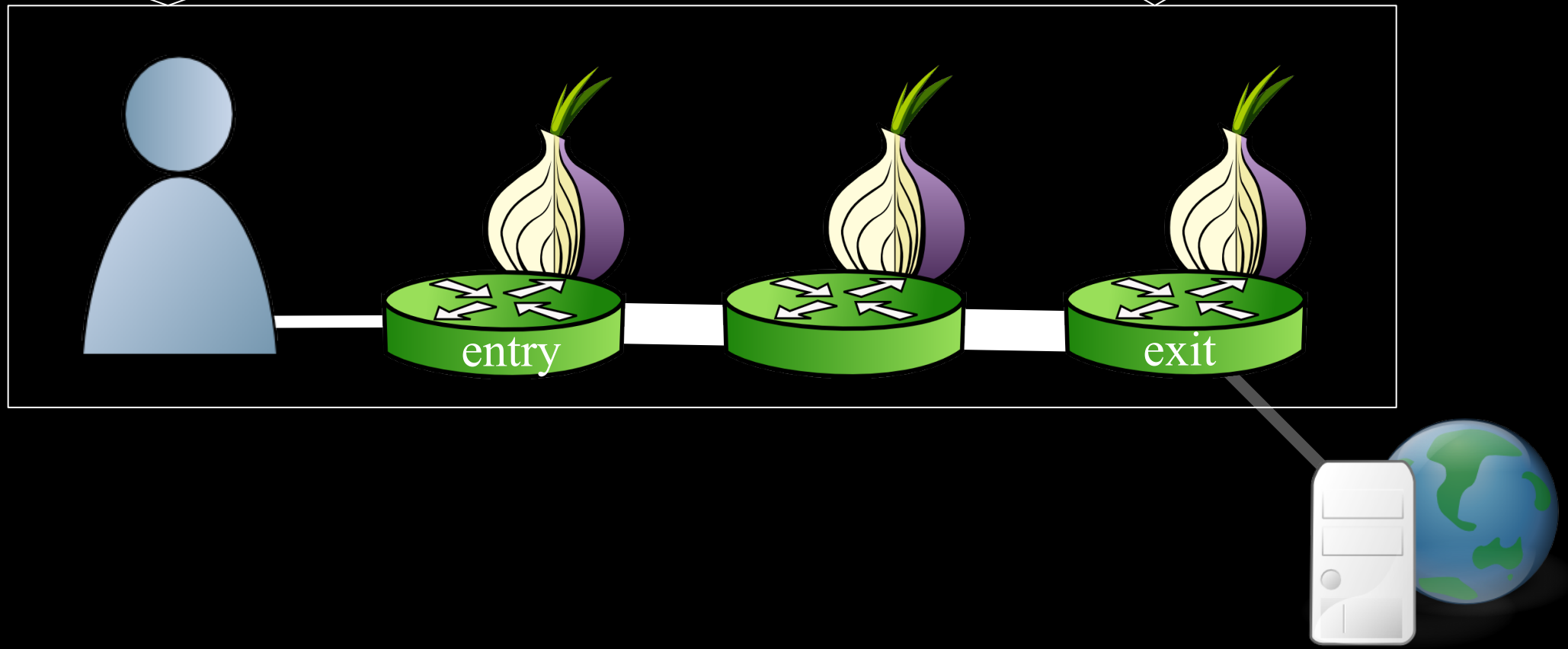
Tor Flow Control



Tor Flow Control

SENDME Signal
Every 100 Cells

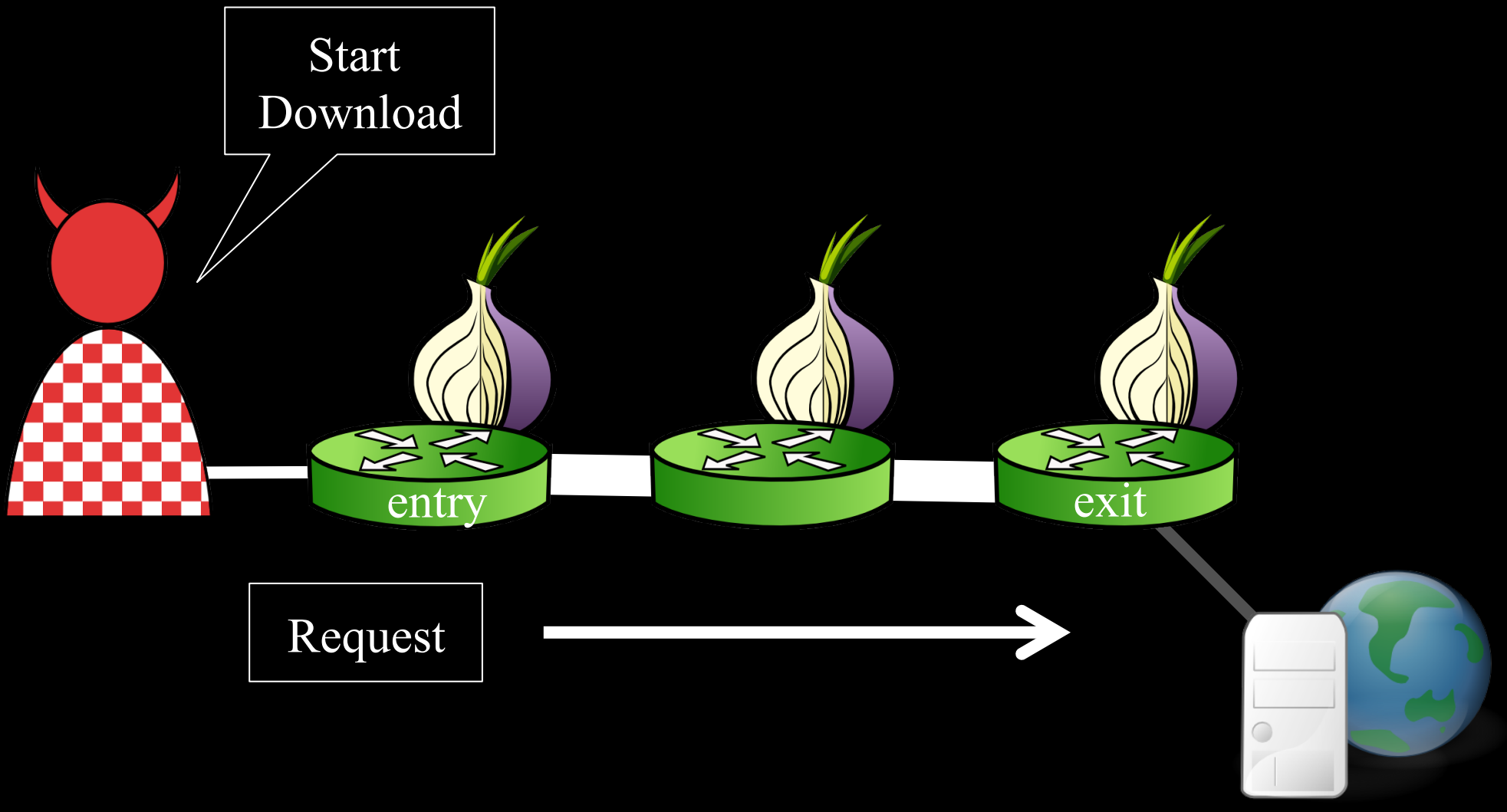
1000 Cell
Limit



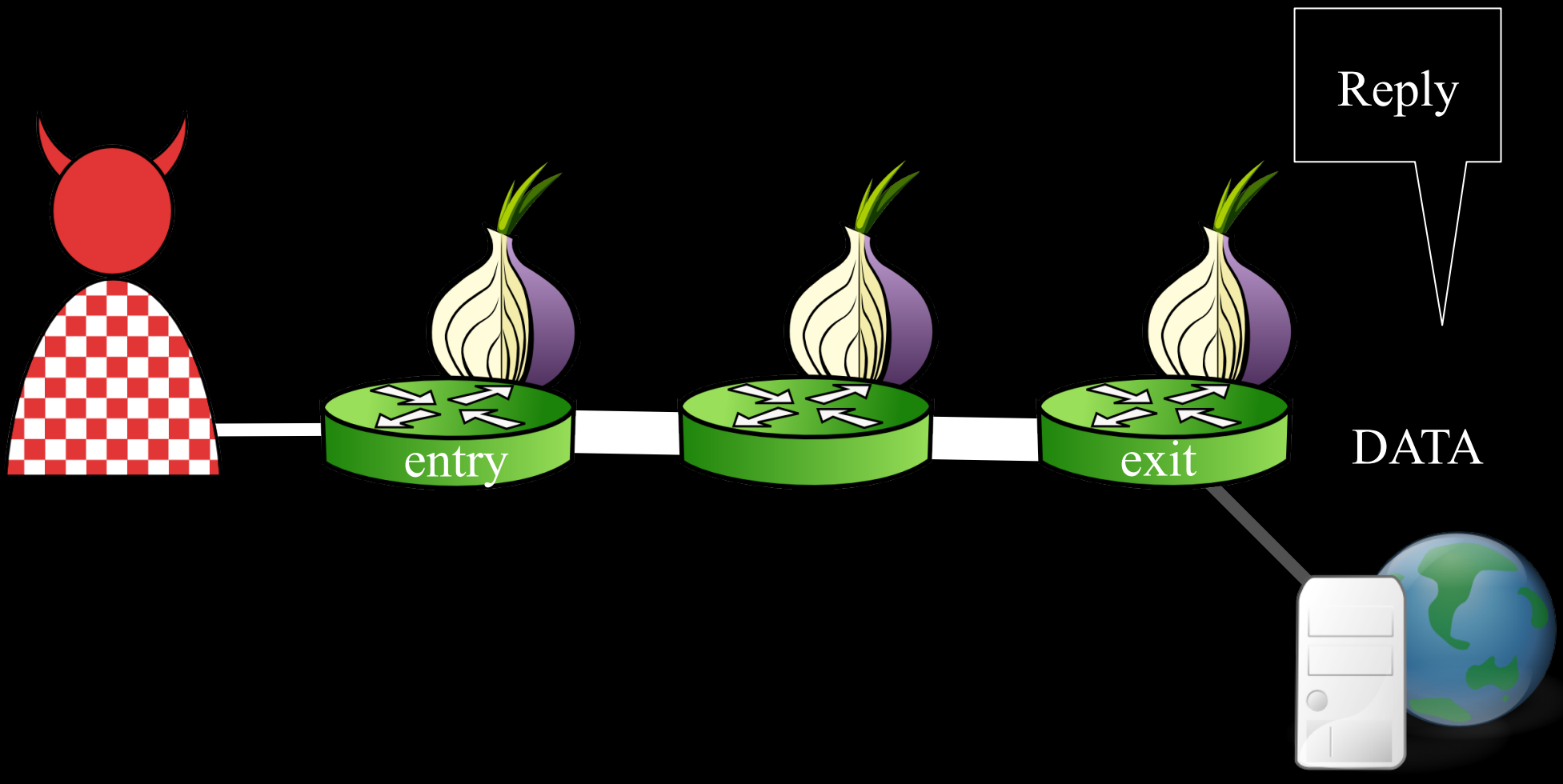
Outline

- The Sniper Attack
  - Low-cost memory consumption attack that disables arbitrary Tor relays
- Deanonymizing Hidden Services
  - Using DoS attacks for deanonymization
- Countermeasures

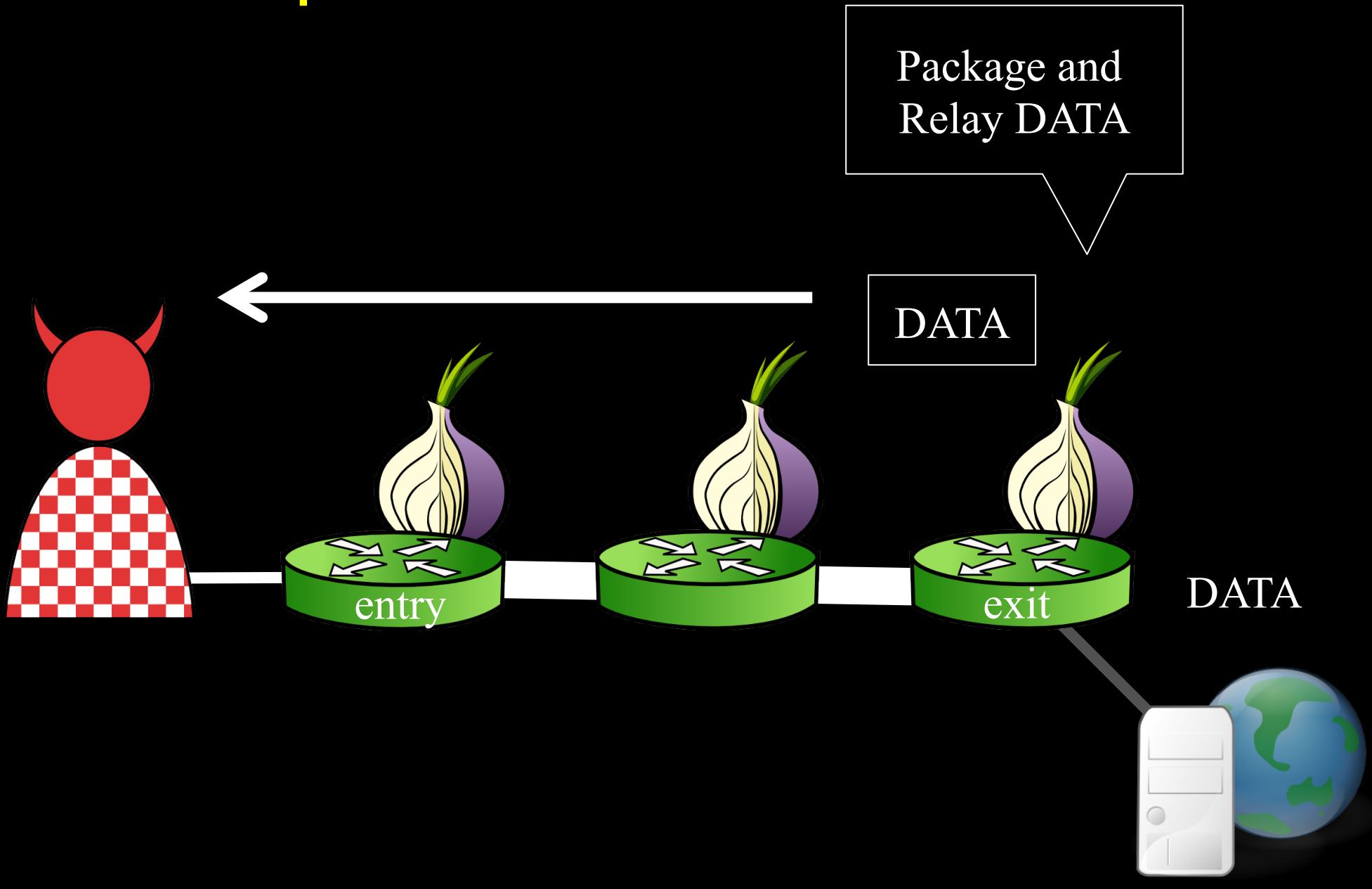
The Sniper Attack



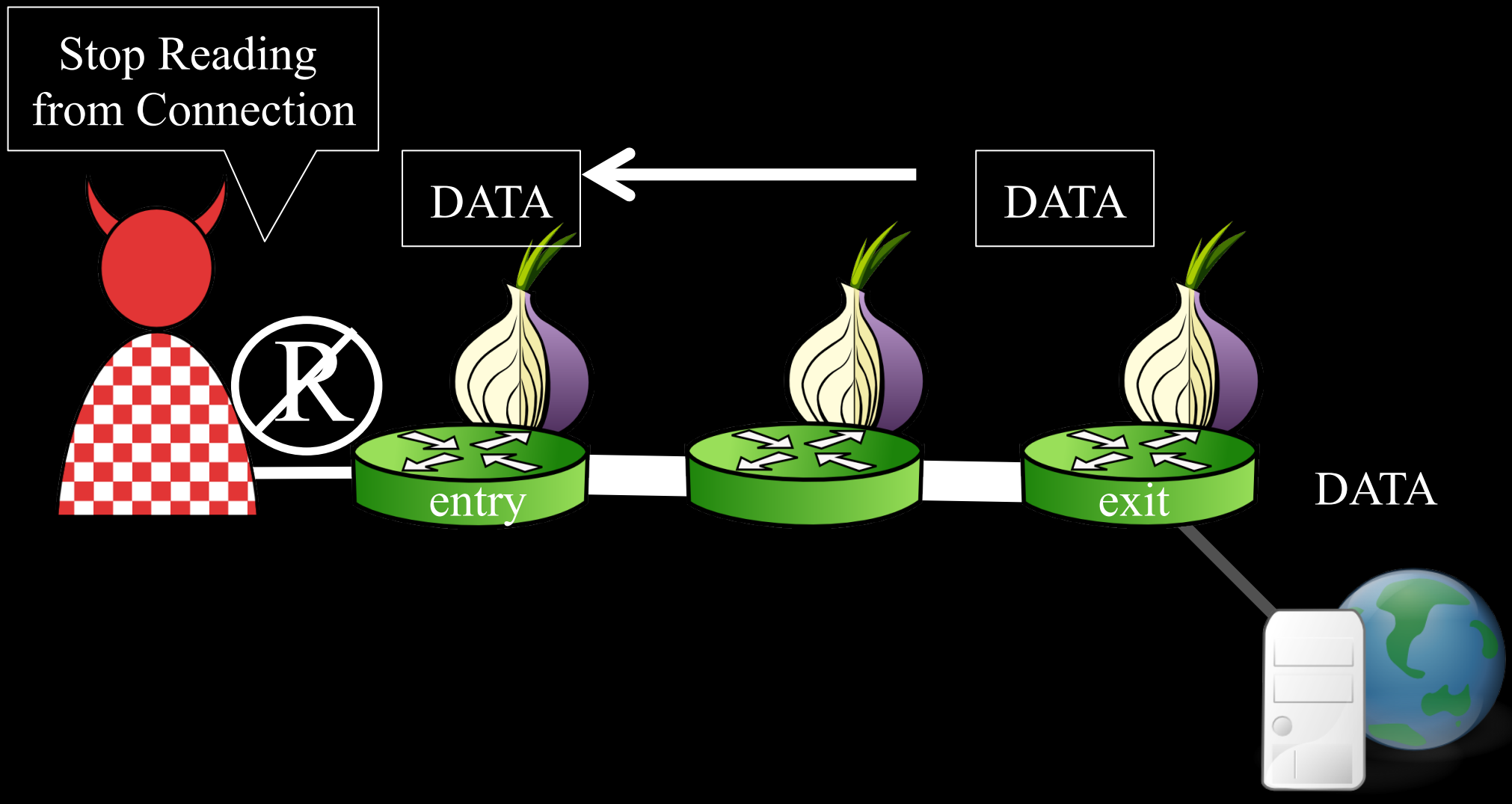
The Sniper Attack



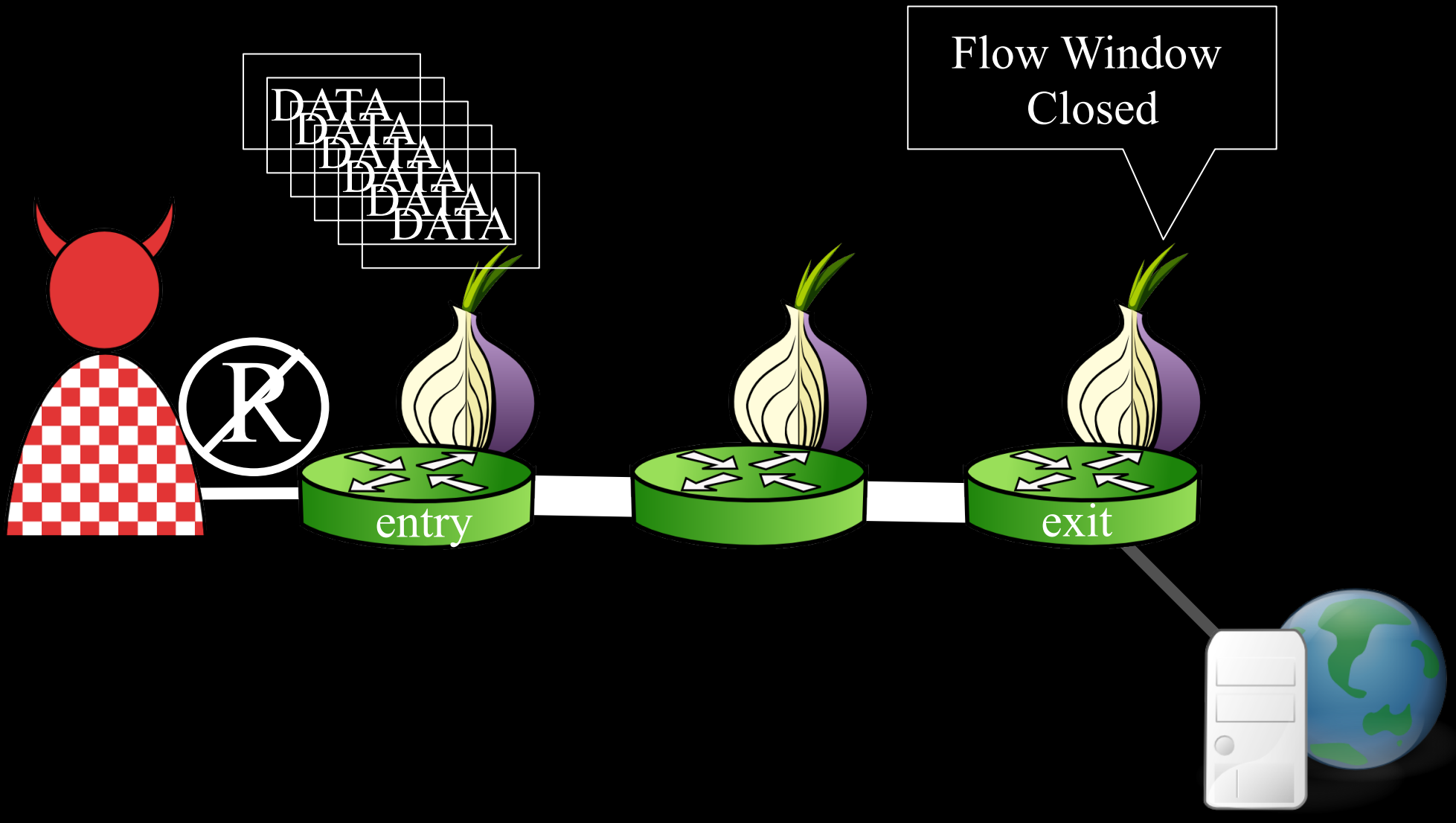
The Sniper Attack



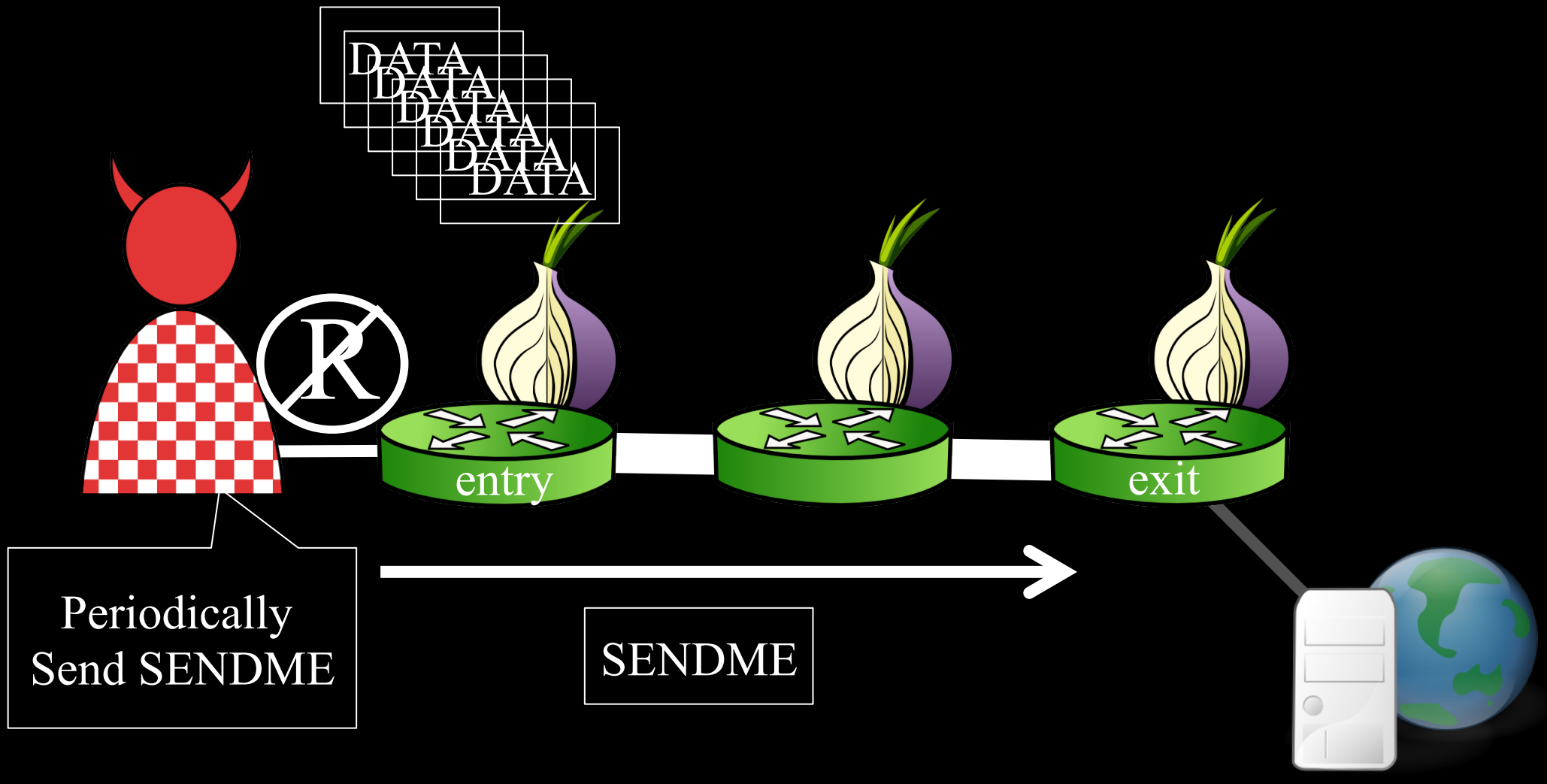
The Sniper Attack



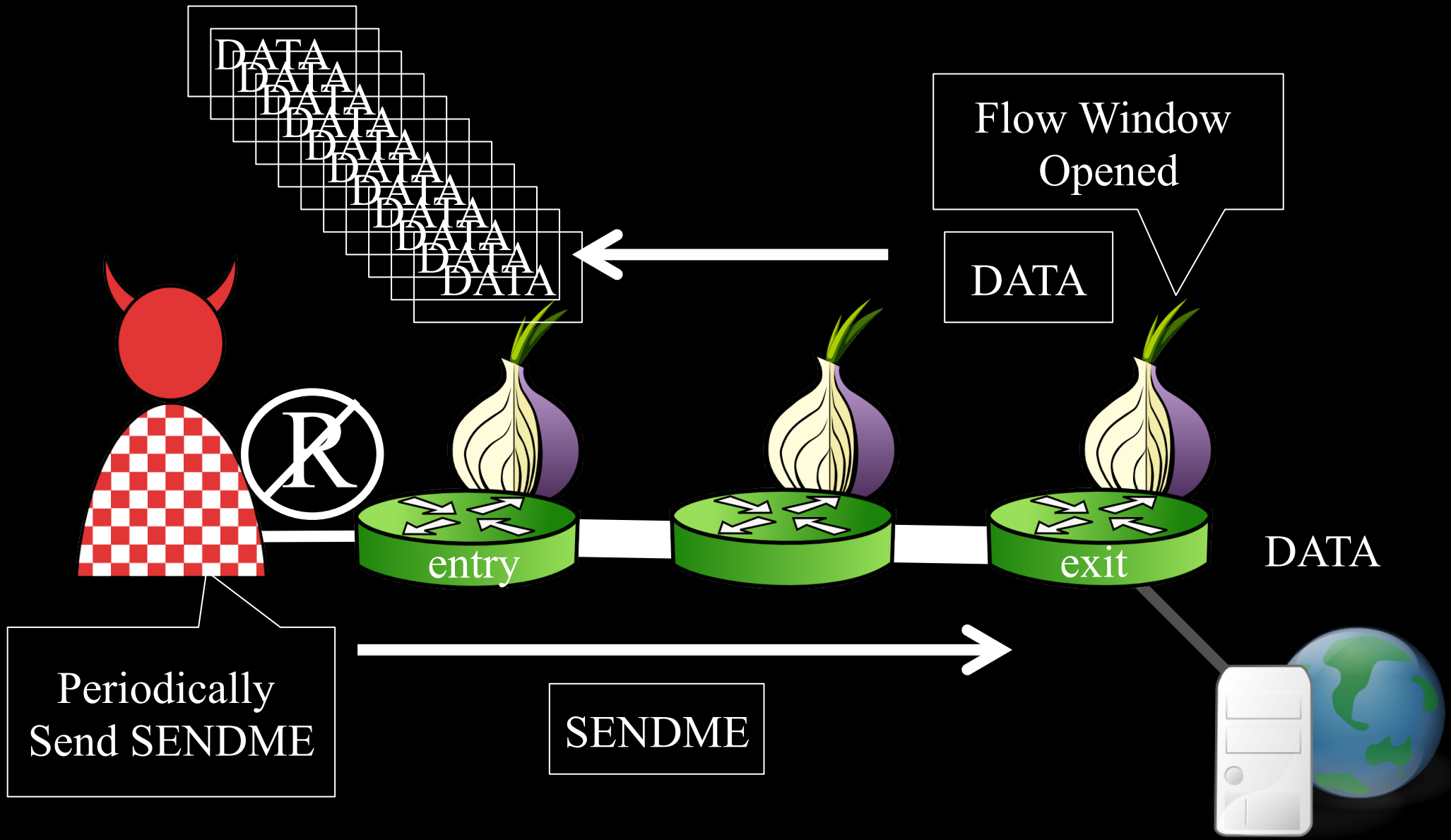
The Sniper Attack



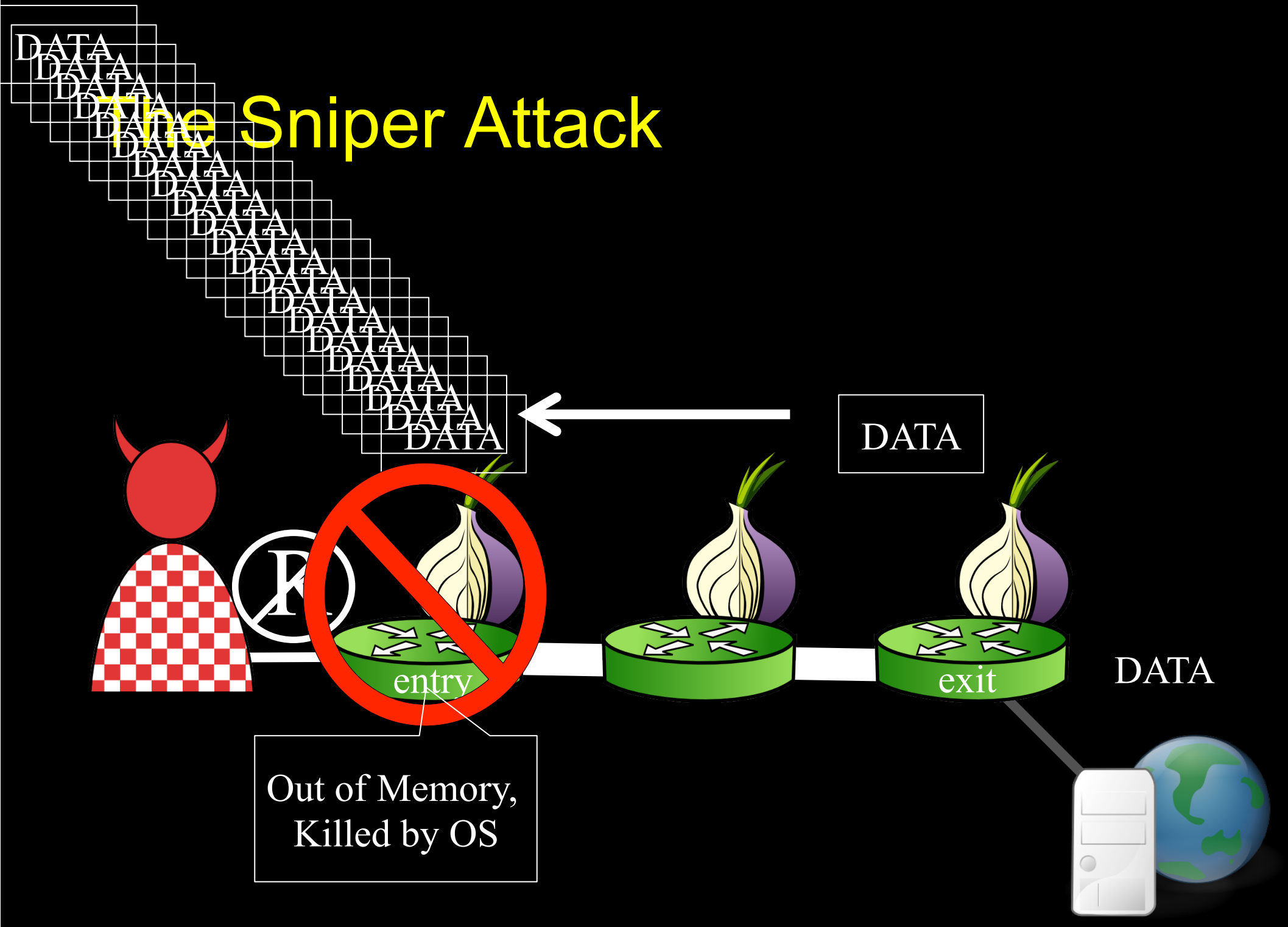
The Sniper Attack



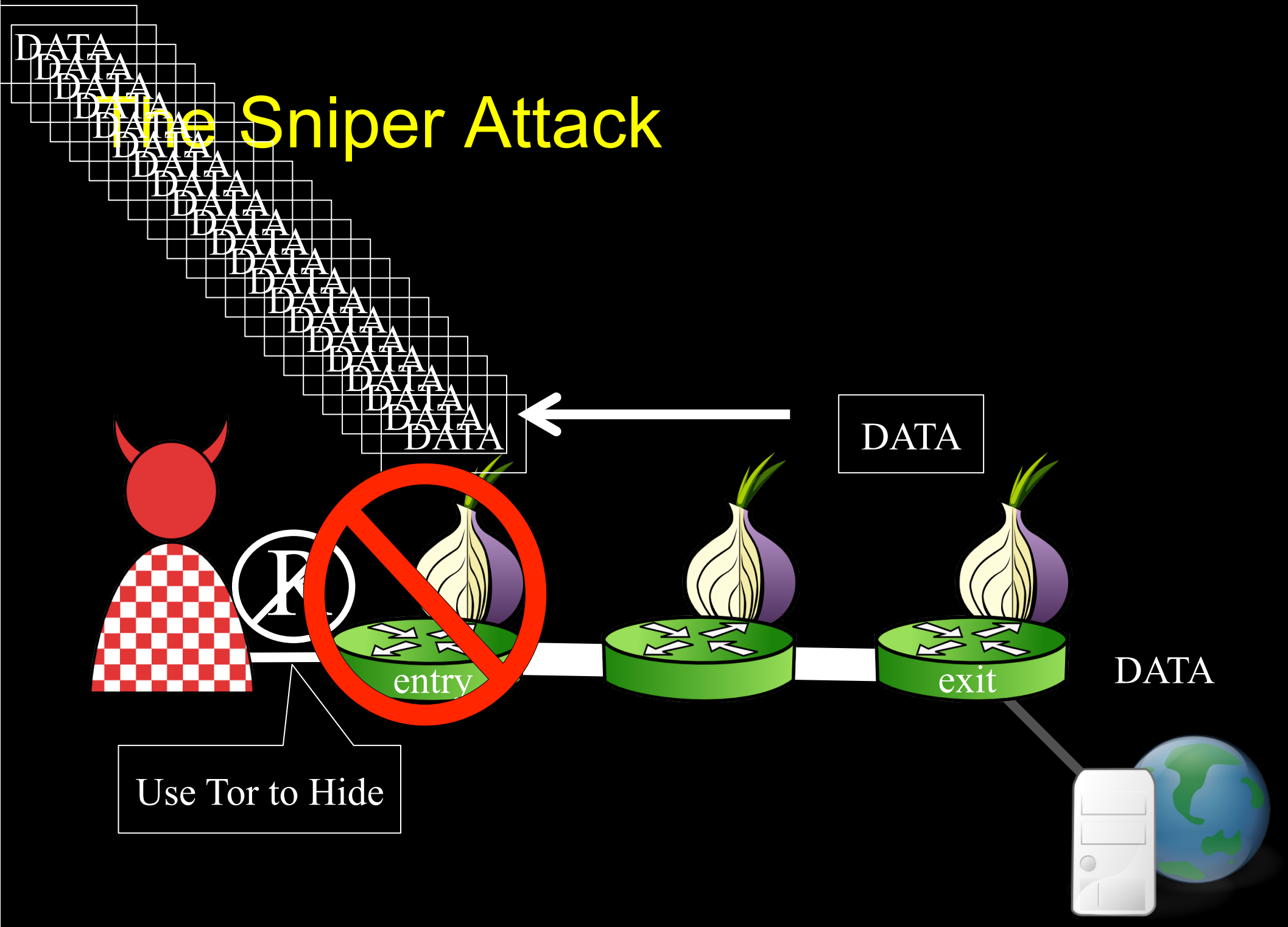
The Sniper Attack



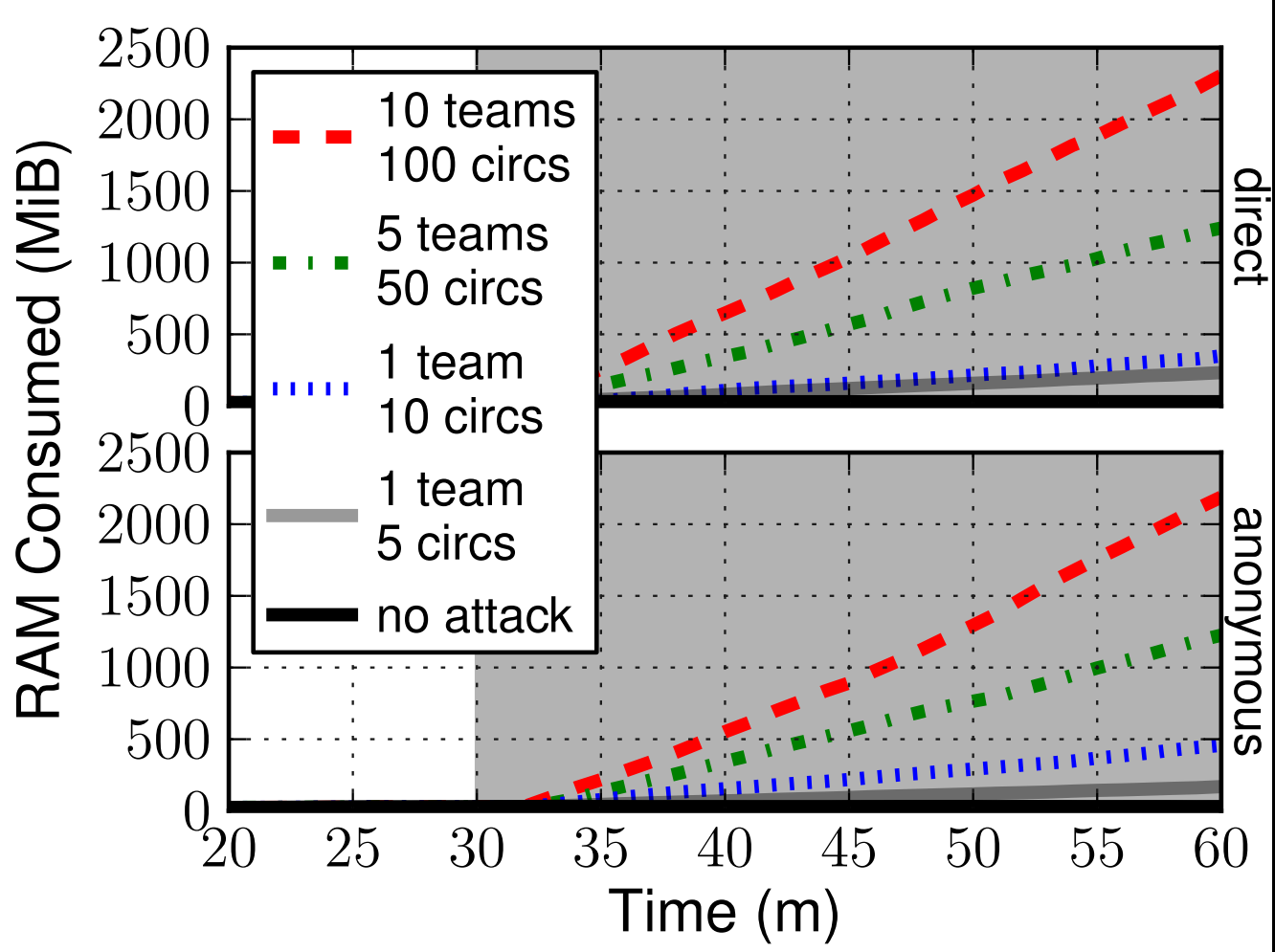
The Sniper Attack



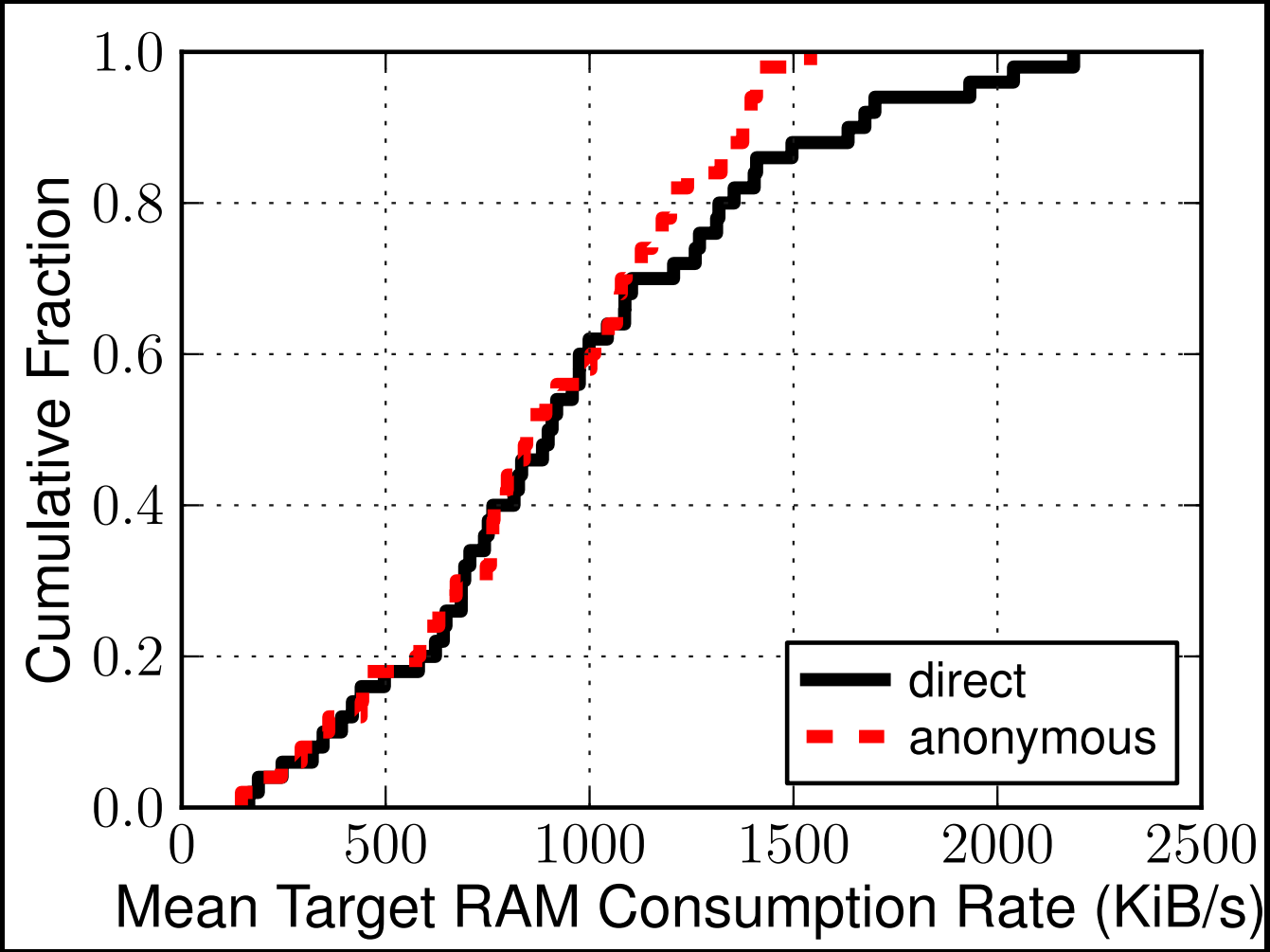
The Sniper Attack



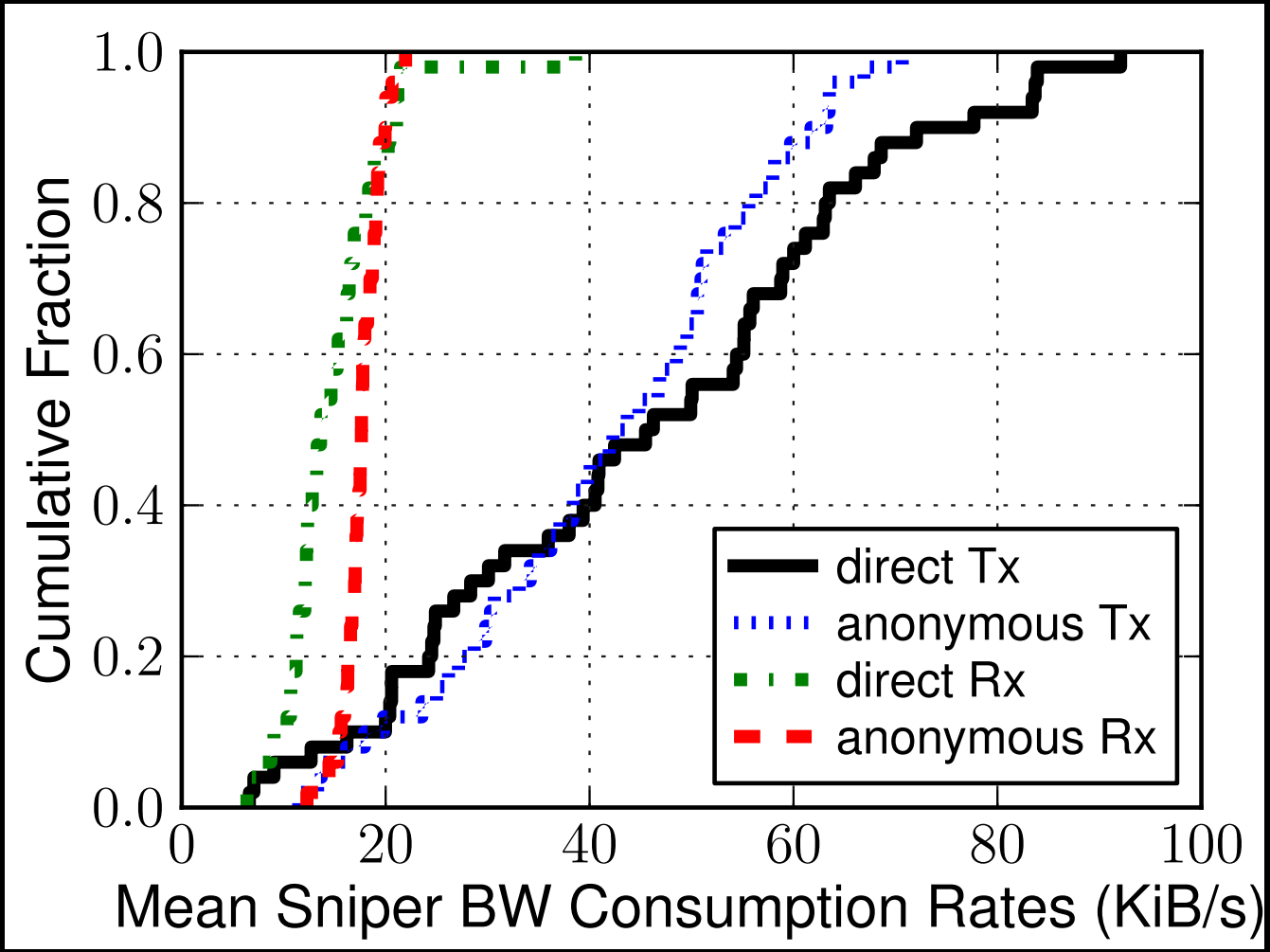
Memory Consumed over Time



Mean RAM Consumed, 50 Relays



Mean BW Consumed, 50 Relays



Speed of Sniper Attack

		Direct		Anonymous	
Relay Groups	**Select %**	**1 GiB**	**8 GiB**	**1 GiB**	**8 GiB**
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
≈ Network Capacity

Speed of Sniper Attack

		Direct		Anonymous	
Relay Groups	**Select %**	**1 GiB**	**8 GiB**	**1 GiB**	**8 GiB**
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	
Relay Groups	**Select %**	**1 GiB**	**8 GiB**	**1 GiB**	**8 GiB**
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	
Relay Groups	**Select %**	**1 GiB**	**8 GiB**	**1 GiB**	**8 GiB**
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

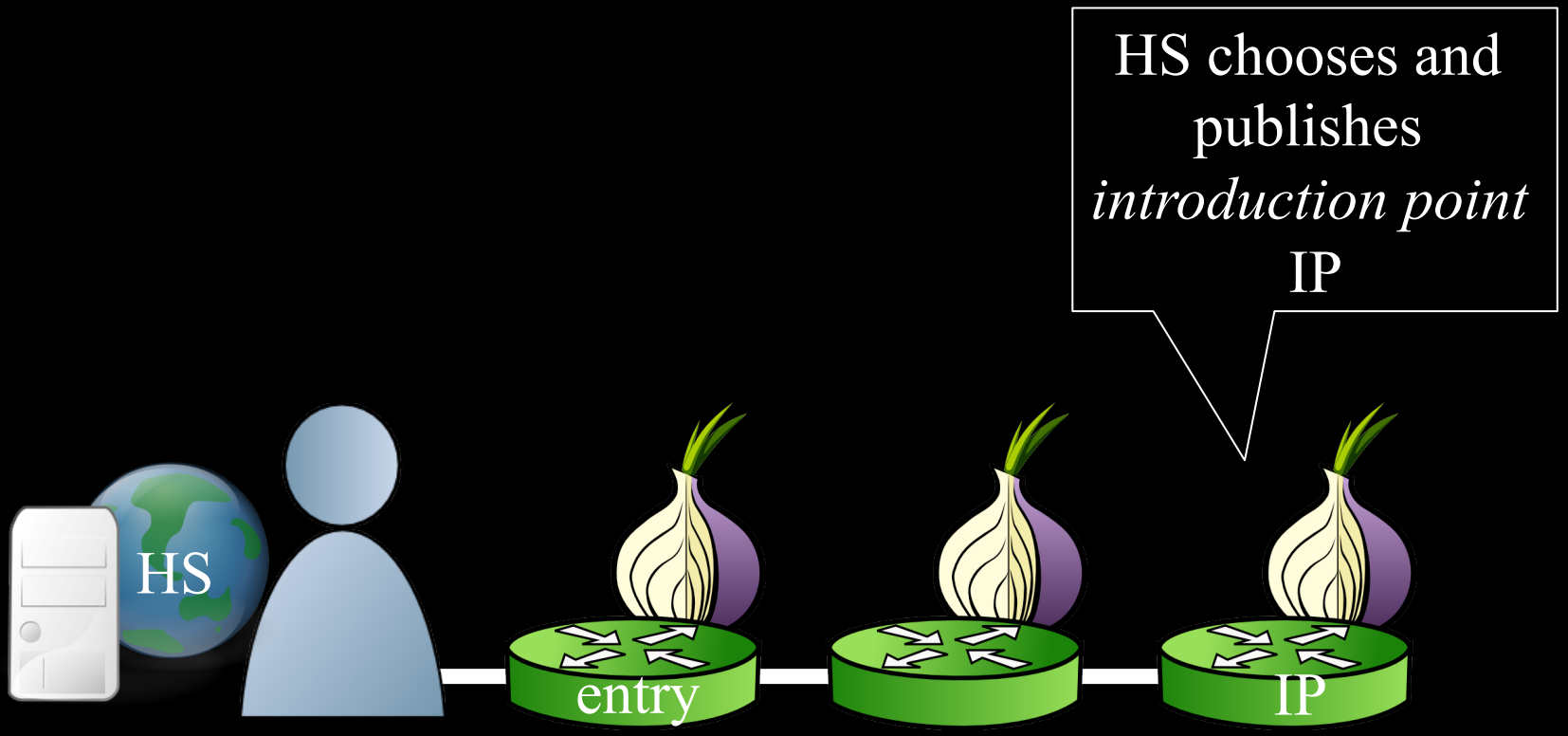
Time (hours:minutes) to Consume RAM

Outline

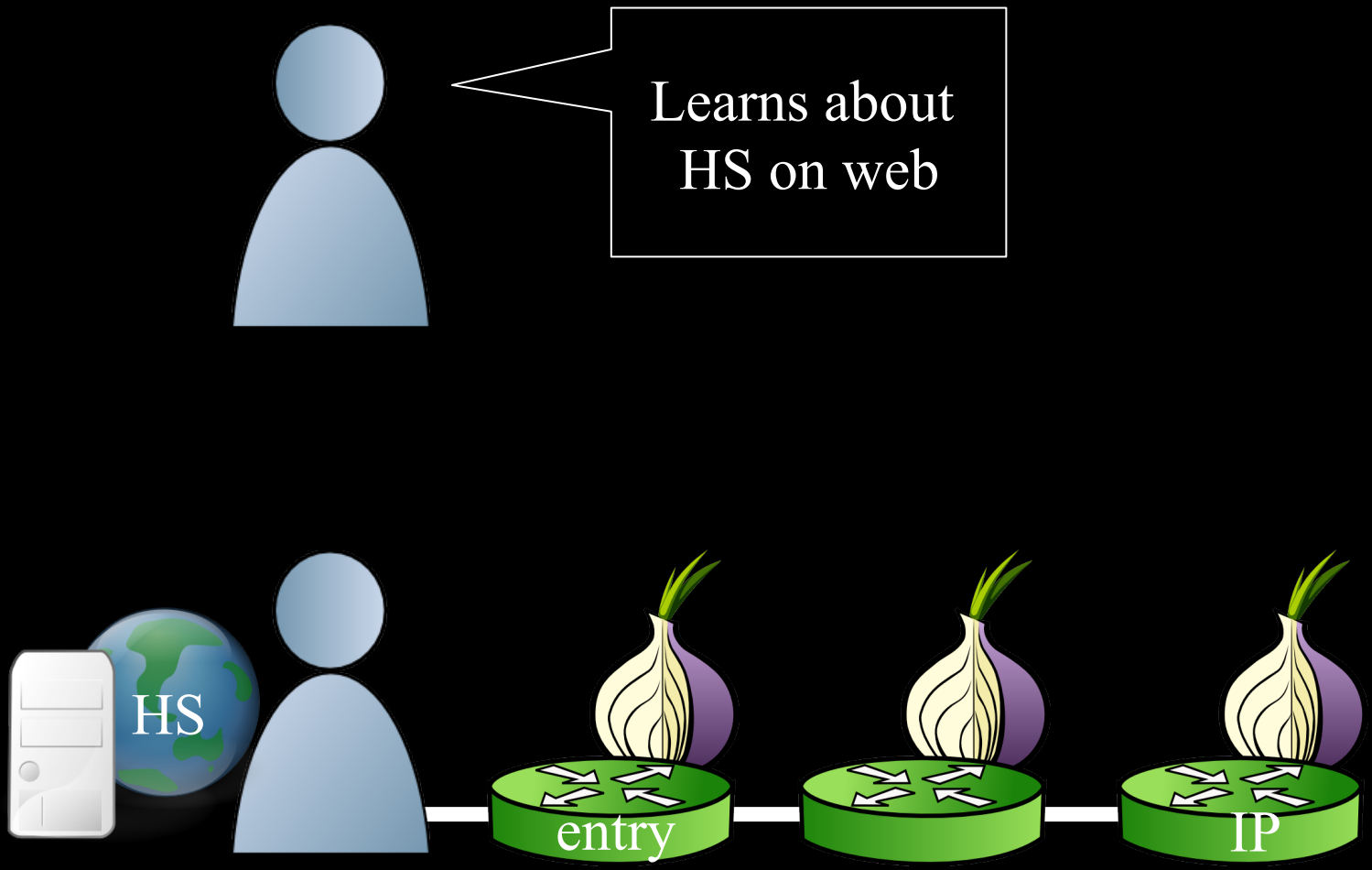
- The Sniper Attack
  - Low-cost memory consumption attack that disables arbitrary Tor relays
- Deanonymizing Hidden Services
  - Using DoS attacks for deanonymization
- Countermeasures

Hidden Services

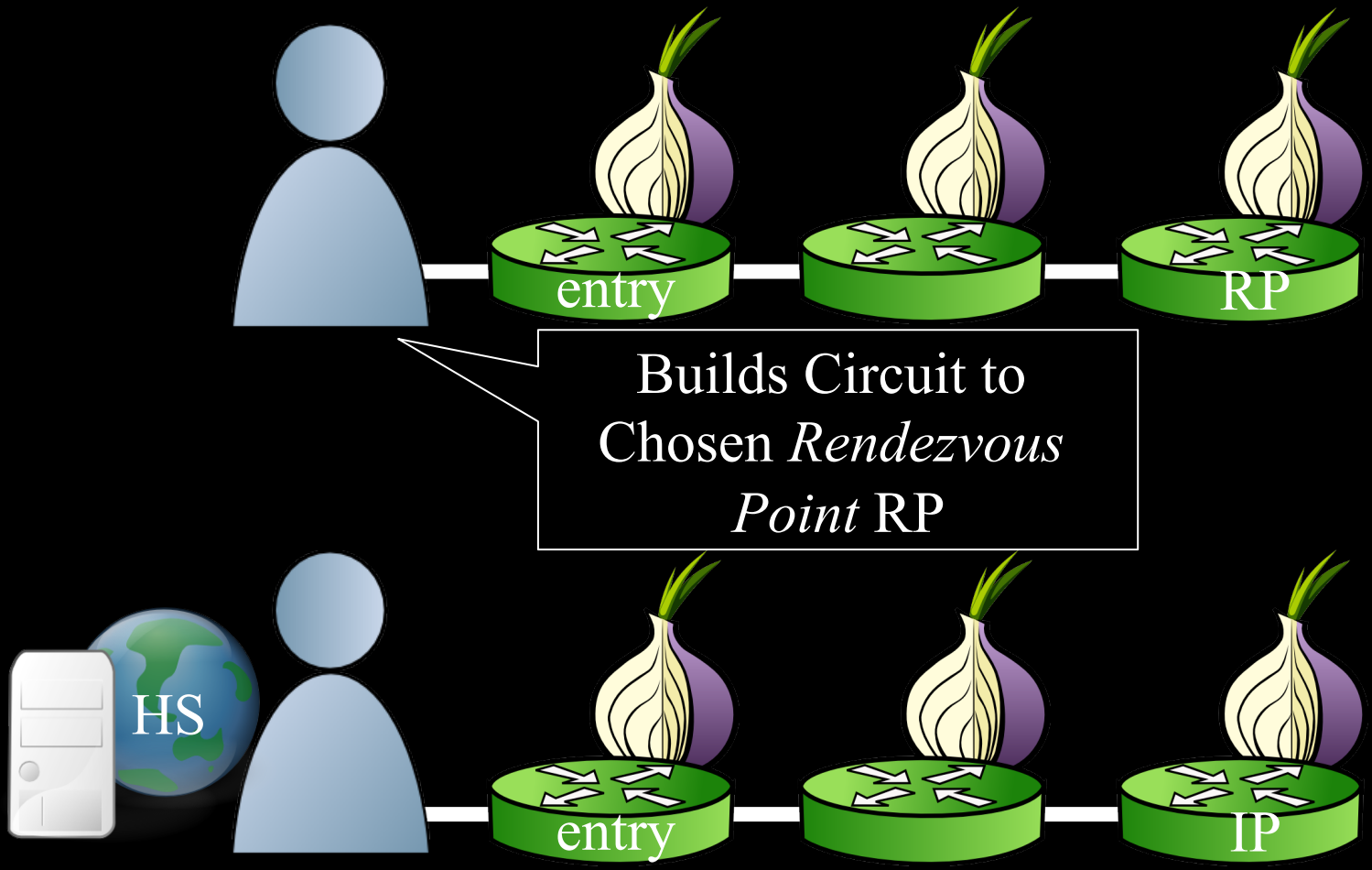
Hidden Services



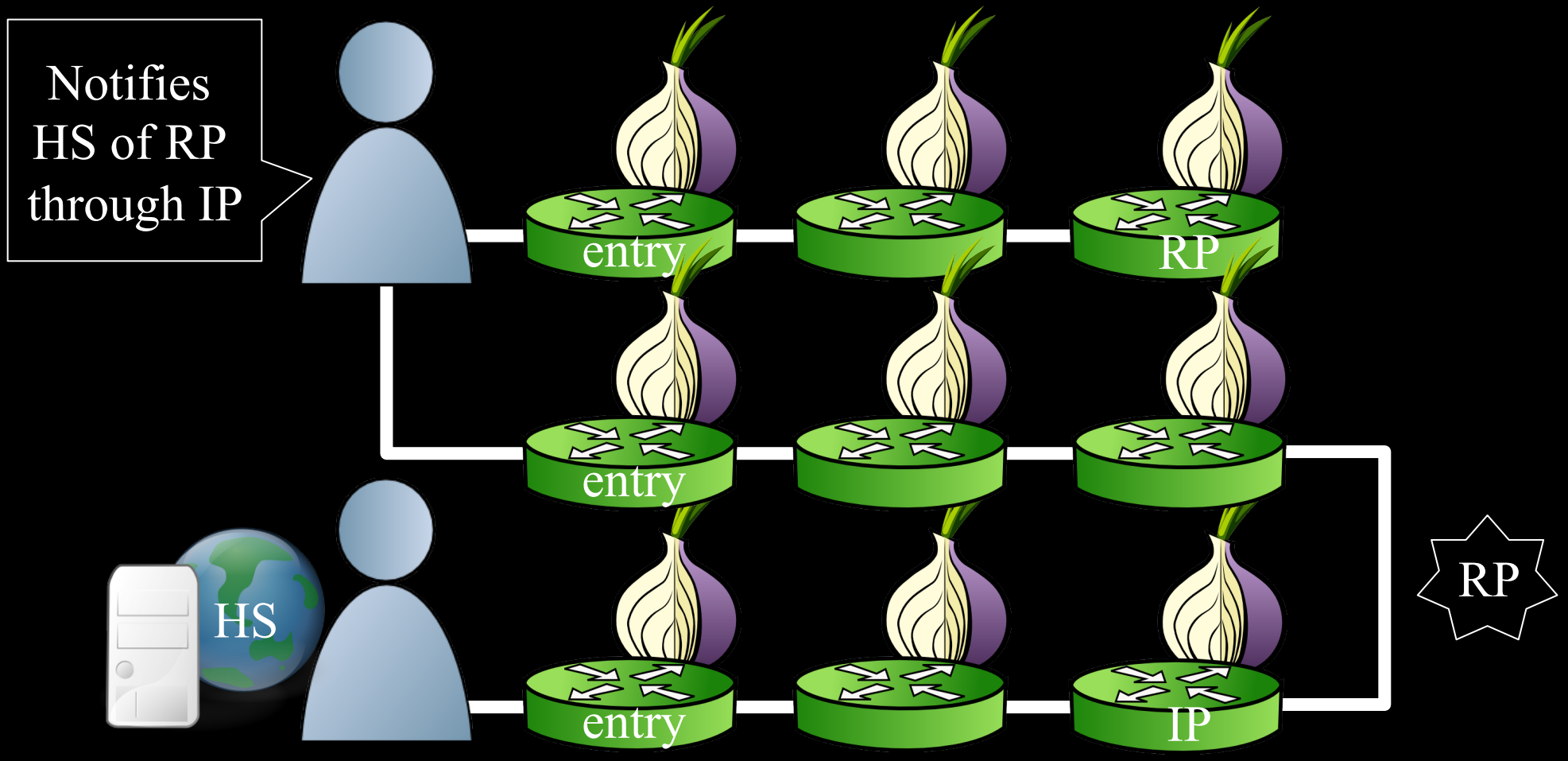
Hidden Services



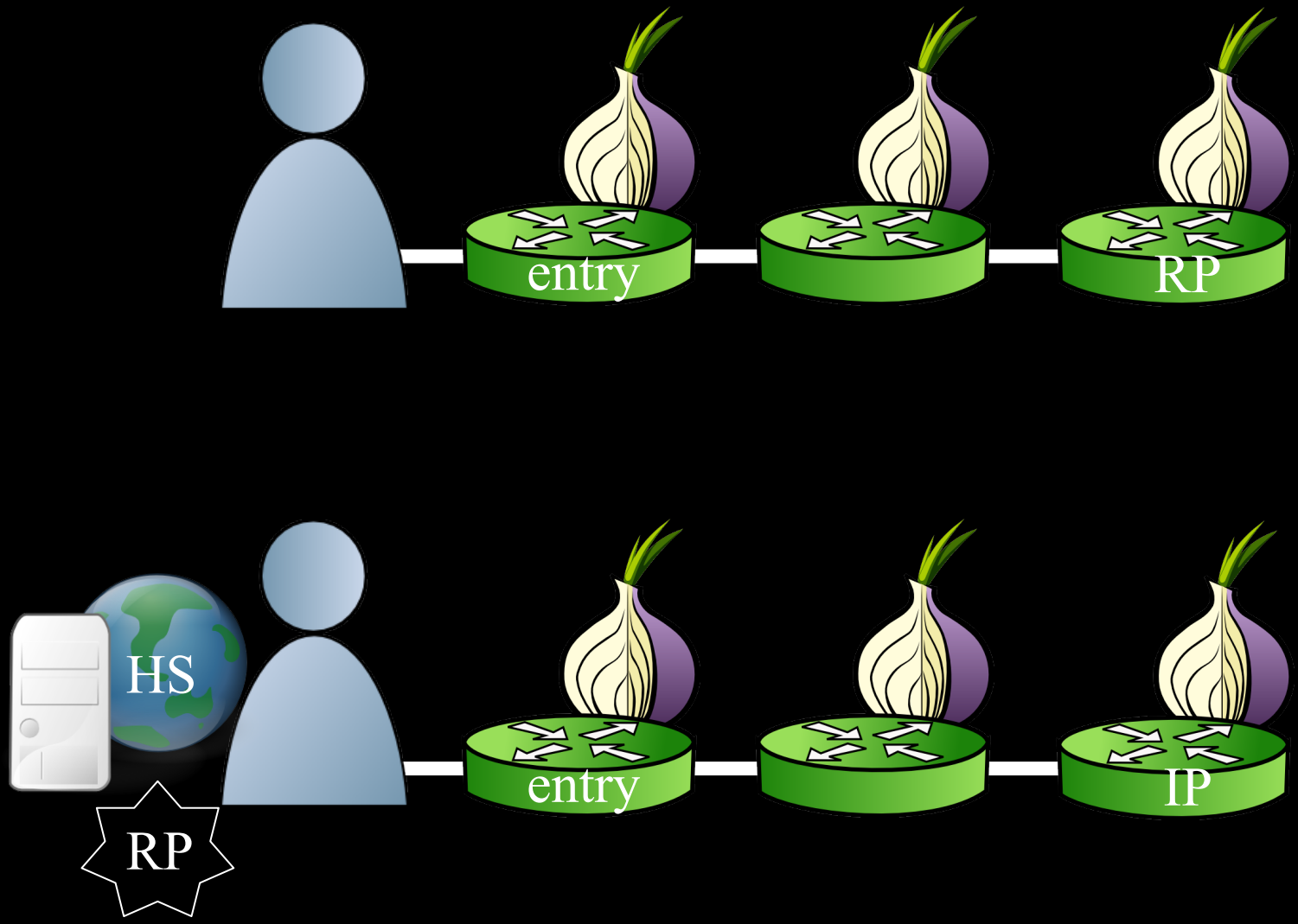
Hidden Services



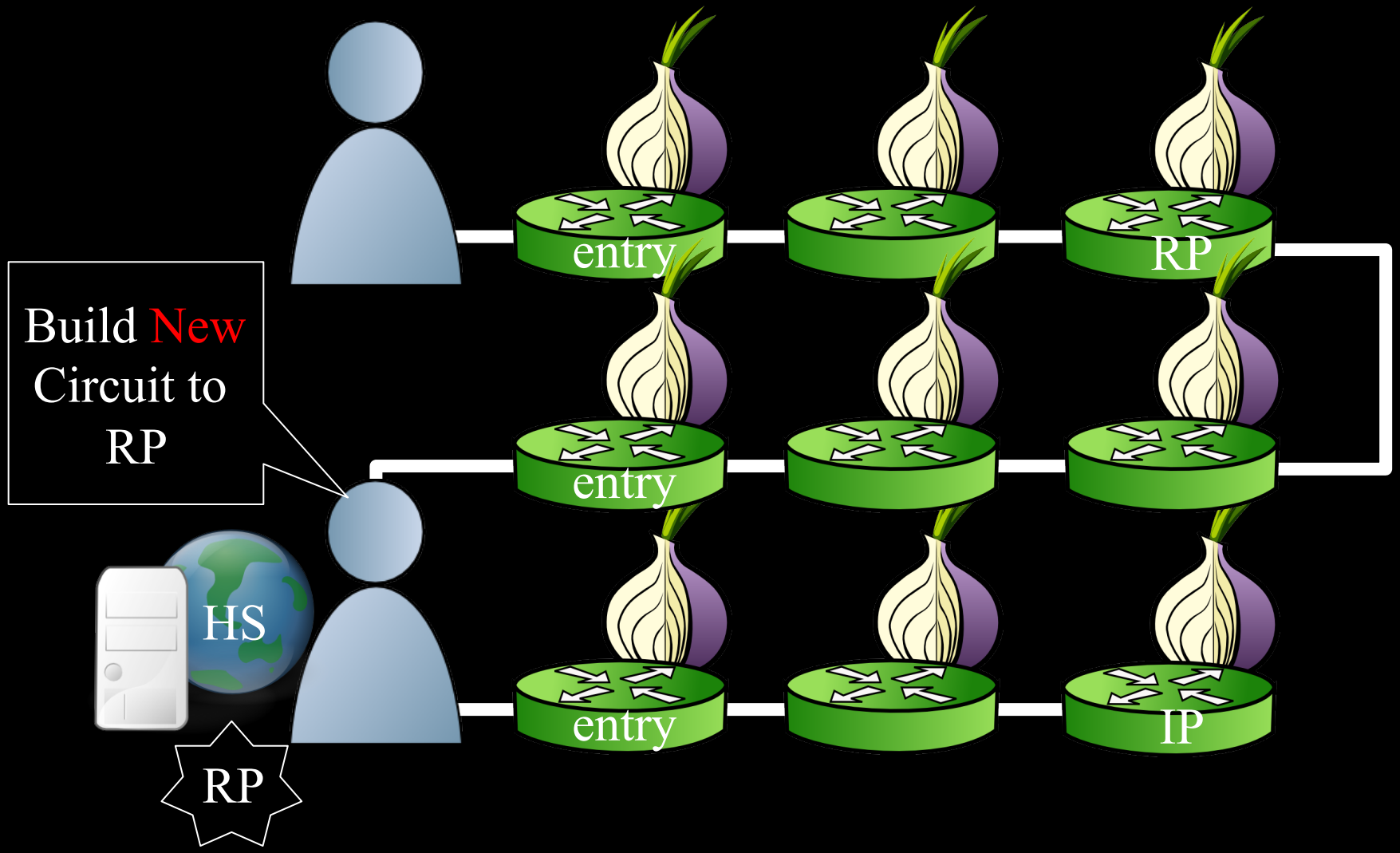
Hidden Services



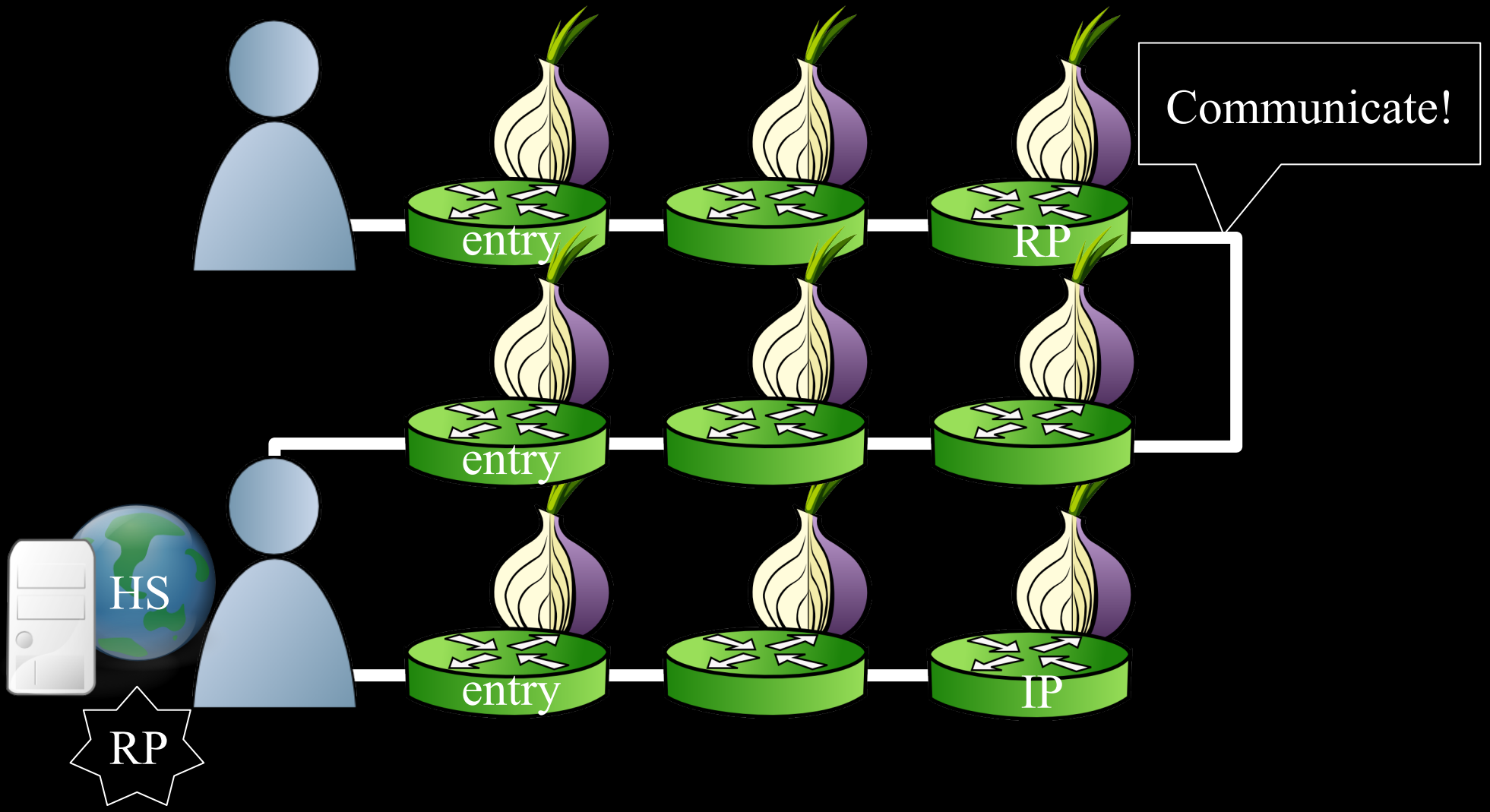
Hidden Services



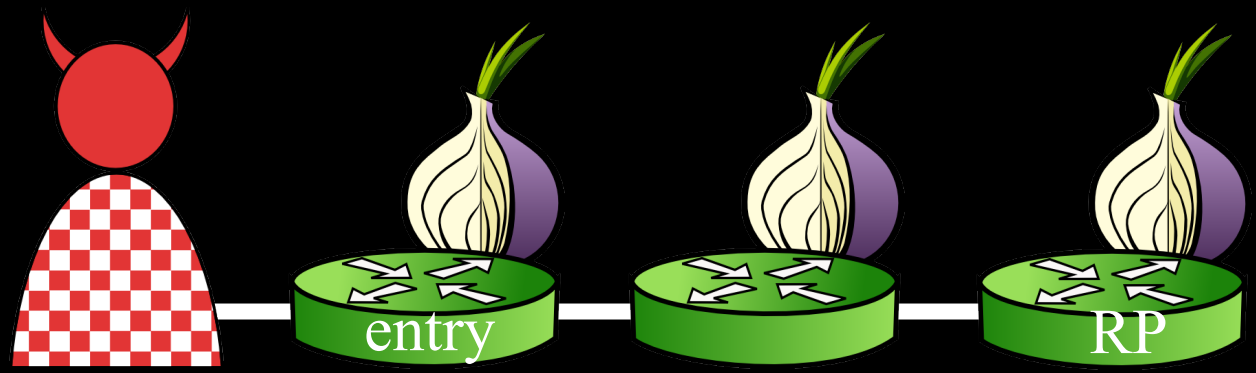
Hidden Services



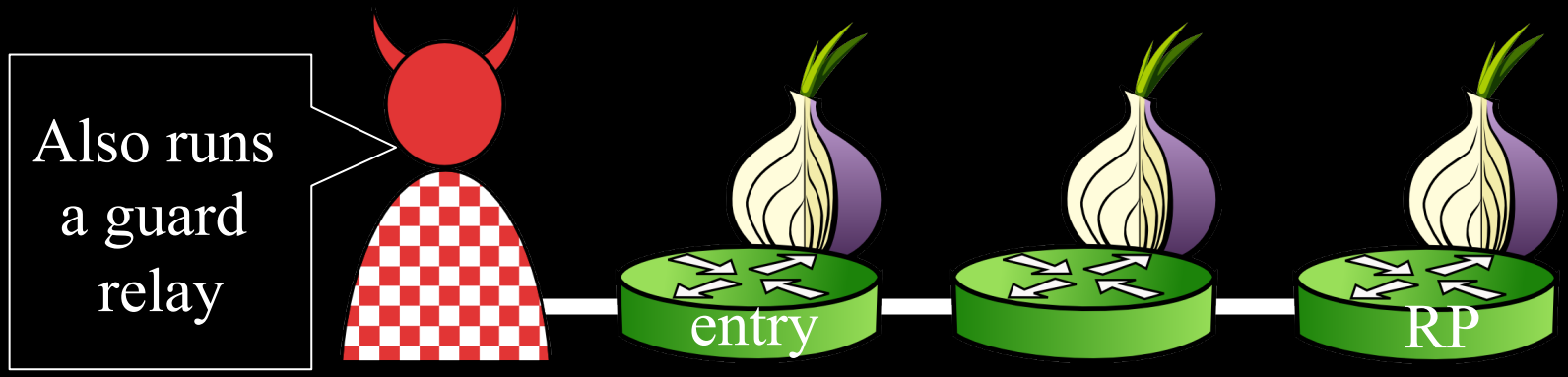
Hidden Services



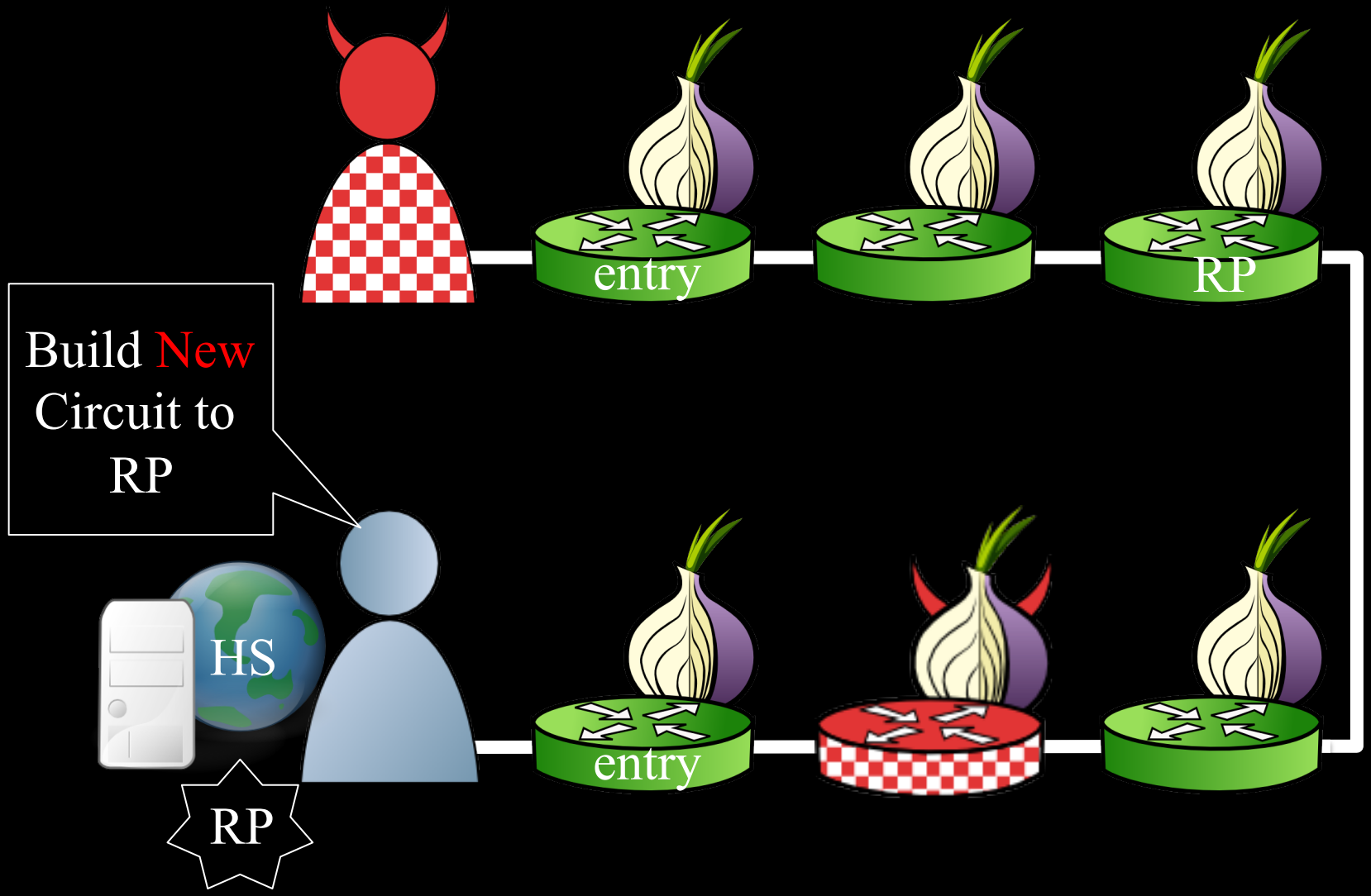
Deanonymizing Hidden Services



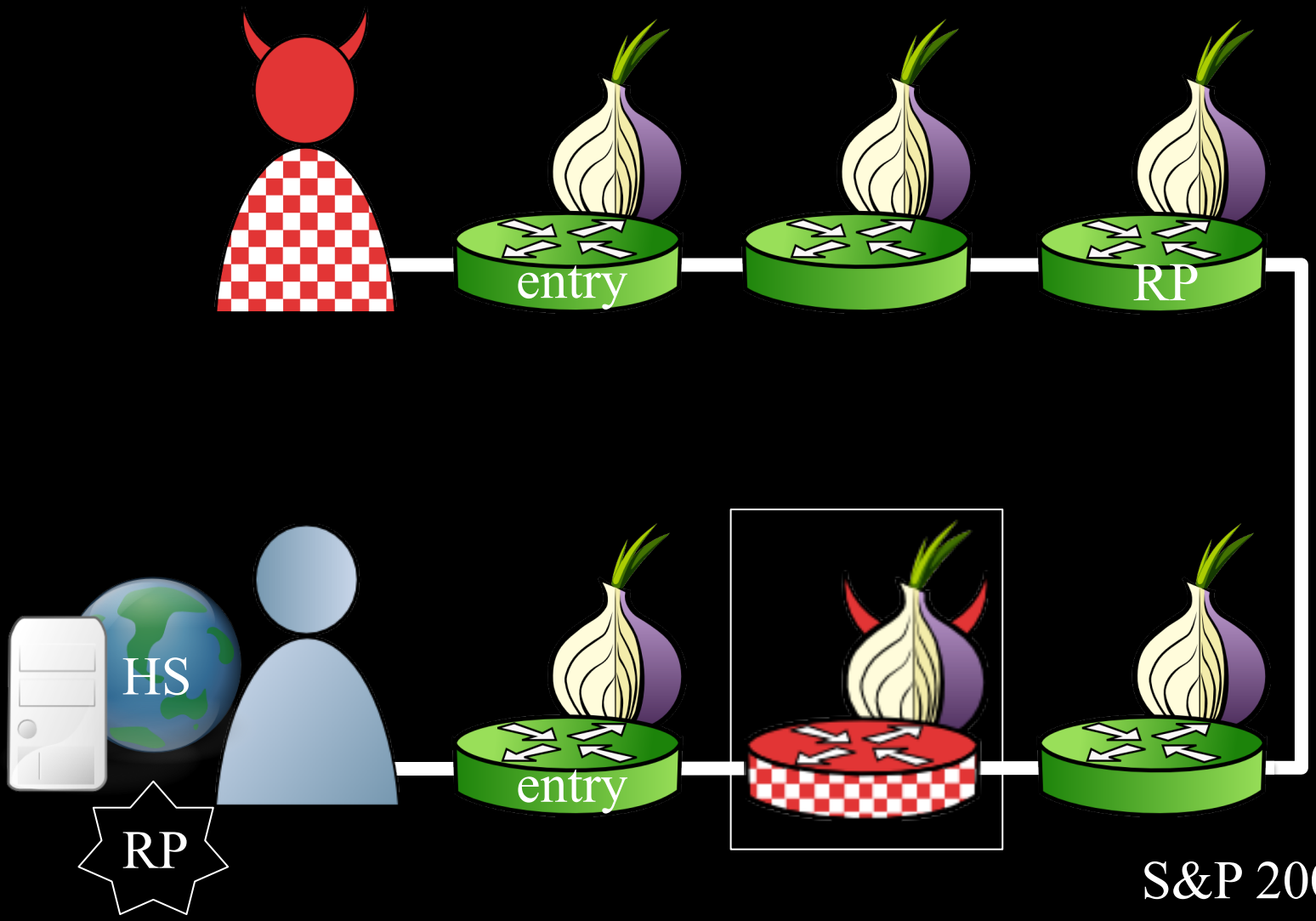
Deanonymizing Hidden Services



Deanonymizing Hidden Services

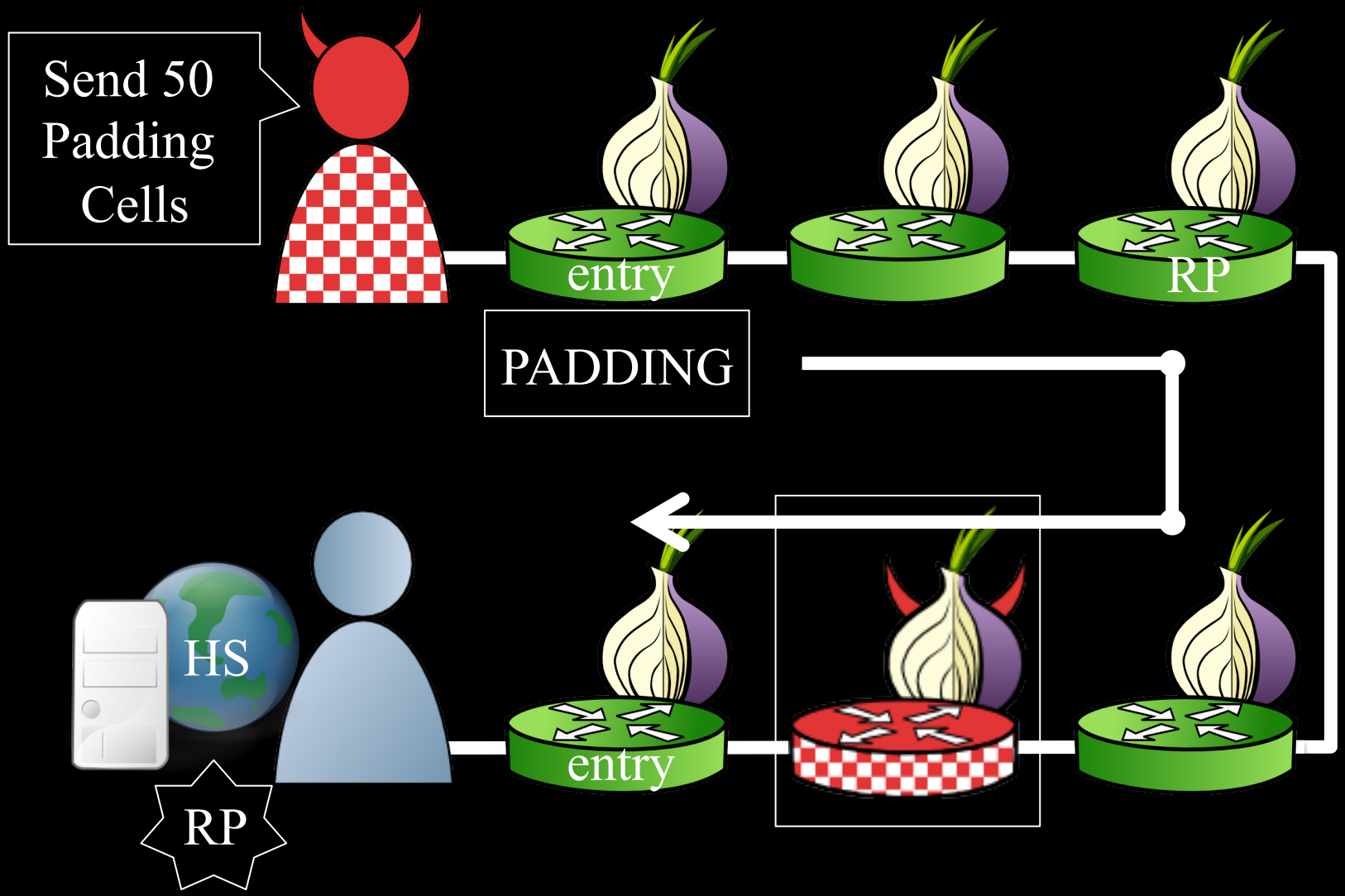


Deanonymizing Hidden Services



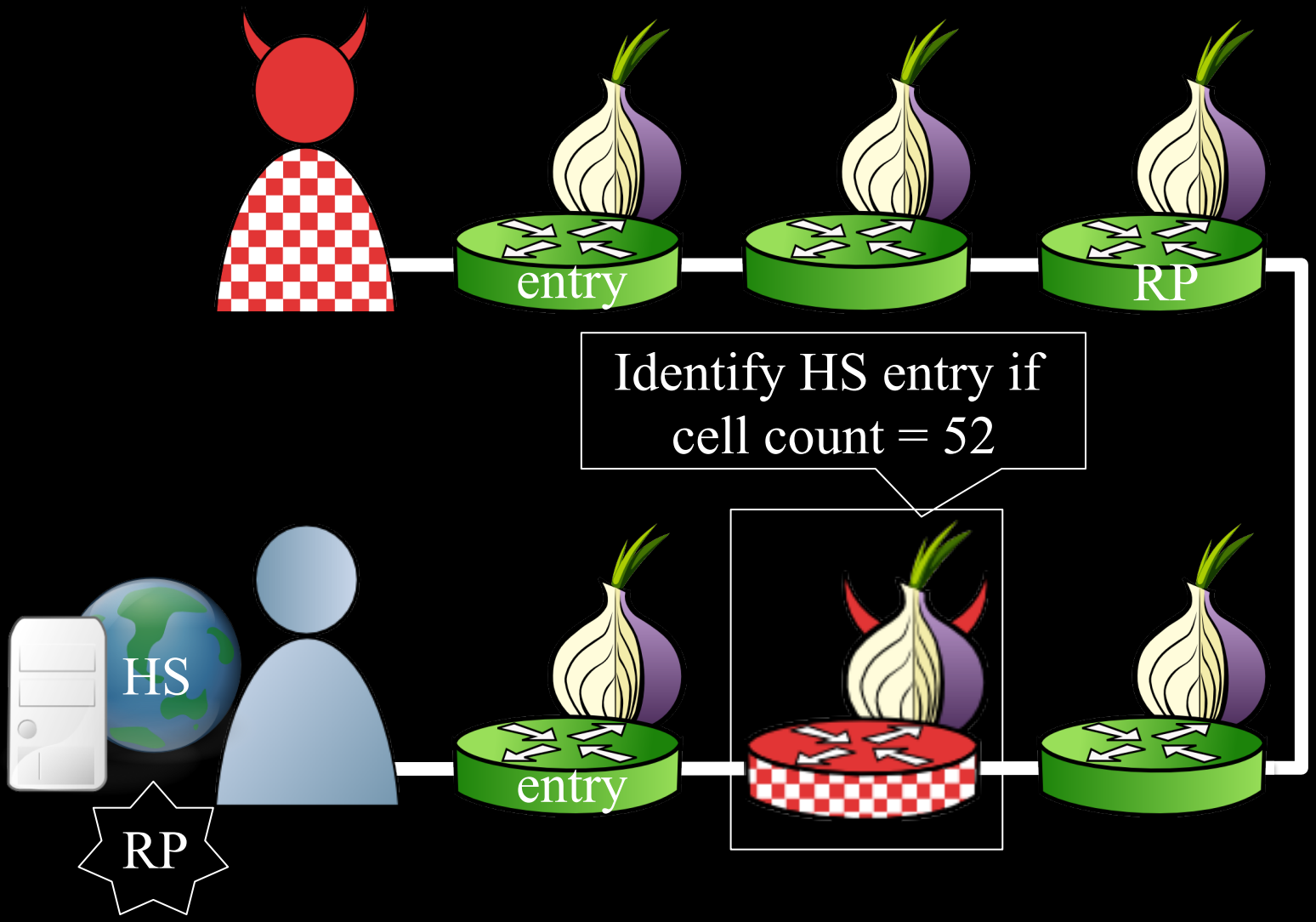
S&P 2006, S&P 2013

Deanonymizing Hidden Services



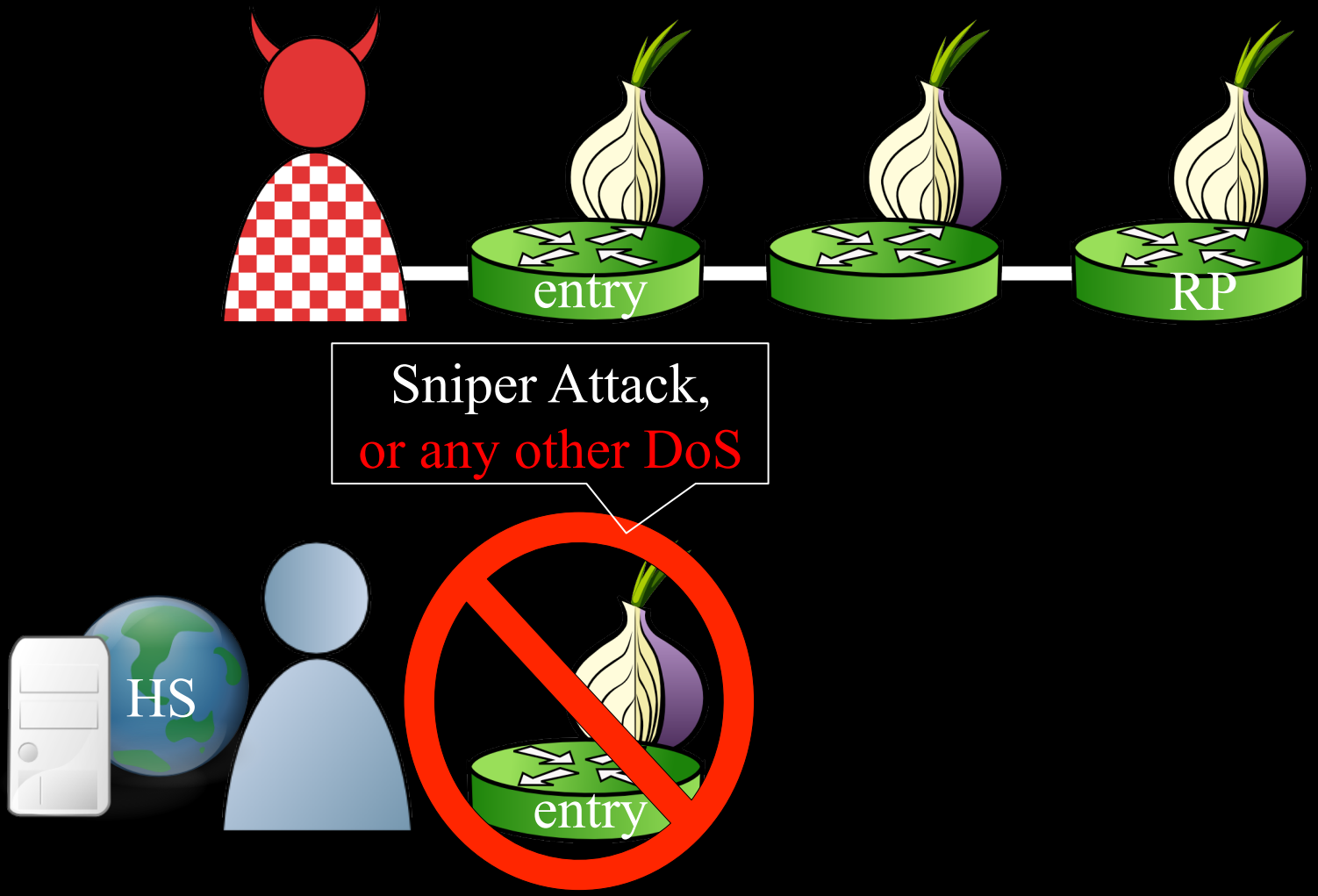
S&P 2013

Deanonymizing Hidden Services

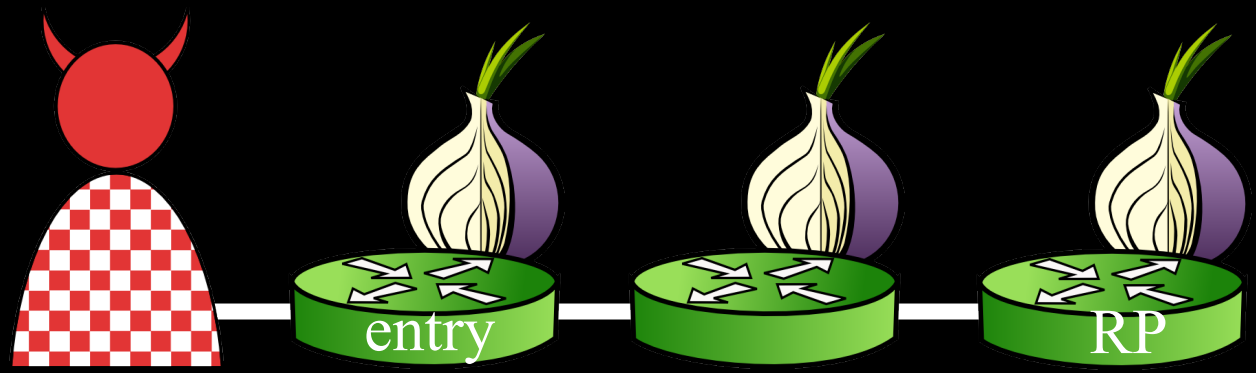


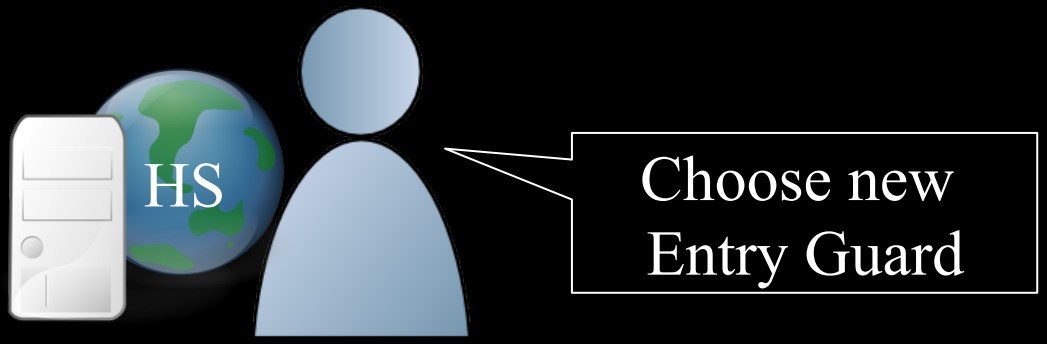
S&P 2013

Deanonymizing Hidden Services

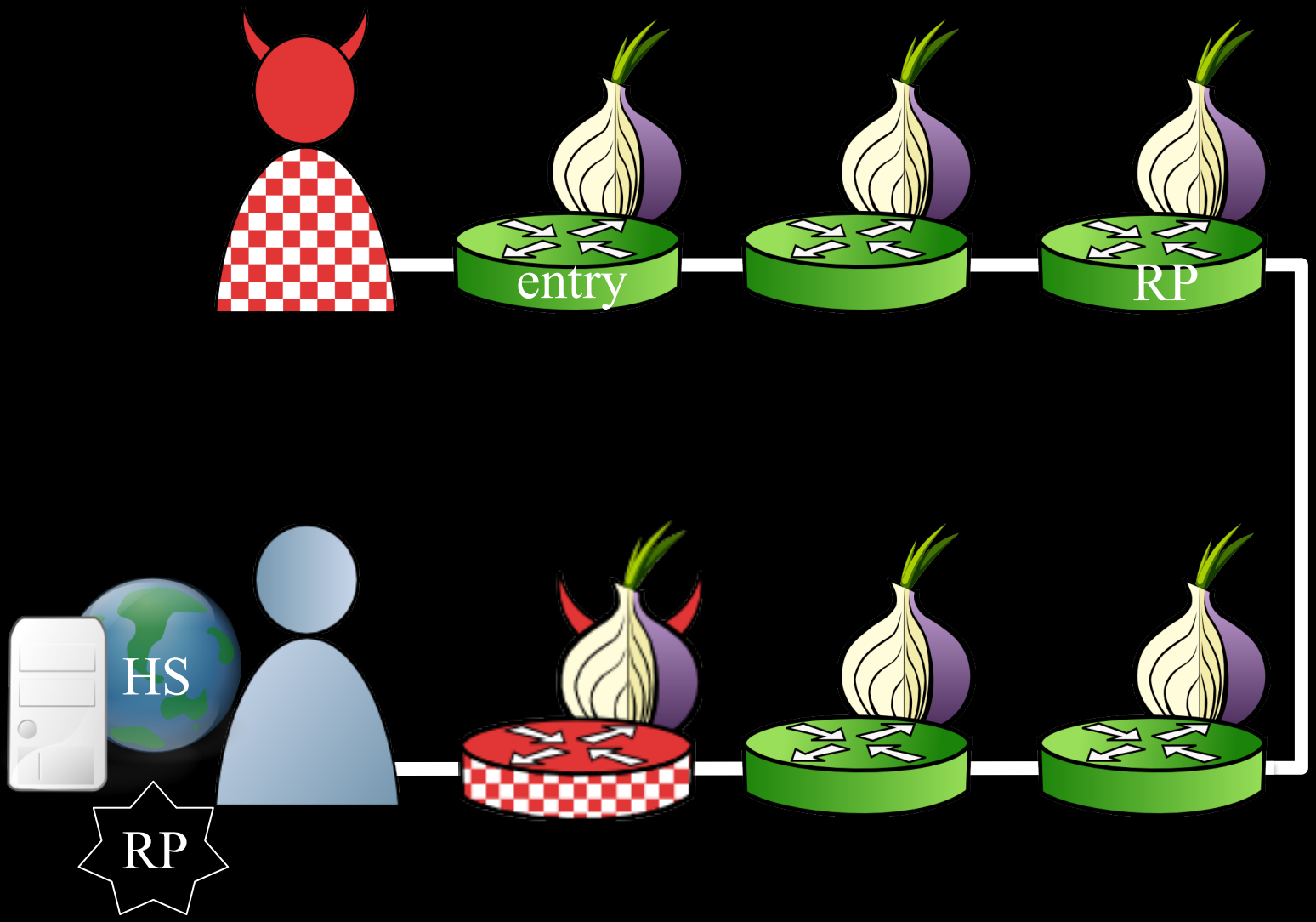


Deanonymizing Hidden Services

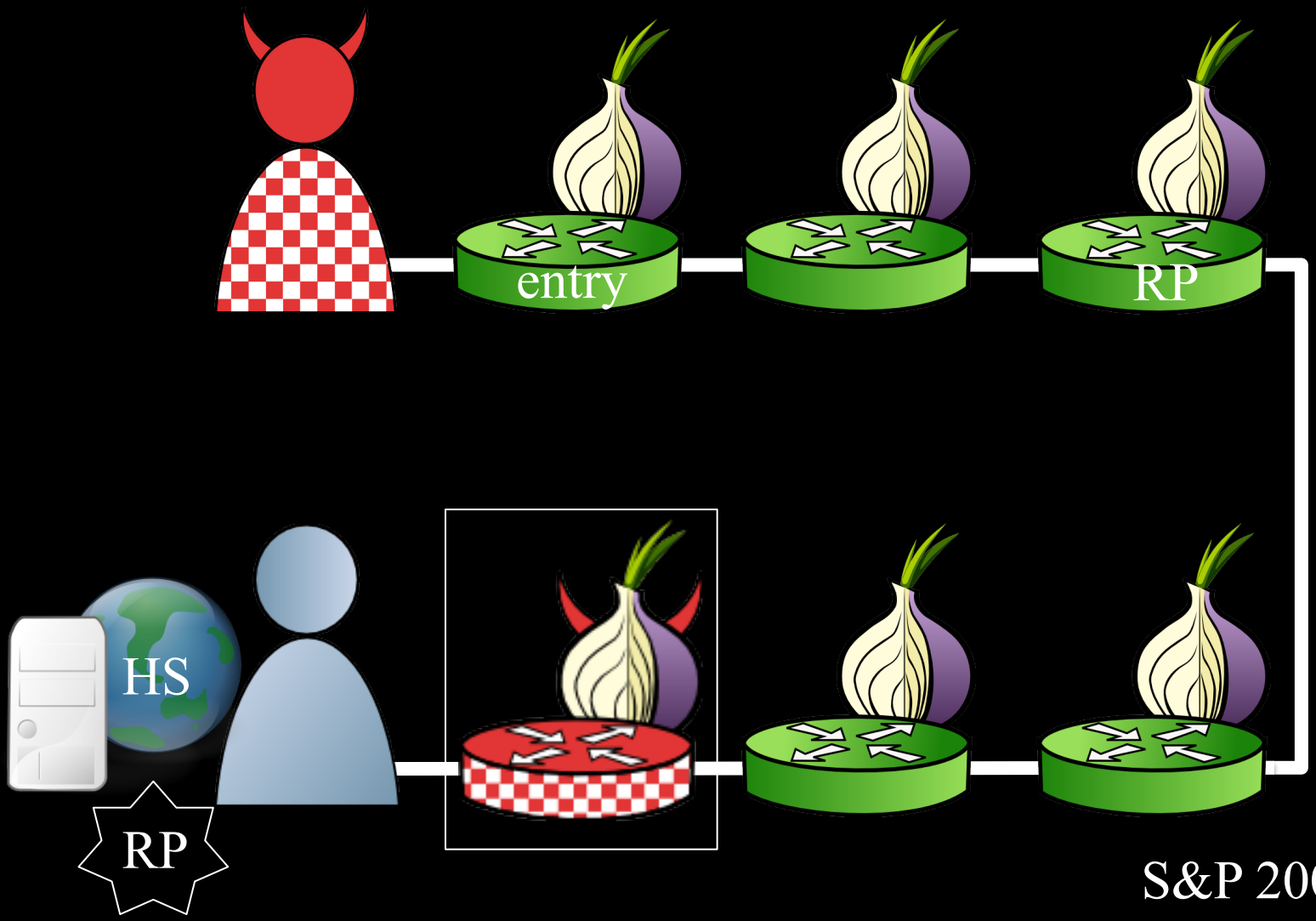




Deanonymizing Hidden Services

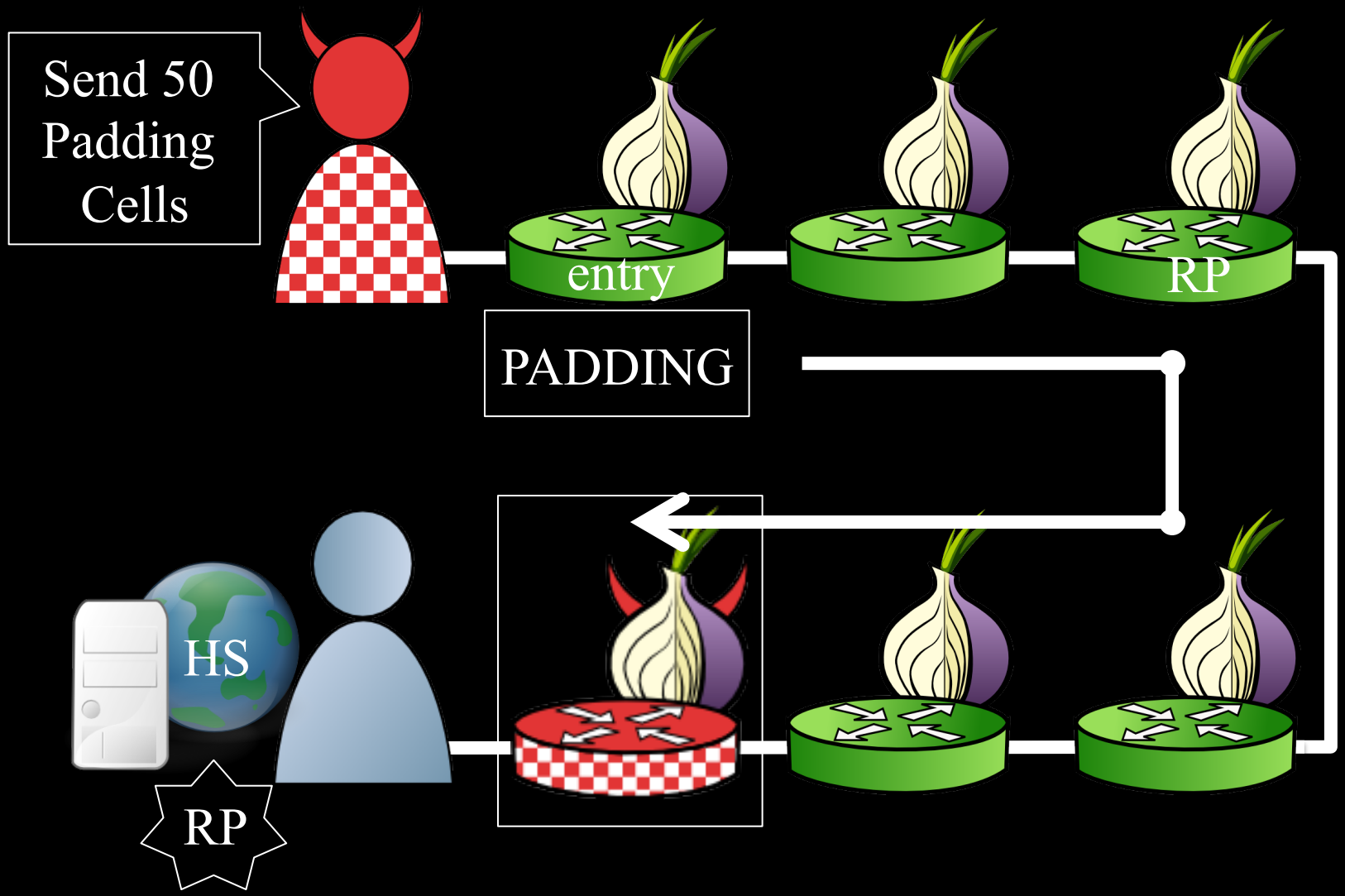


Deanonymizing Hidden Services



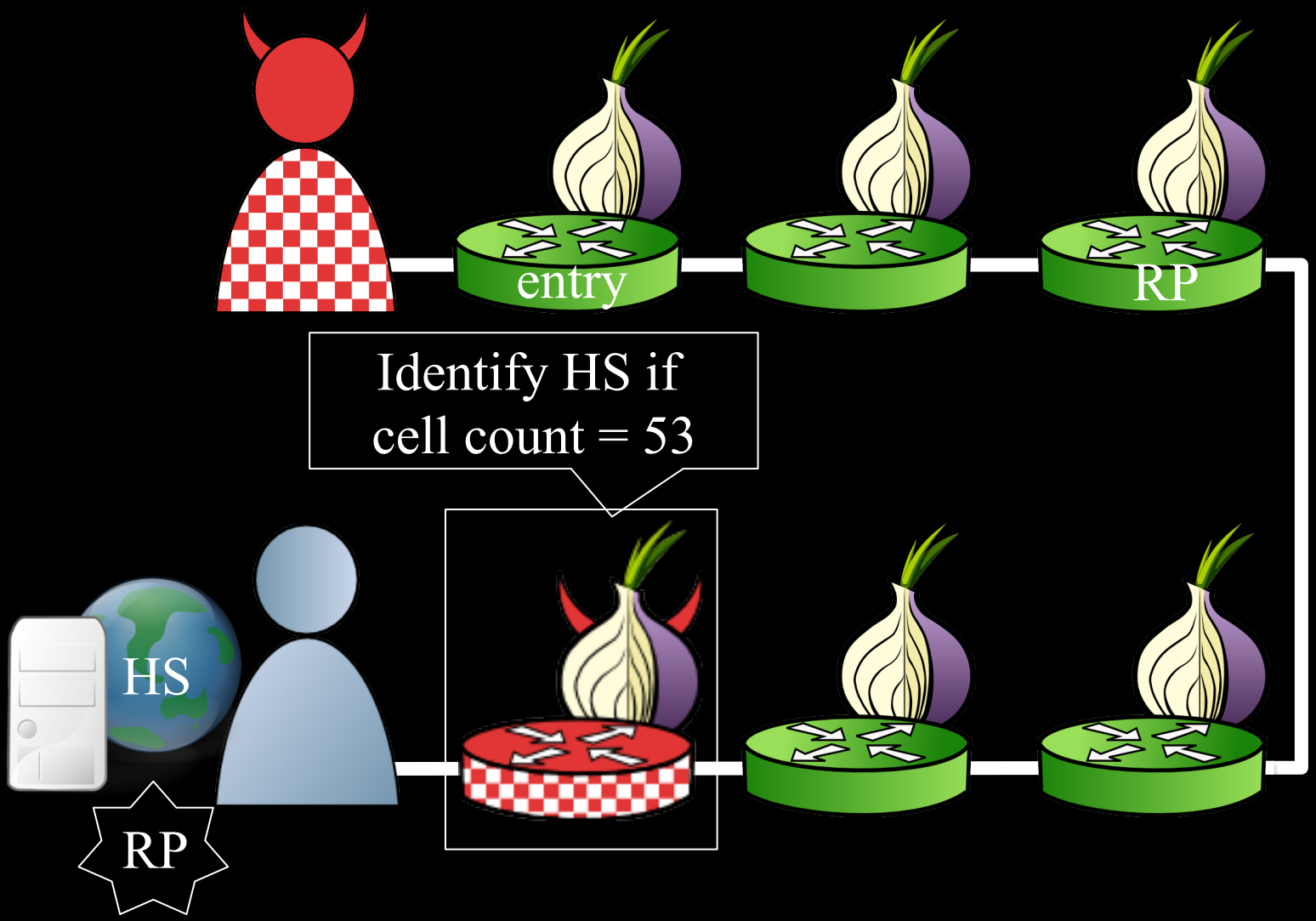
S&P 2006, S&P 2013

Deanonymizing Hidden Services



S&P 2013

Deanonymizing Hidden Services



S&P 2013

Outline

- The Sniper Attack
  - Low-cost memory consumption attack that disables arbitrary Tor relays
- Deanonymizing Hidden Services
  - Using DoS attacks for deanonymization
- Countermeasures

Countermeasures

- Sniper Attack Defenses
  - Authenticated SENDMEs
  - Queue Length Limit
  - Adaptive Circuit Killer
- Deanonymization Defenses
  - Entry-guard Rate-limiting
  - Middle Guards

Questions?

cs.umn.edu/~jansen
rob.g.jansen@nrl.navy.mil

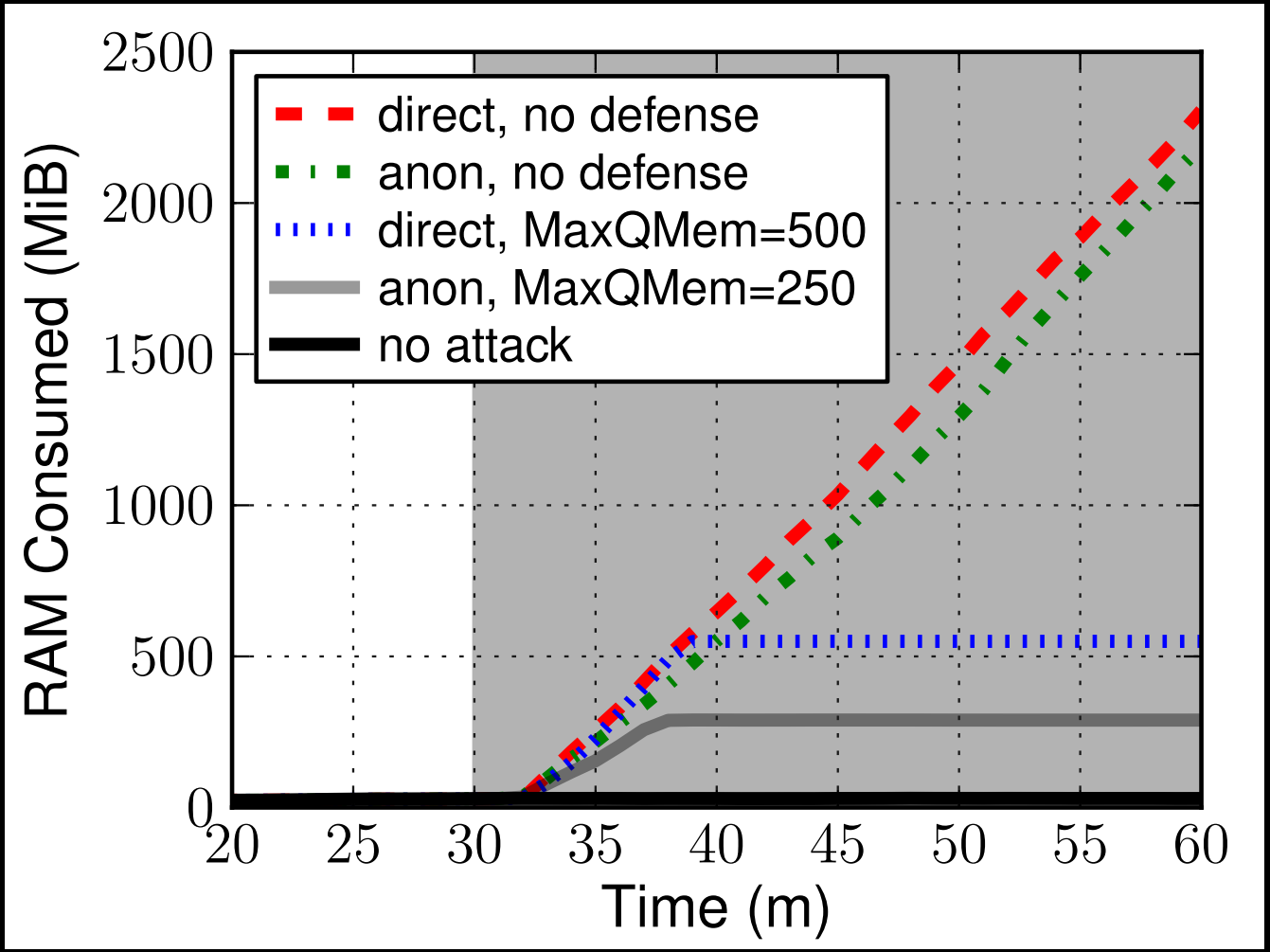
think like an adversary

Speed of Deanonymization

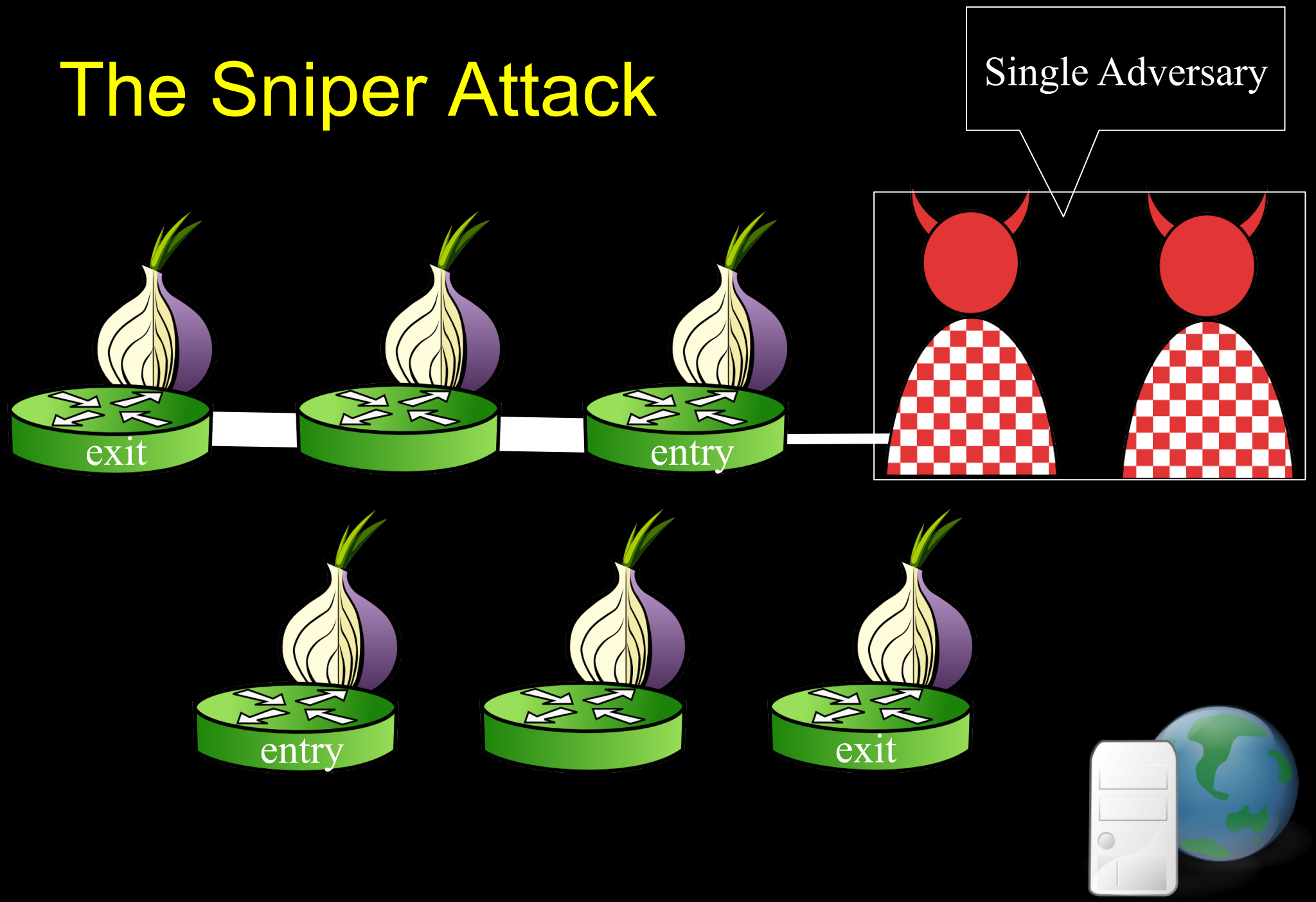
Guard BW (MiB/s)	Guard Probability (%)	Average # Rounds	Average # Sniped	Average Time (h) 1 GiB	Average Time (h) 8 GiB
8.41	0.48	66	133	46	279
16.65	0.97	39	79	23	149
31.65	1.9	24	48	13	84
66.04	3.8	13	26	6	44
96.61	5.4	9	19	5	31

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

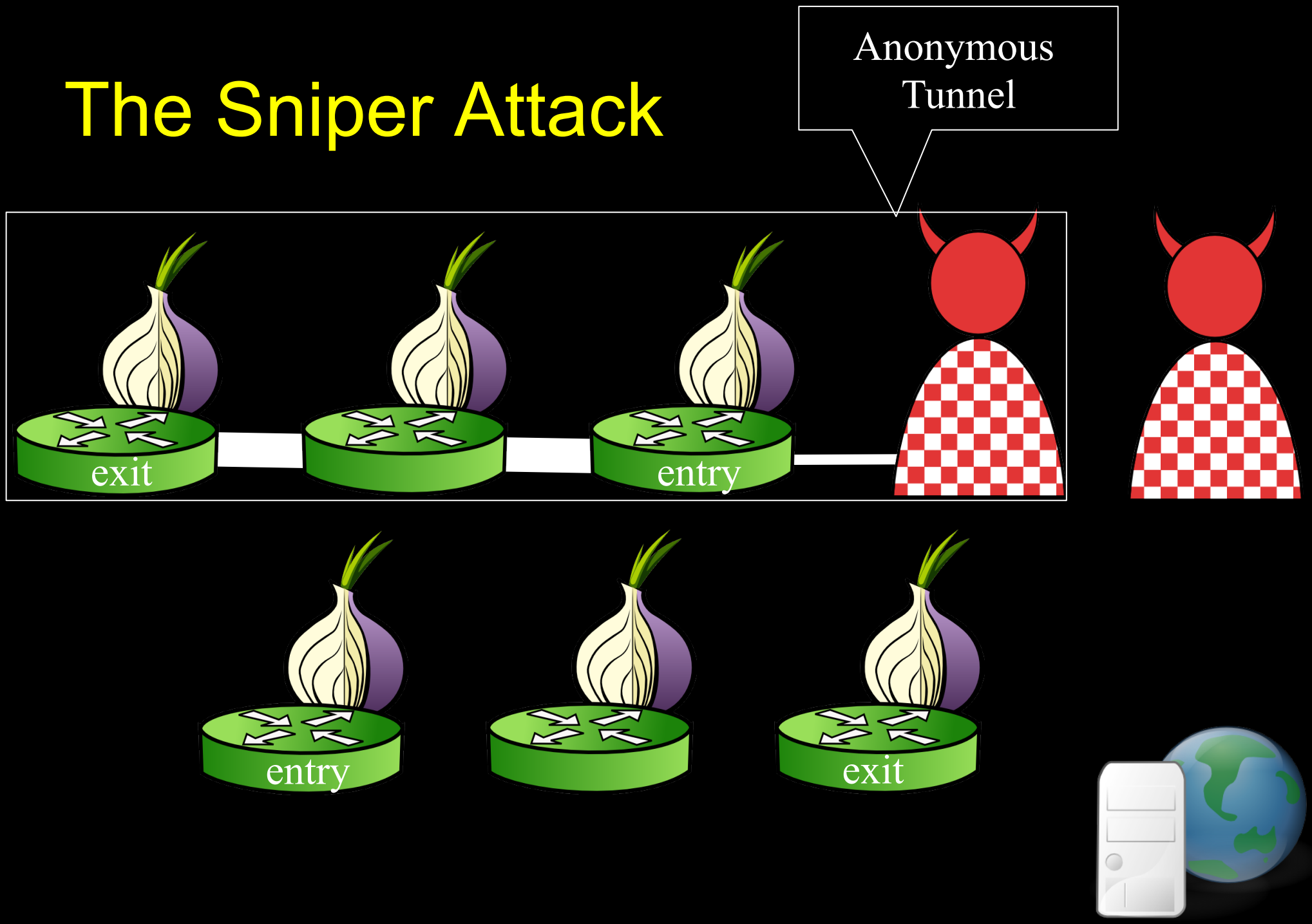
Circuit Killer Defense



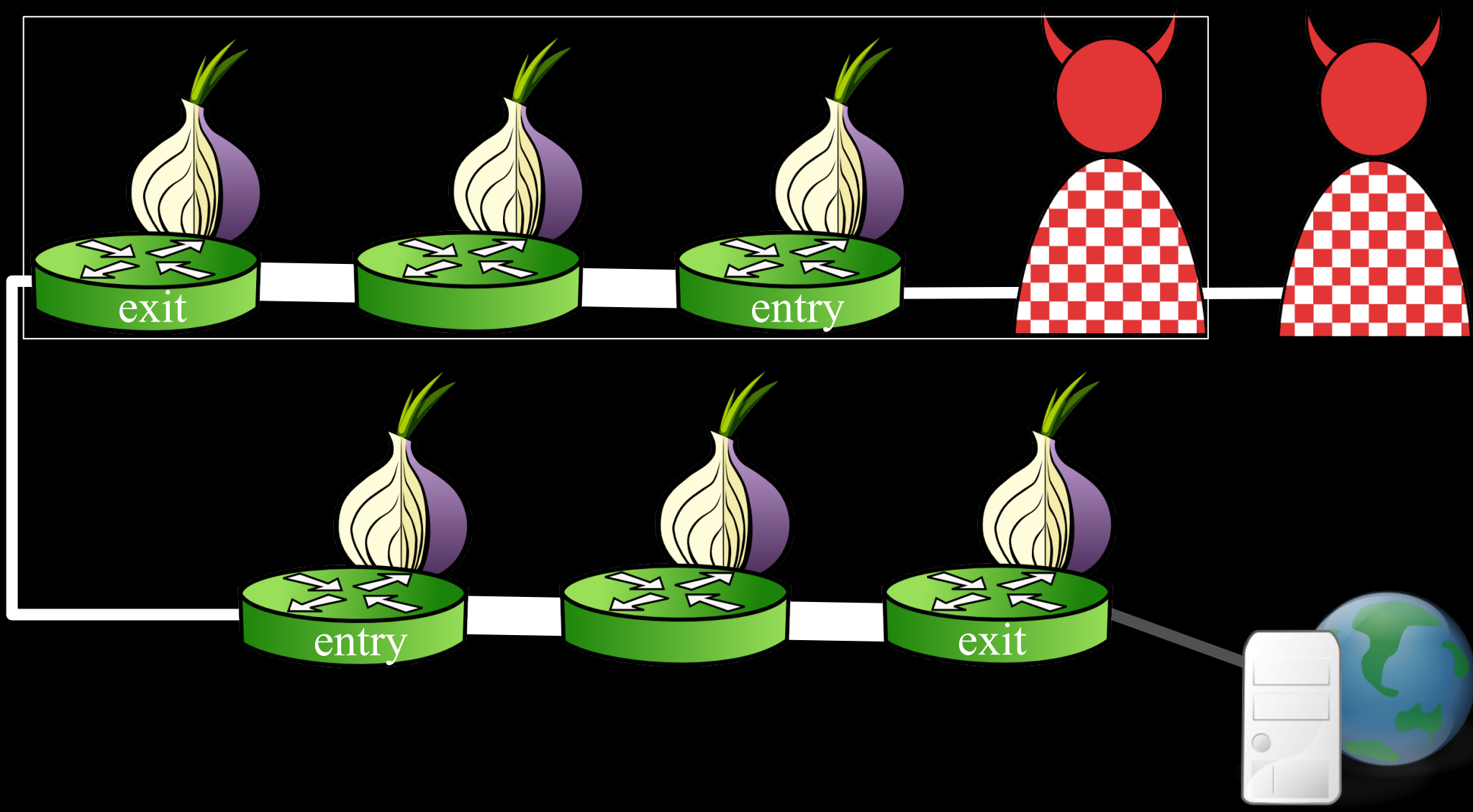
The Sniper Attack



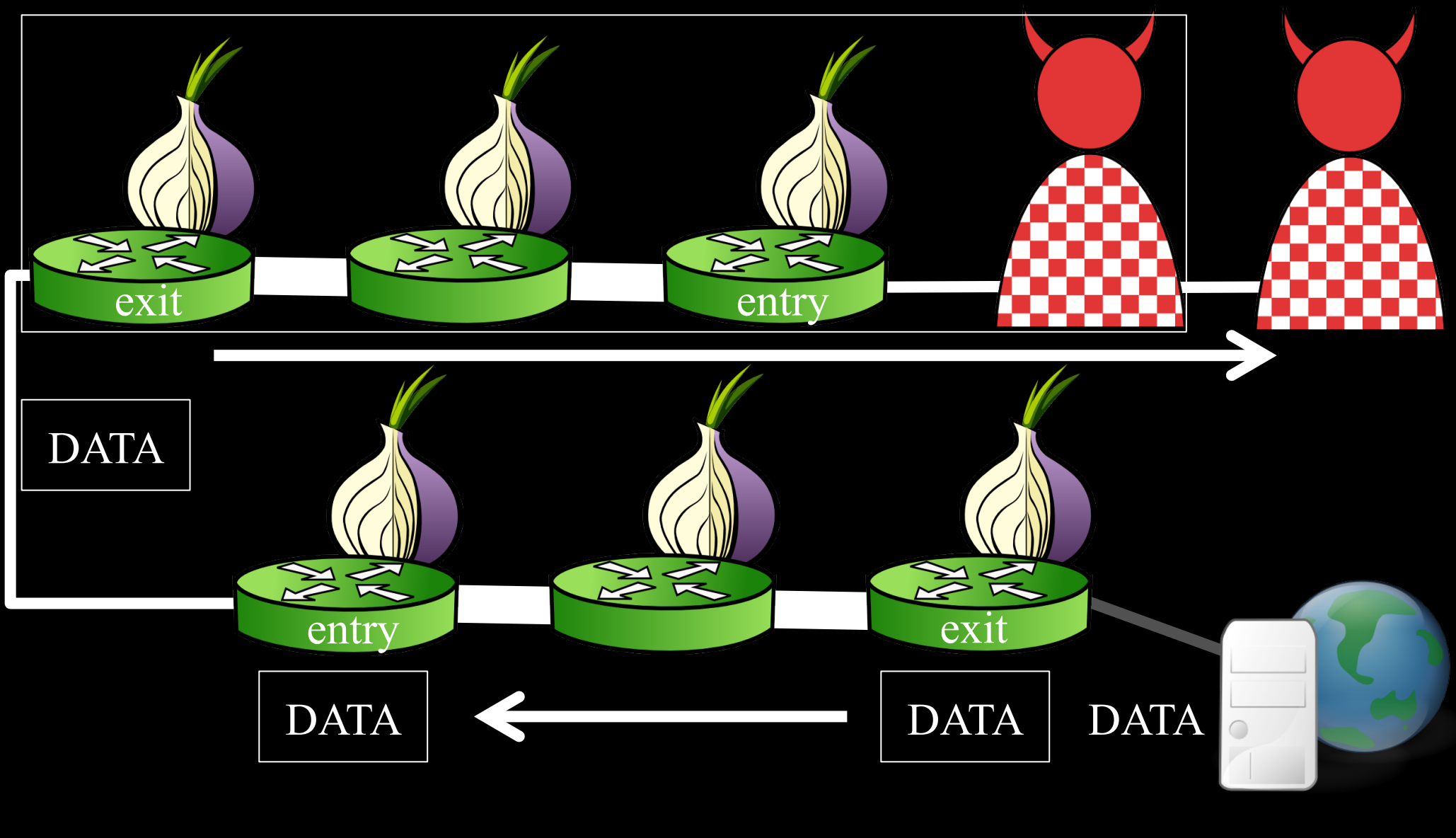
The Sniper Attack



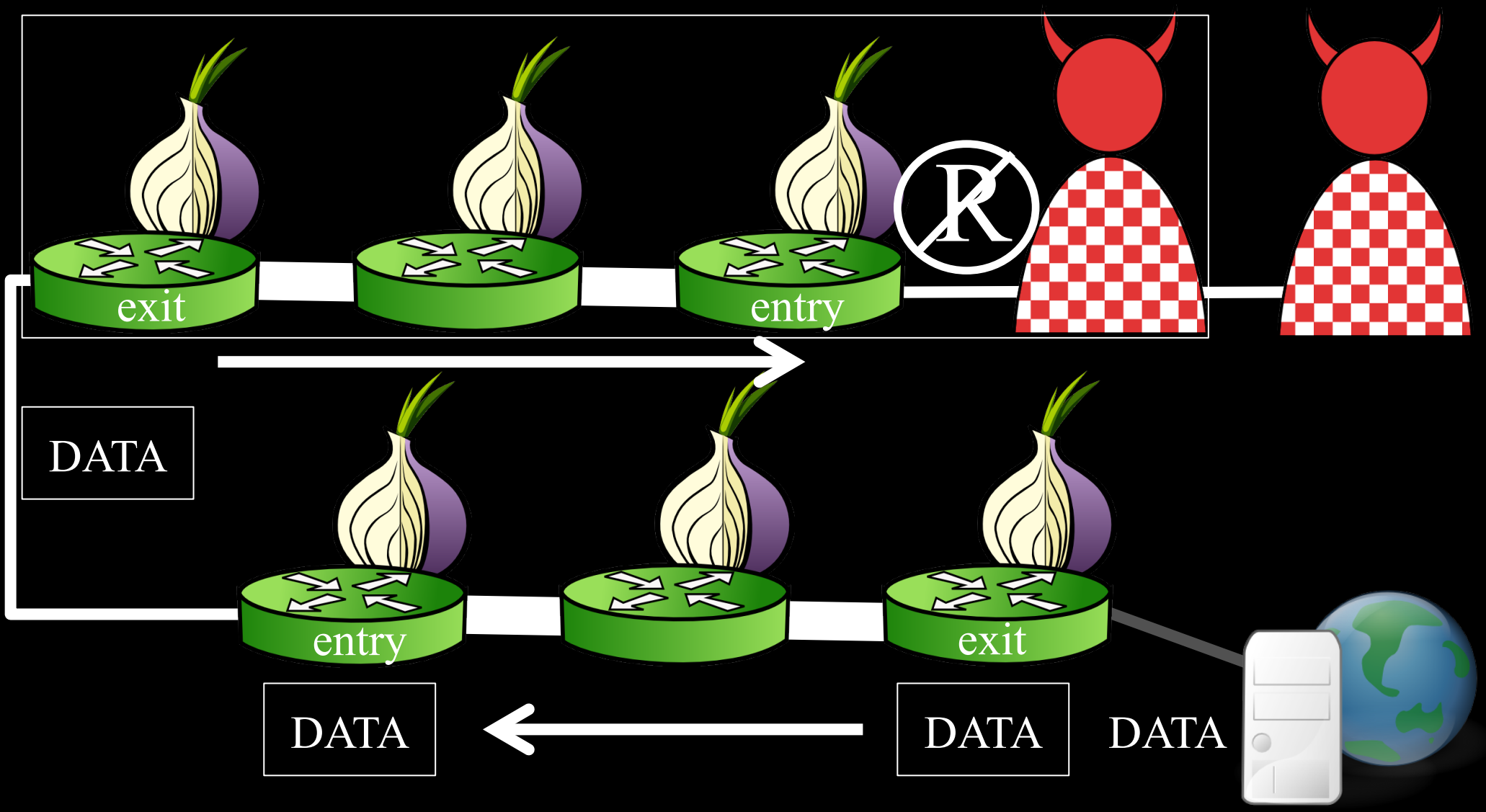
The Sniper Attack



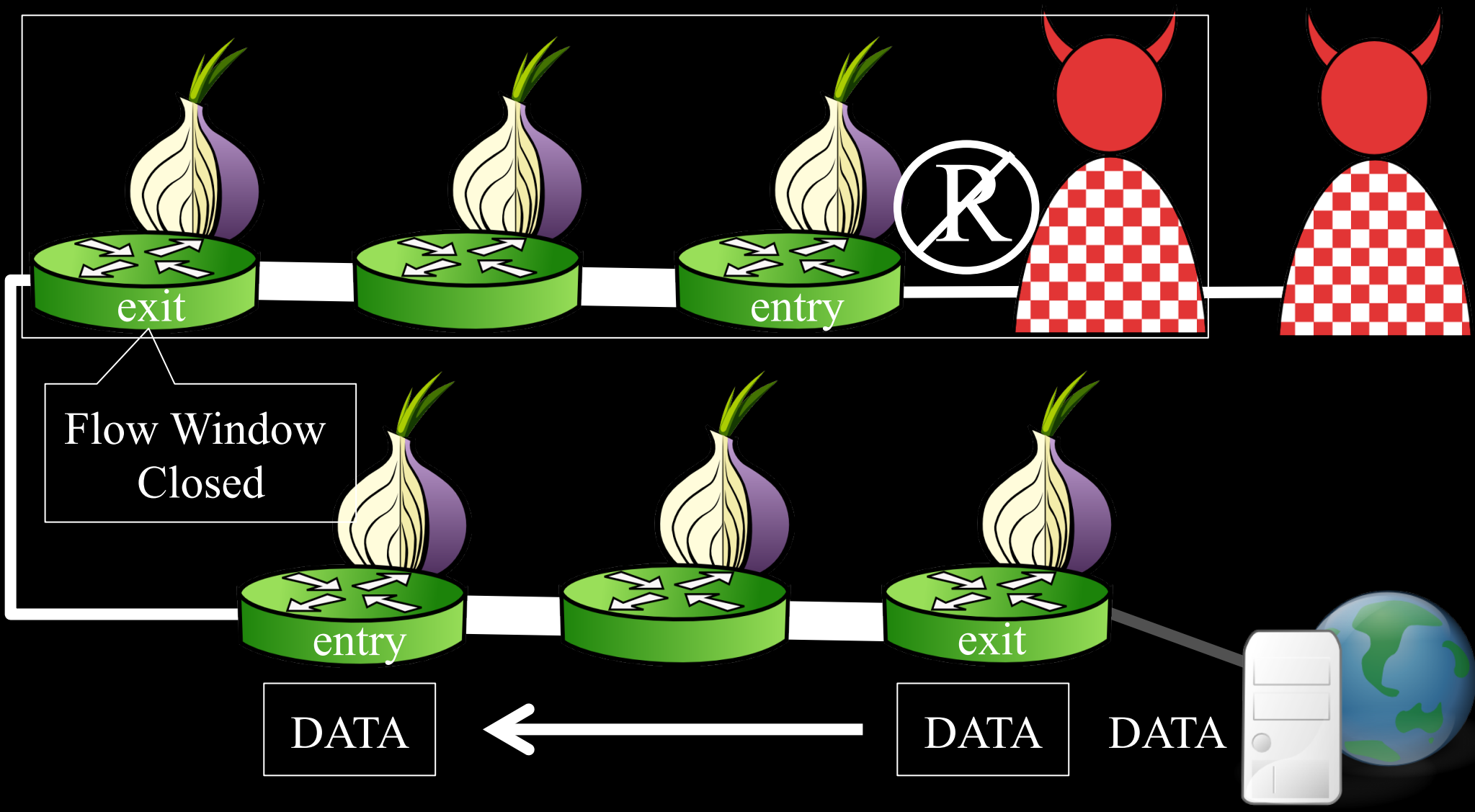
The Sniper Attack



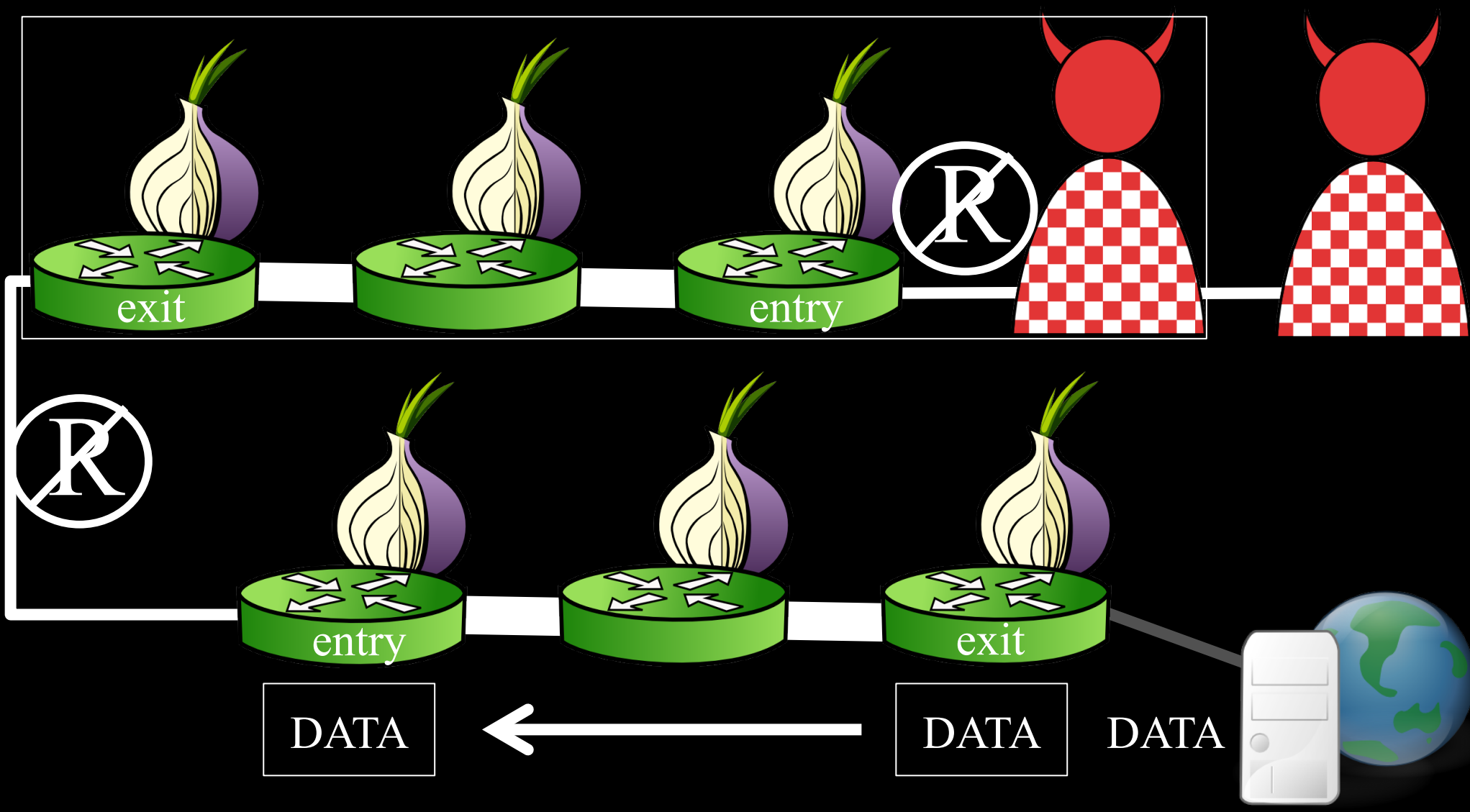
The Sniper Attack



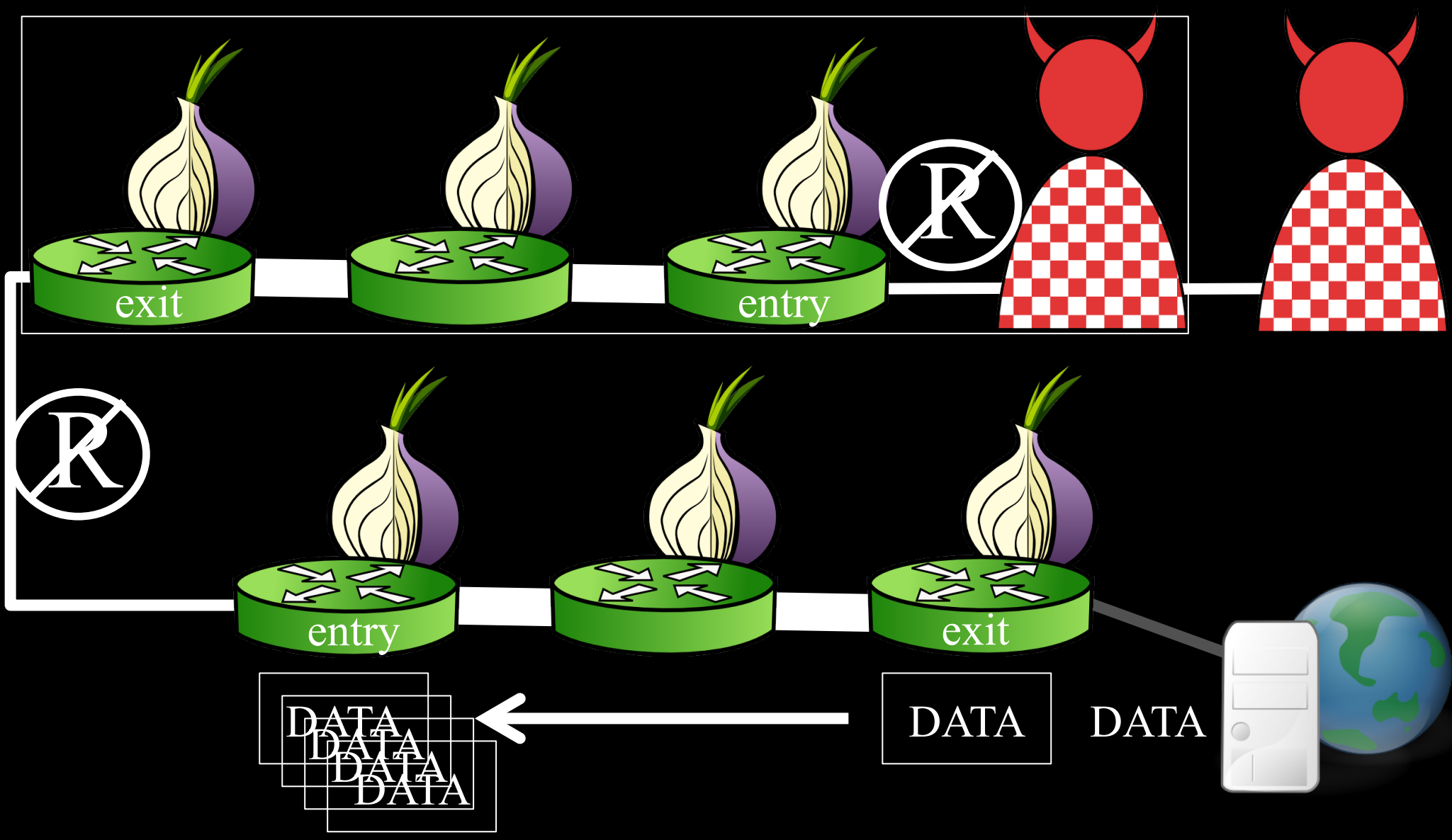
The Sniper Attack



The Sniper Attack



The Sniper Attack



The Sniper Attack