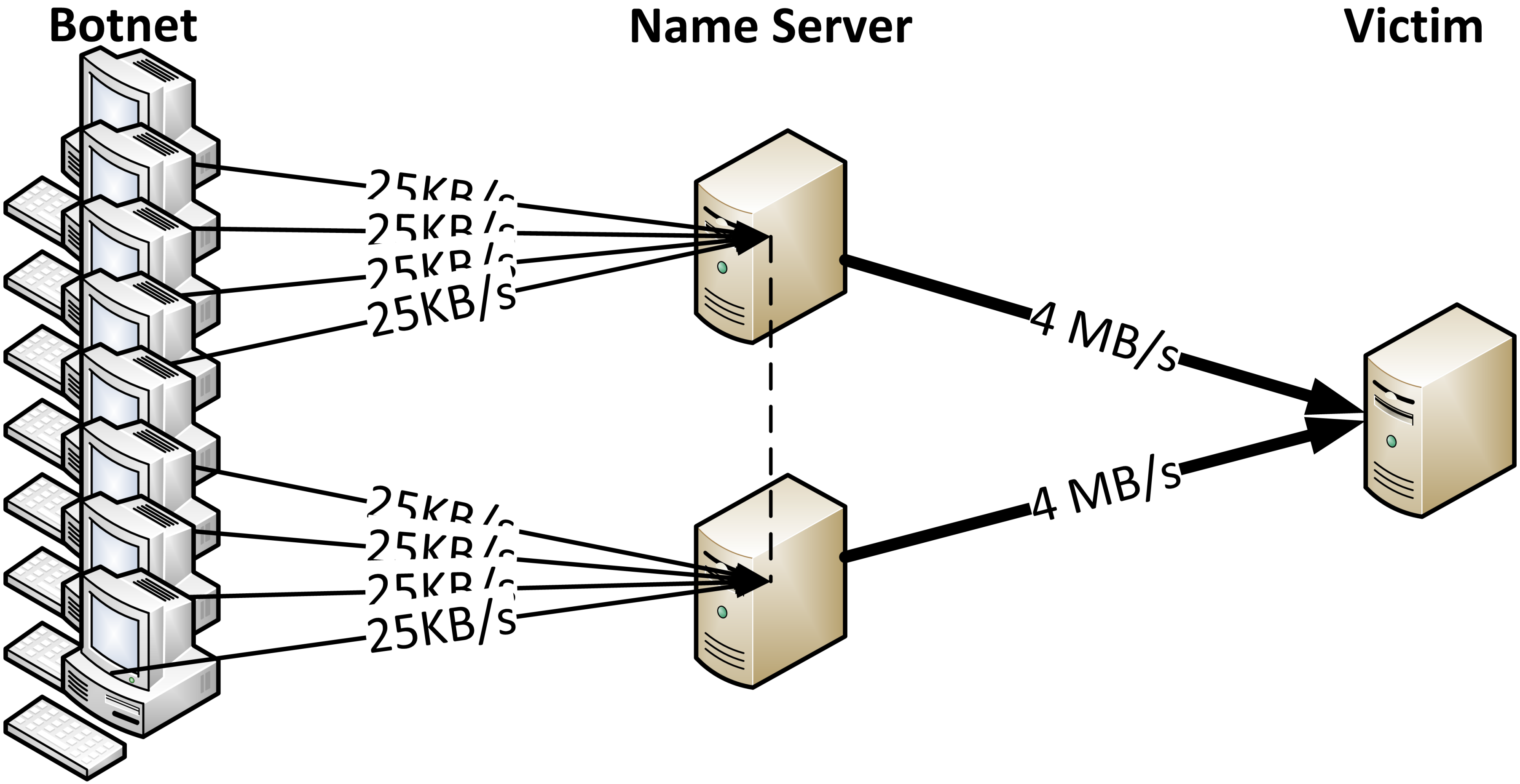
Authors:
Thijs Rozekrans
<thijs.rozekrans@os3.nl>
Javy de Koning
<javydekoning@gmail.com>

Defending against DNS reflection amplification attacks

What is a DNS reflection amplification attack?



Spamhaus…

```
Javy$ dig ANY ripe.net @8.8.4.4
+dnssec | grep SIZE
;; MSG SIZE  rcvd: 2509
```

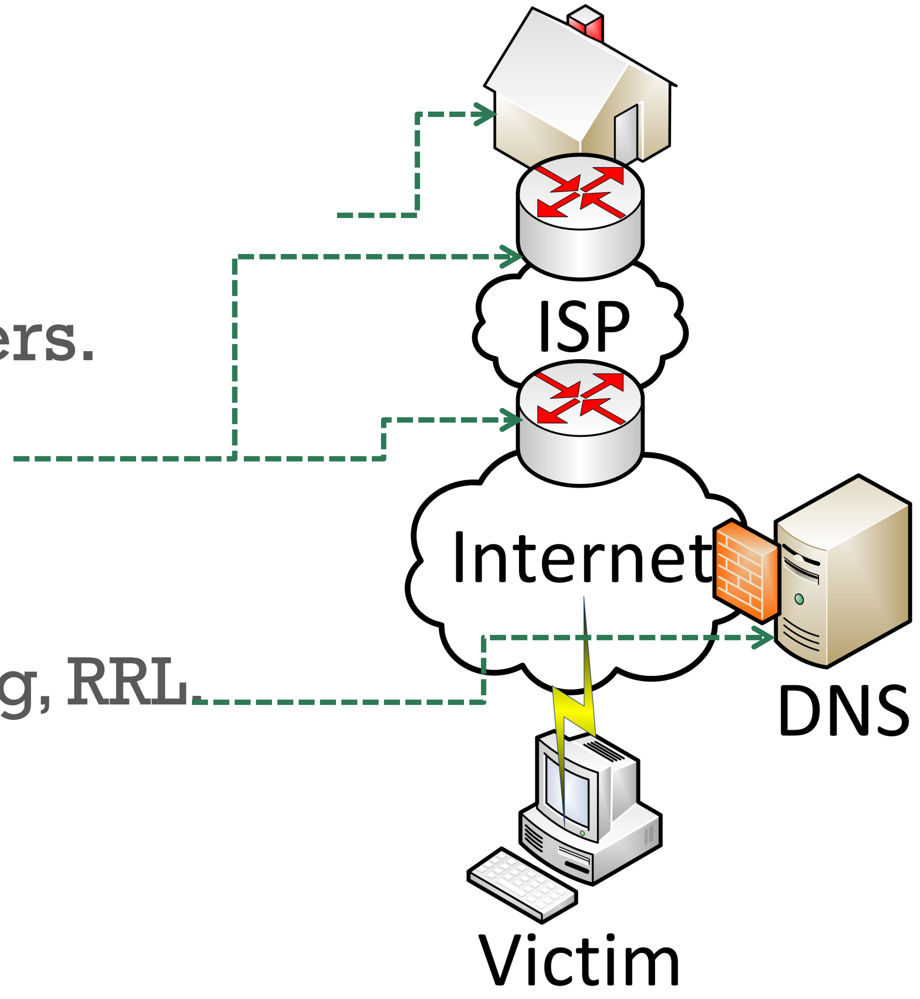
```
Javy$ tcpdump -i en1 udp port 53 and
dst 8.8.4.4
…
ANY? ripe.net. (37)
```

Research Question

*”What **measures** can be taken to defend against **DNS amplification attacks** on **authoritative name servers**, and what is the **effectiveness** of **Response Rate Limiting**?”*

Which defense mechanisms are available? Where to defend?

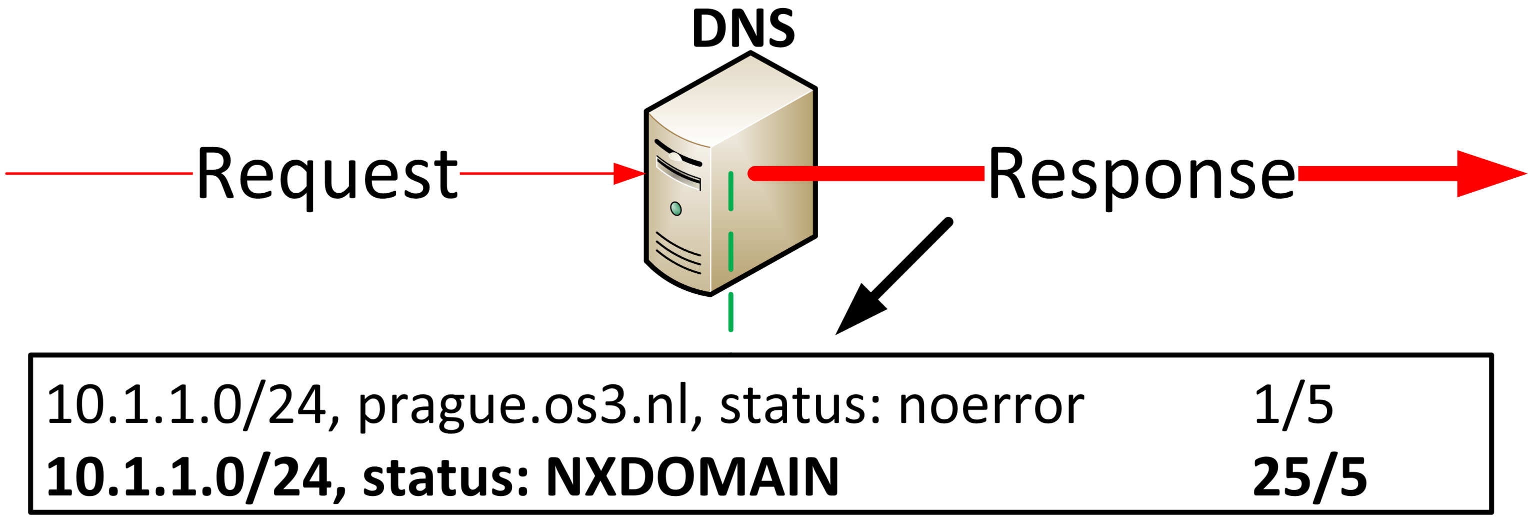
- (Botnet) PC.
  - Patches, Antivirus etc.
- Internet Service Providers.
  - BCP38: Ingress filtering.
- DNS.
  - Firewall, TCP, Dampening, RRL.



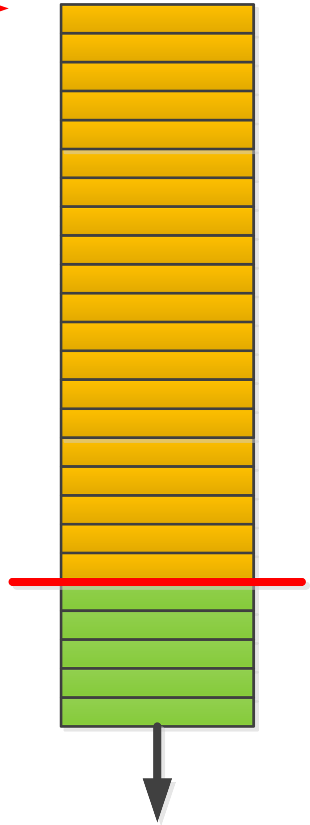
Why focus on RRL?

- The only technique that is used in large numbers;
- Implementations for BIND, NSD and Knot;
- Research proposed by NLnet Labs;

RRL Explained



10.1.1.0/24, prague.os3.nl, status: noerror	1/5
10.1.1.0/24, status: NXDOMAIN	**25/5**

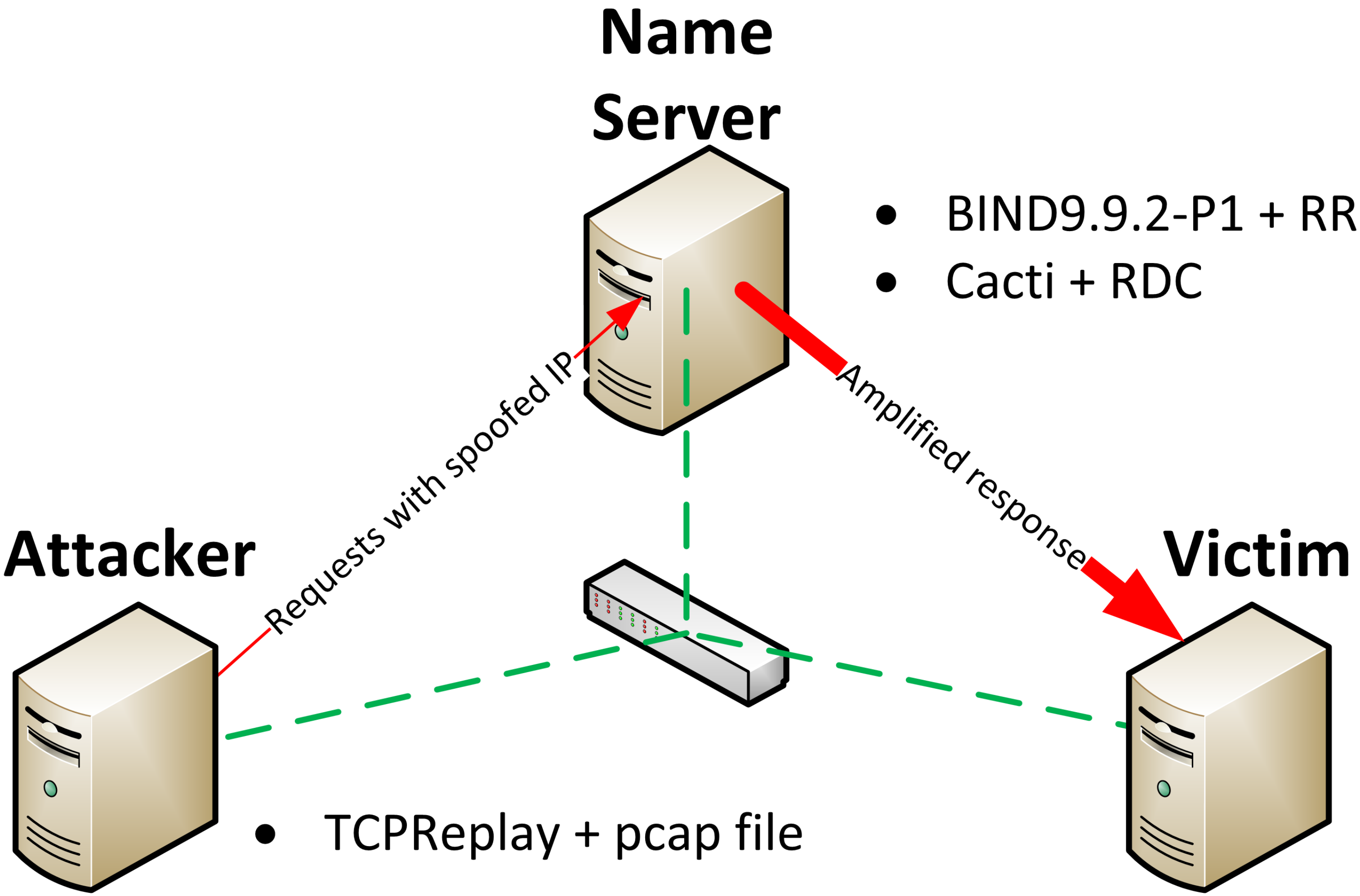


- MAX Responses per second = 5
- Window size = 5 sec

How is the effectiveness of RRL measured?

- 5 Different attacks
  - Repeating query (ANY)
  - Varying query (25%, 50%, 75%, 100%)
- Inbound vs outbound traffic (Amplification Ratio)
- Slip settings

Lab setup.

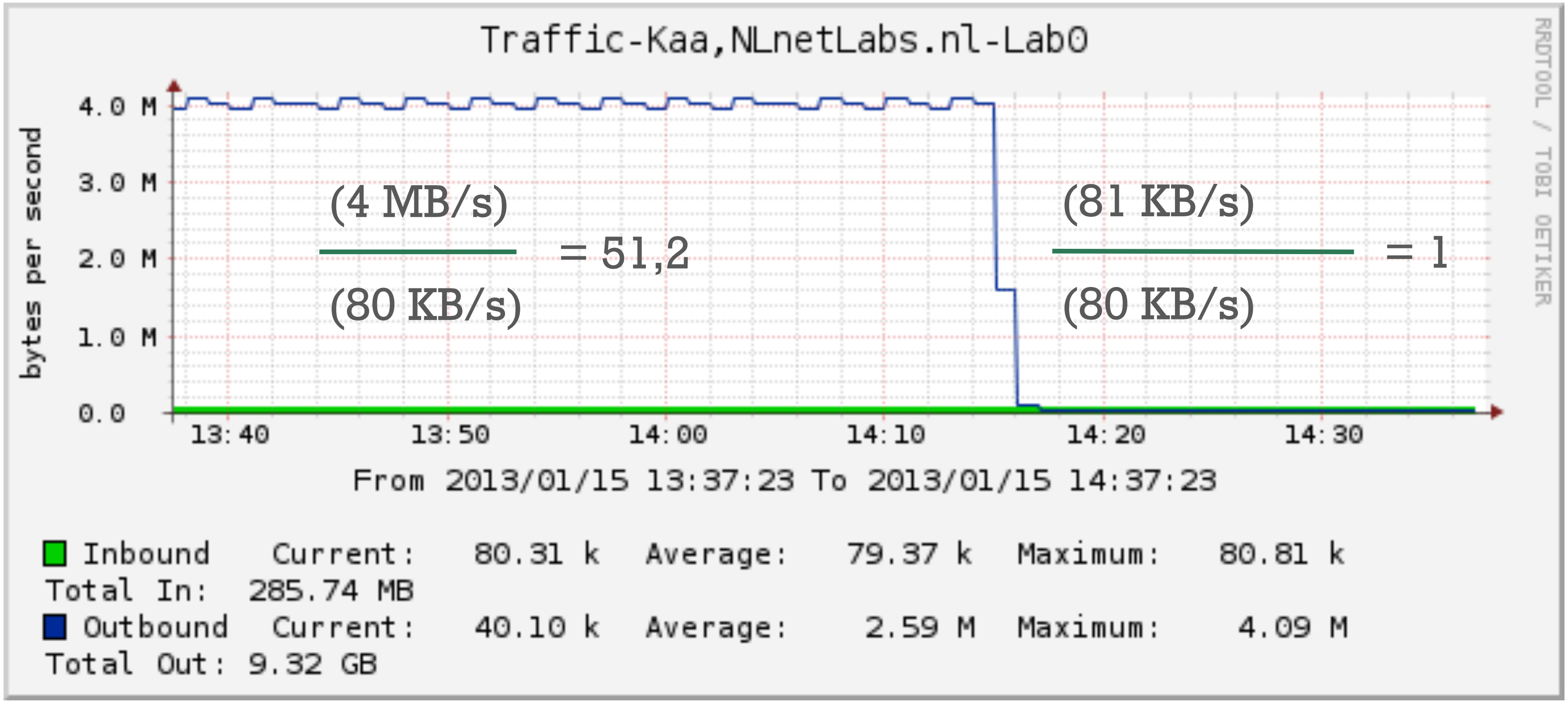


- BIND9.9.2-P1 + RRL
- Cacti + RDC

- TCPReplay + pcap file

+ RRL Measurements

Measurements 1/7 – Repeating ANY attack



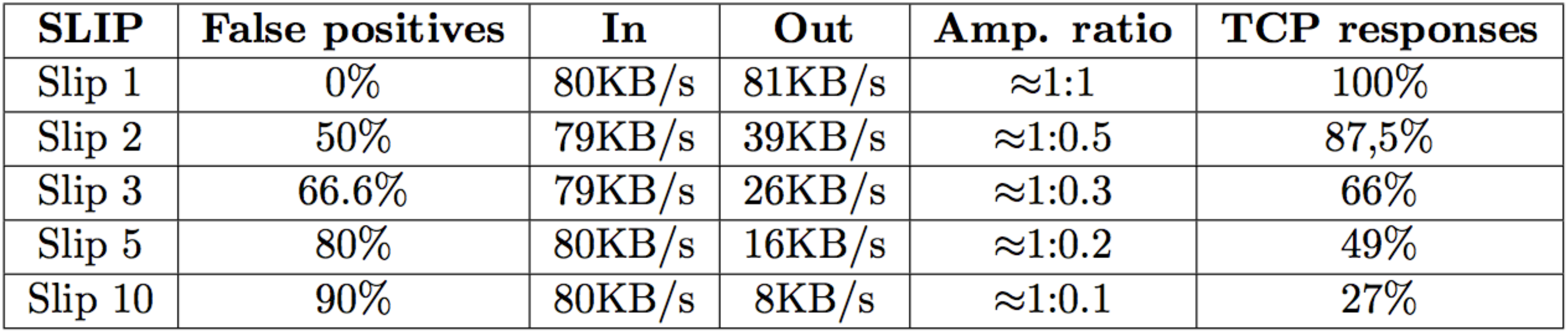
From 2013/01/15 13:37:23 To 2013/01/15 14:37:23

$$\frac{(4\ MB/s)}{(80\ KB/s)} = 51{,}2$$

$$\frac{(81\ KB/s)}{(80\ KB/s)} = 1$$

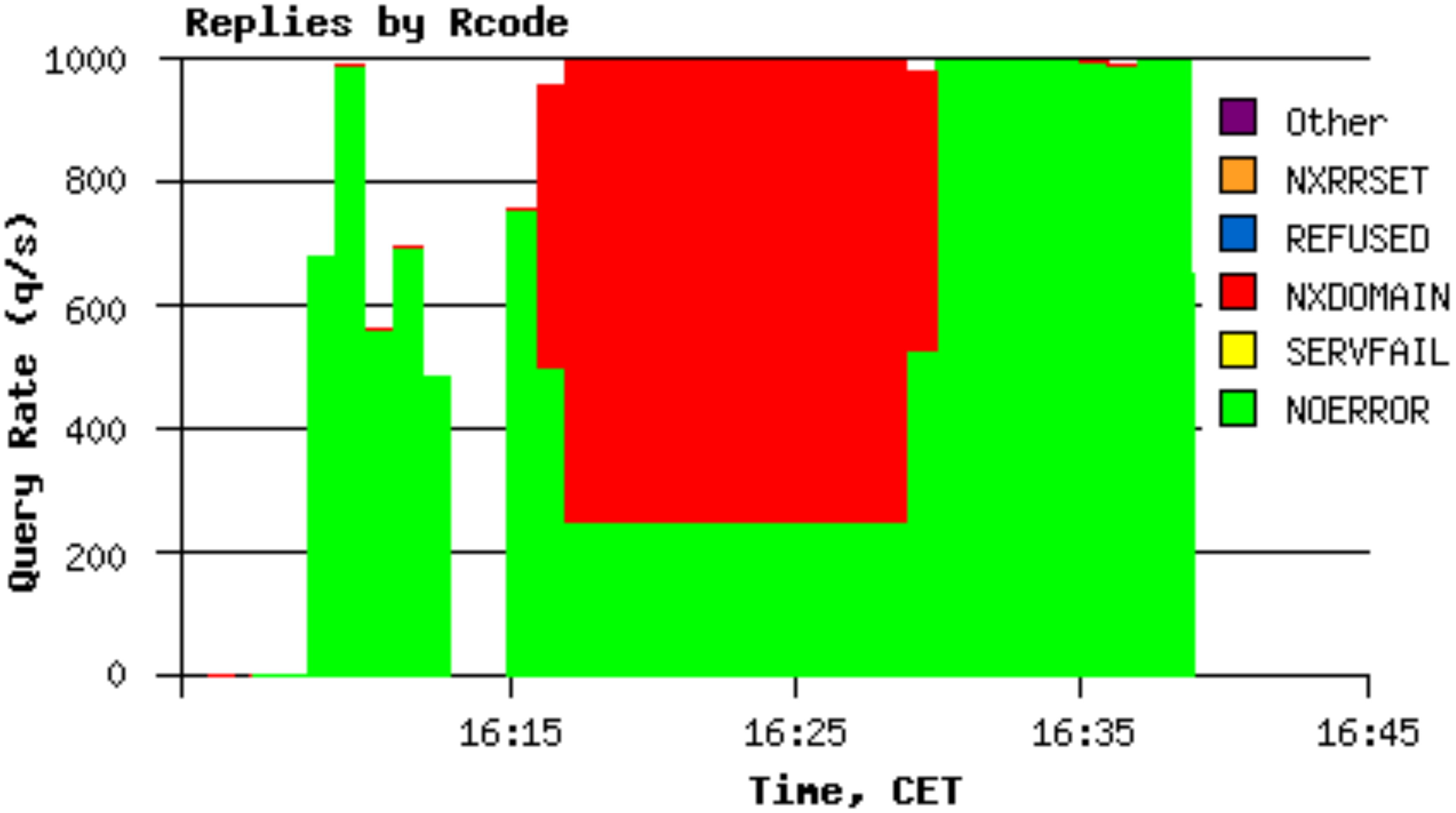
```
🟩 Inbound    Current:    80.31 k   Average:    79.37 k   Maximum:    80.81 k
Total In:   285.74 MB
🟦 Outbound   Current:    40.10 k   Average:     2.59 M   Maximum:     4.09 M
Total Out:  9.32 GB
```

+ Measurements 2/7 – Repeating ANY attack

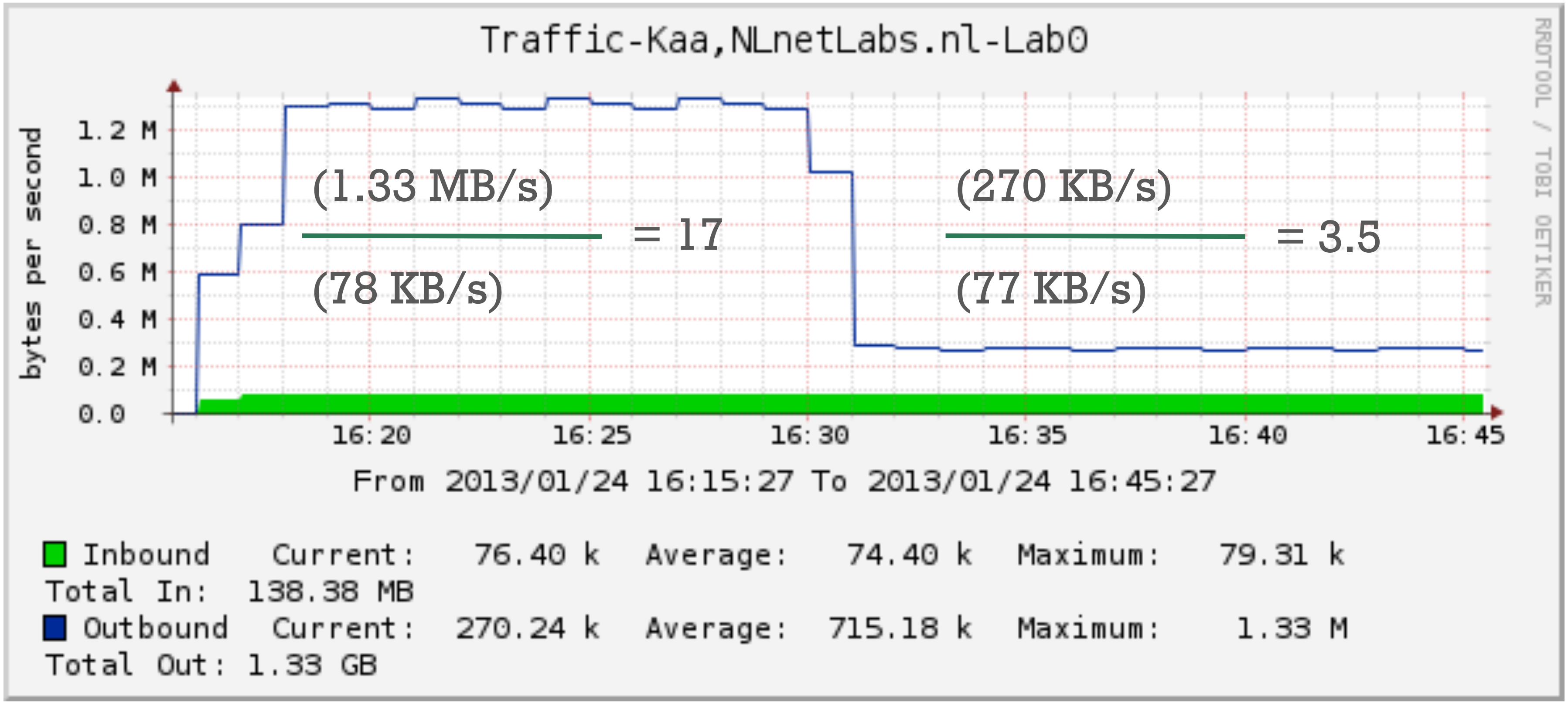


SLIP	False positives	In	Out	Amp. ratio	TCP responses
Slip 1	0%	80KB/s	81KB/s	≈1:1	100%
Slip 2	50%	79KB/s	39KB/s	≈1:0.5	87,5%
Slip 3	66.6%	79KB/s	26KB/s	≈1:0.3	66%
Slip 5	80%	80KB/s	16KB/s	≈1:0.2	49%
Slip 10	90%	80KB/s	8KB/s	≈1:0.1	27%

Measurements 3/7 – Varying query attack (25%)



Measurements 4/7 – Varying query attack (25%)



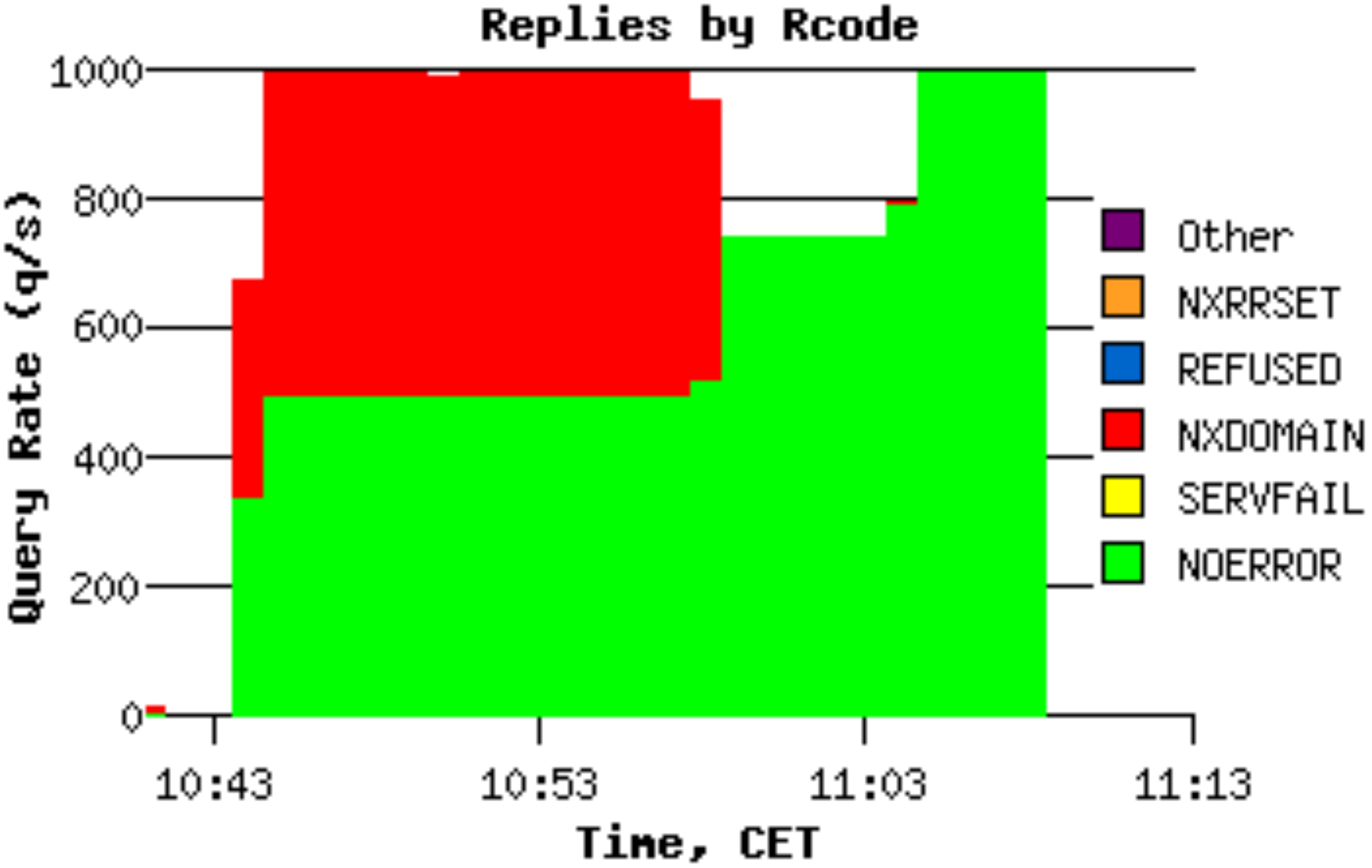
$$\frac{(1.33\ \text{MB/s})}{(78\ \text{KB/s})} = 17$$

$$\frac{(270\ \text{KB/s})}{(77\ \text{KB/s})} = 3.5$$

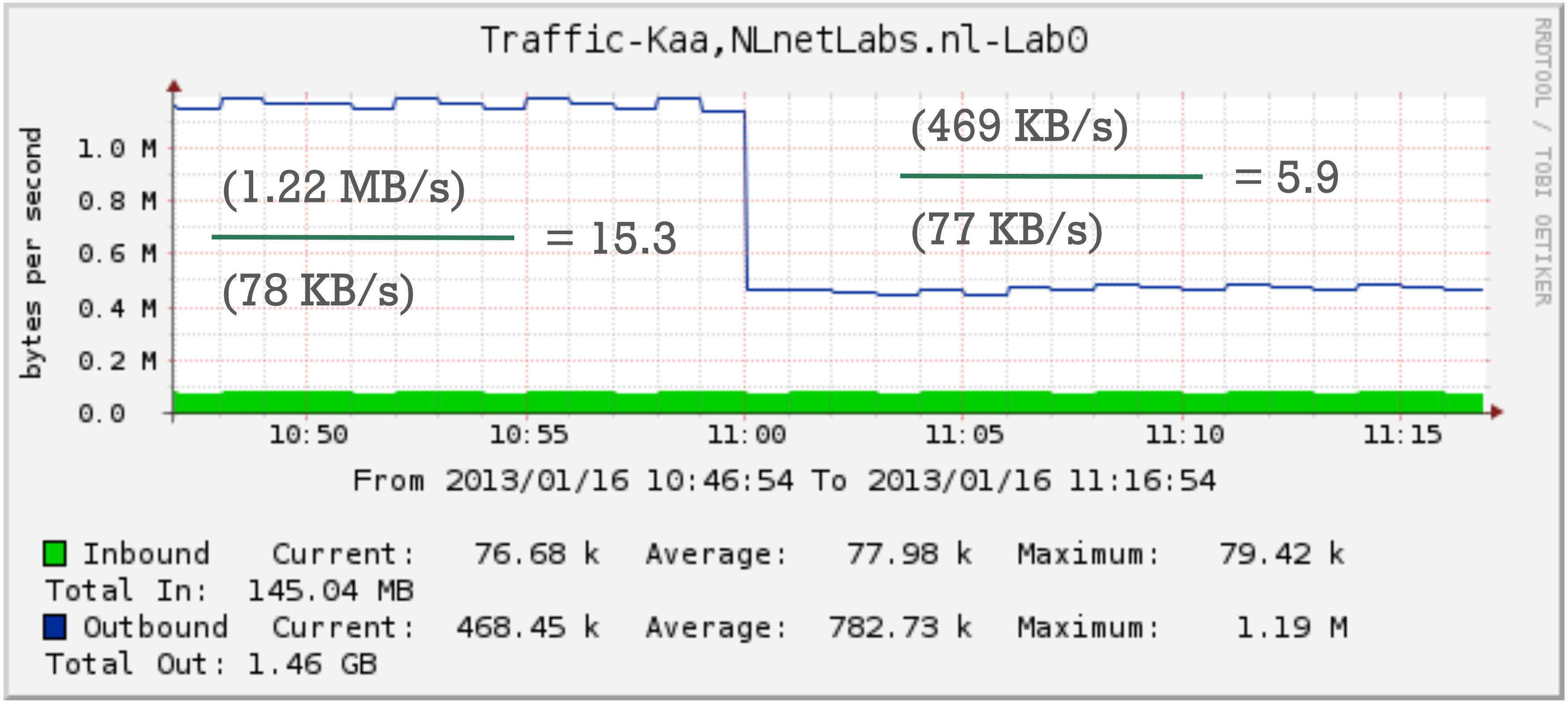
From 2013/01/24 16:15:27 To 2013/01/24 16:45:27

```
🟩 Inbound    Current:    76.40 k   Average:    74.40 k   Maximum:    79.31 k
Total In:  138.38 MB
🟦 Outbound   Current:   270.24 k   Average:   715.18 k   Maximum:     1.33 M
Total Out: 1.33 GB
```

Measurements 5/7 – Varying query attack (50%)



Measurements 6/7 – Varying query attack (50%)

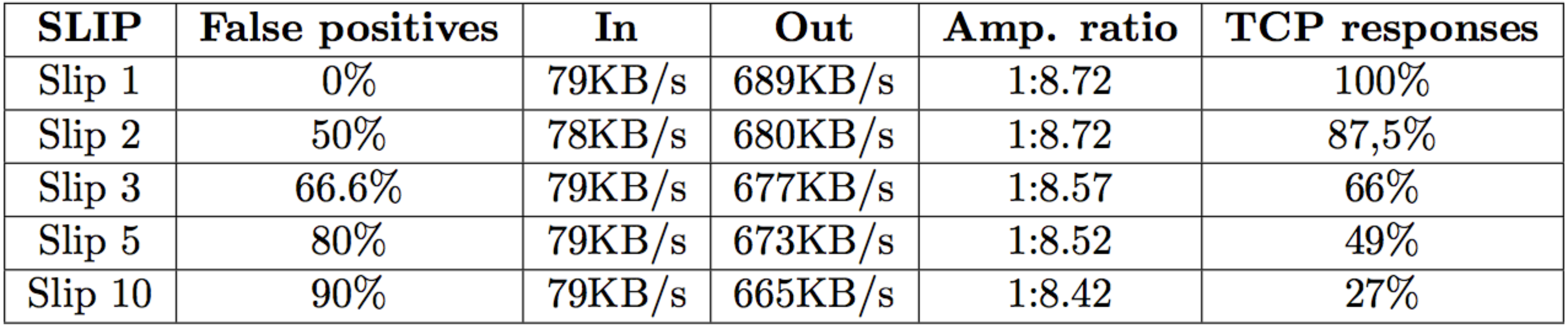


$$\frac{(1.22\ MB/s)}{(78\ KB/s)} = 15.3$$

$$\frac{(469\ KB/s)}{(77\ KB/s)} = 5.9$$

```
🟩 Inbound   Current:   76.68 k   Average:   77.98 k   Maximum:   79.42 k
Total In:  145.04 MB
🟦 Outbound  Current:  468.45 k   Average:  782.73 k   Maximum:    1.19 M
Total Out: 1.46 GB
```

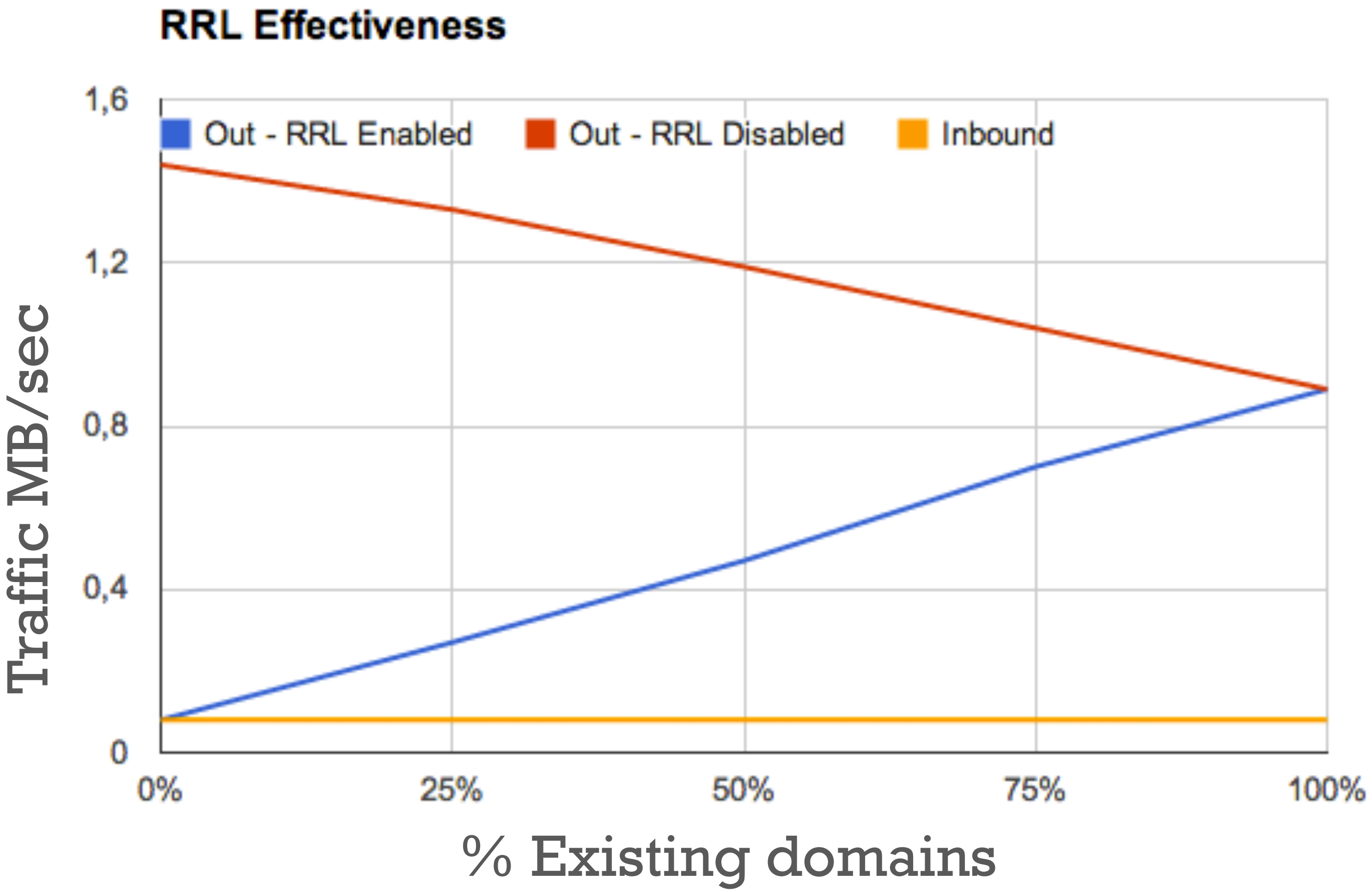
+ Measurements 7/7 – Varying query attack (75%)



SLIP	False positives	In	Out	Amp. ratio	TCP responses
Slip 1	0%	79KB/s	689KB/s	1:8.72	100%
Slip 2	50%	78KB/s	680KB/s	1:8.72	87,5%
Slip 3	66.6%	79KB/s	677KB/s	1:8.57	66%
Slip 5	80%	79KB/s	673KB/s	1:8.52	49%
Slip 10	90%	79KB/s	665KB/s	1:8.42	27%

+

Results


RRL Effectiveness
1,6
1,2
0,8
0,4
0
🟦 Out - RRL Enabled
🟥 Out - RRL Disabled
🟧 Inbound
0%
25%
50%
75%
100%
Traffic MB/sec
% Existing domains

DNS Dampening

- Penalty points for every request
- Successful against distributed attacks
- Needs tailoring
- No mechanism to counter false positives
- To aggressive

+ Conclusion

- RRL effective vs attacks generating the same response
- RRL ineffective vs distributed attacks
- Other approaches needed for future attacks
- Need to push BCP38

- What's next?!

Q&A