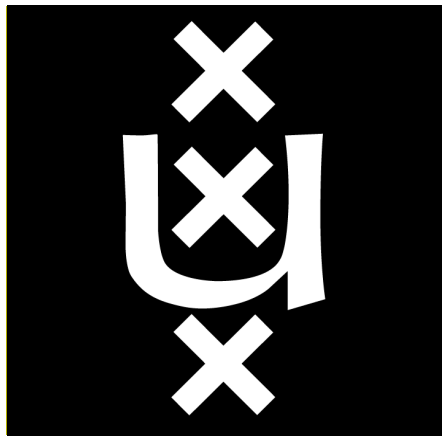
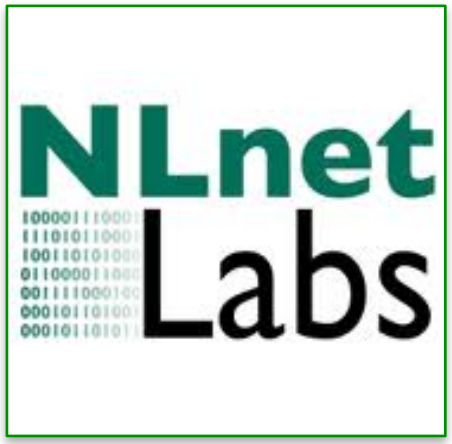
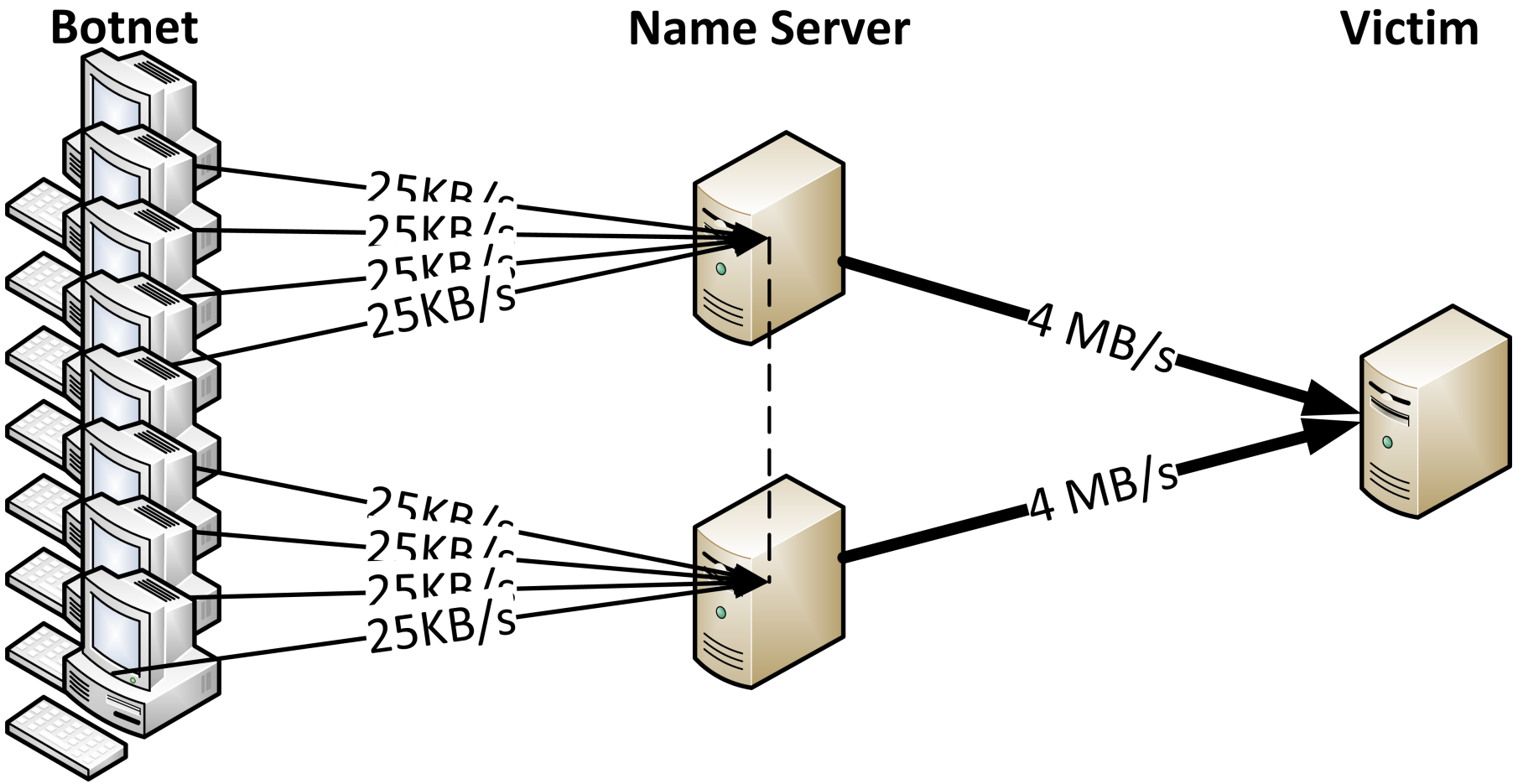
Authors:
Thijs Rozekrans
Javy de Koning





Defending against DNS reflection amplification attacks

What is a DNS reflection amplification attack?

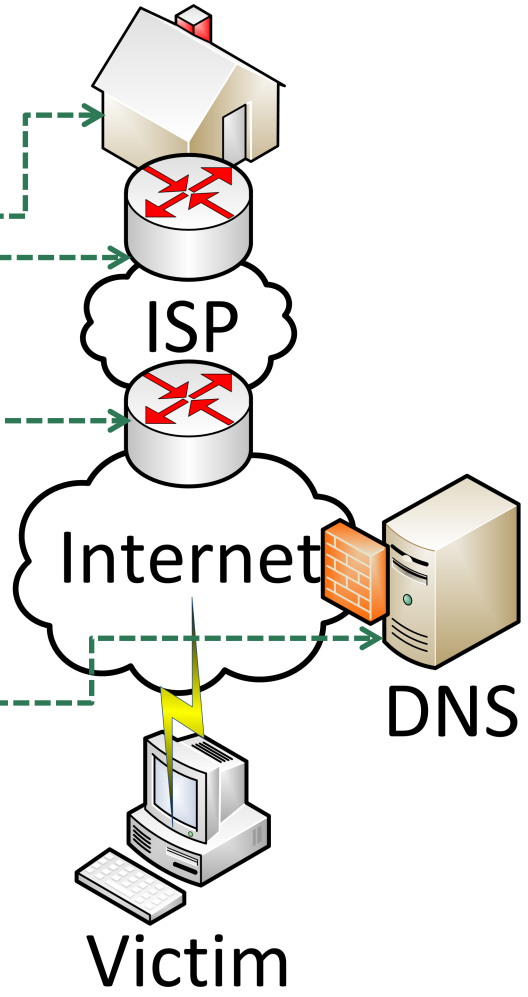


Research Question

”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 controlled PC.
  - Patches, Antivirus, Antispyware etc.
- ISP.
  - BCP38: Ingress filtering.
- DNS.
  - Firewall, TCP, Dampening, RRL.



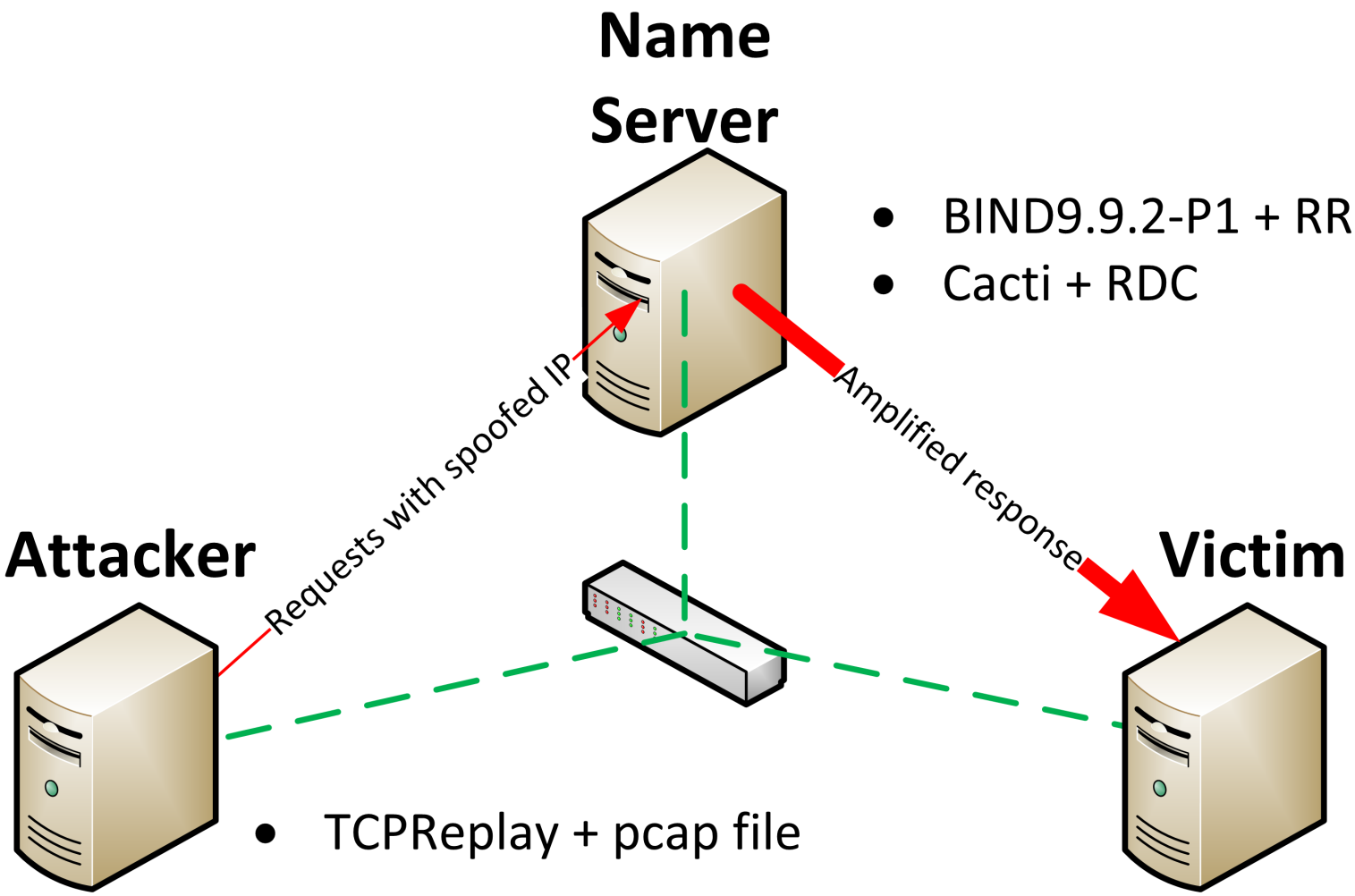
Why focus on RRL?

- Most promising;
- The only technique that is actively used and supported;
- Available for BIND and NSD;
- Research proposed by NLnet Labs.

How is the effectiveness of RRL measured?

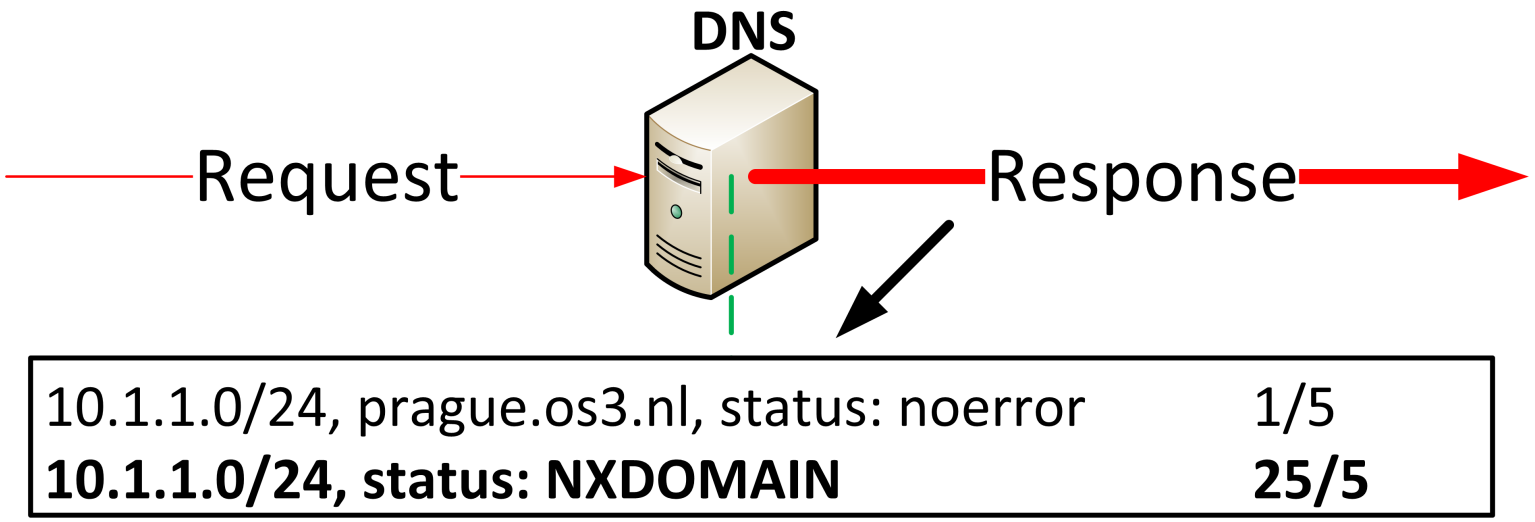
- 5 Different attacks
  - Repeating query (ANY)
  - Varying query (25%, 50%, 75%, 100%)
- Inbound vs outbound traffic (Amplification Ratio)
- Slip settings

Lab setup.


Name Server
BIND9.9.2-P1 + RRL
Cacti + RDC
Requests with spoofed IP
Amplified response
Attacker
Victim
TCPReplay + pcap file

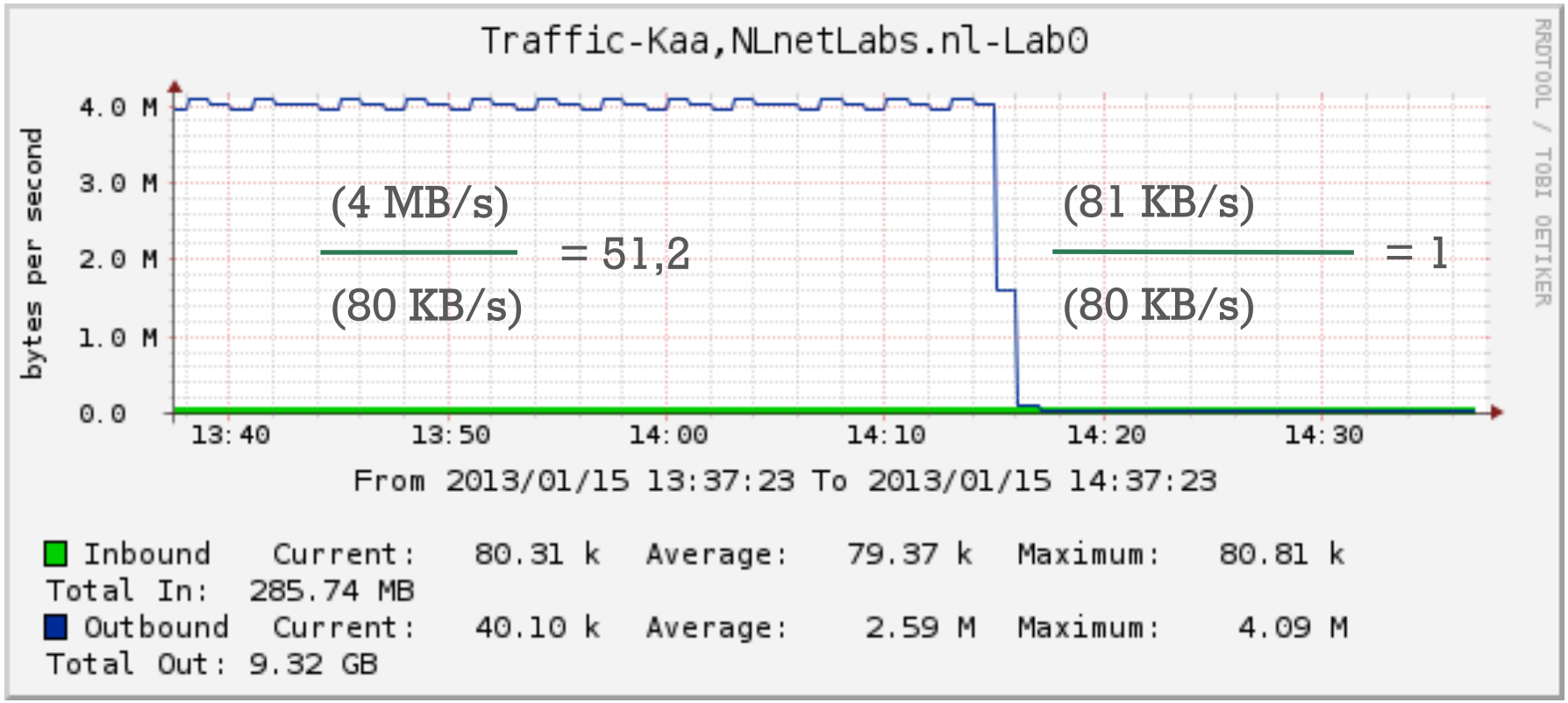
RRL Measurements

RRL Explained



- MAX Responses per second = 5
- Window size = 5
- Maximum bucket = 25
- Minimum bucket = 0

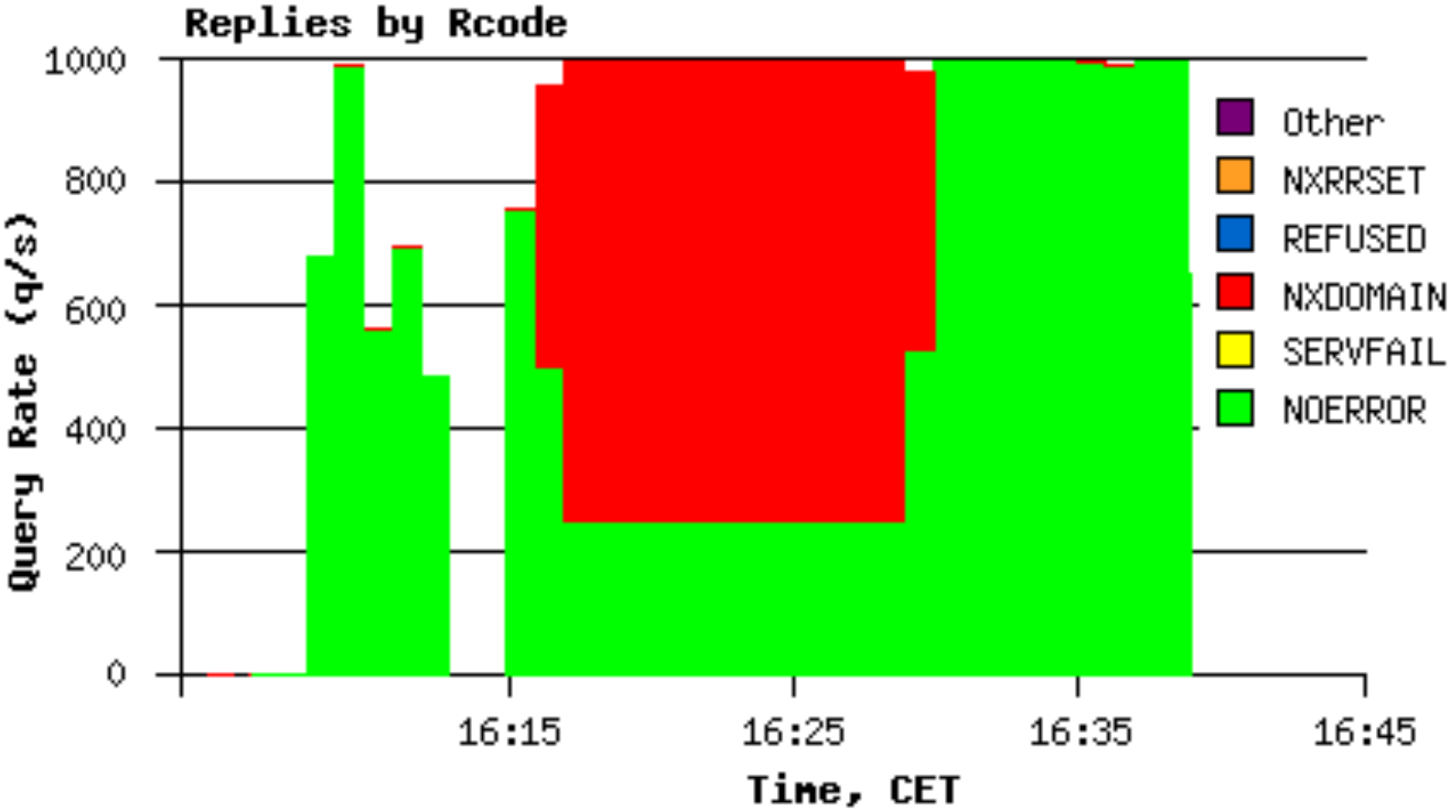
Measurements 1/5 – Repeating ANY attack



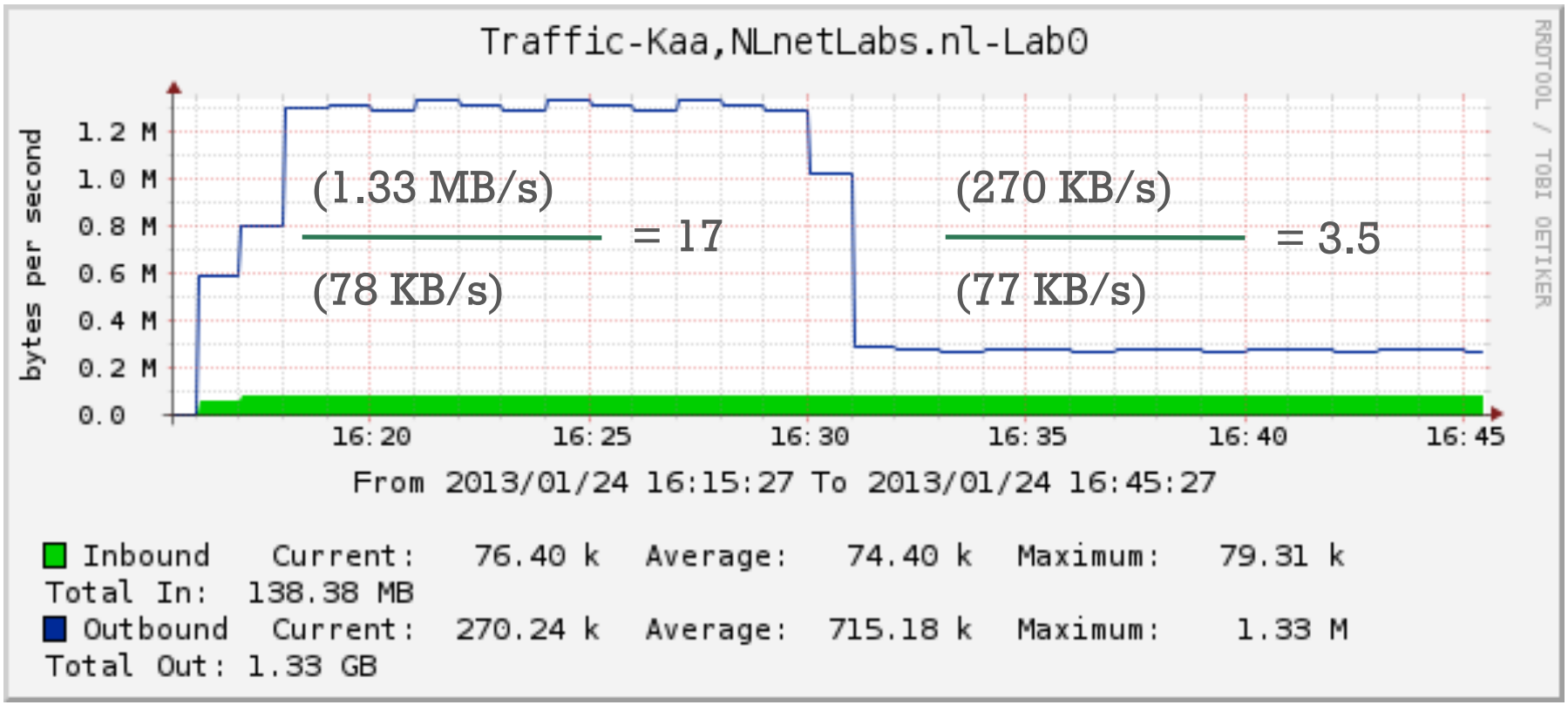
Measurements 1/5 – Repeating ANY attack

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%

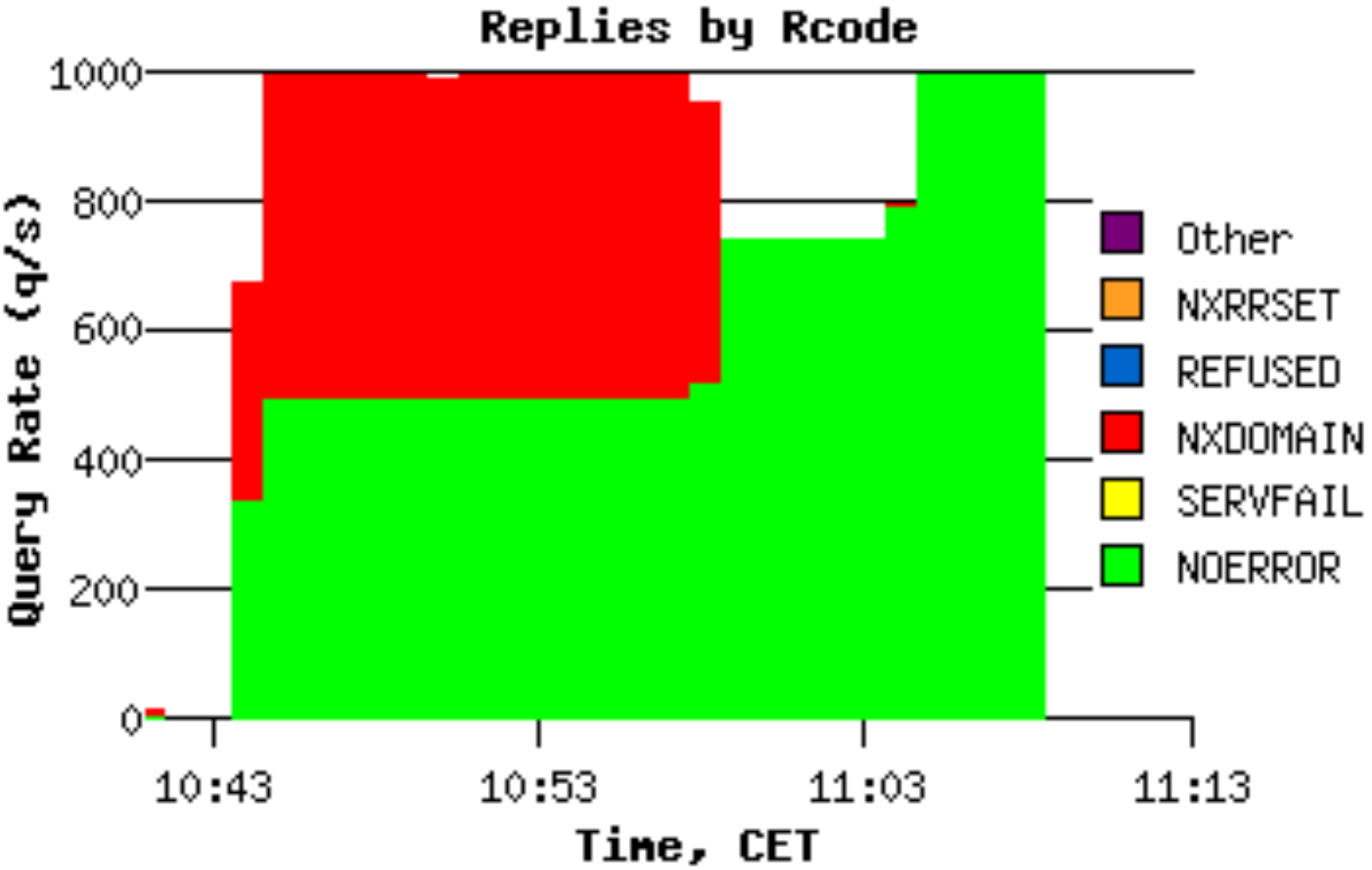
Measurements 2/5 – Varying query attack (25%)



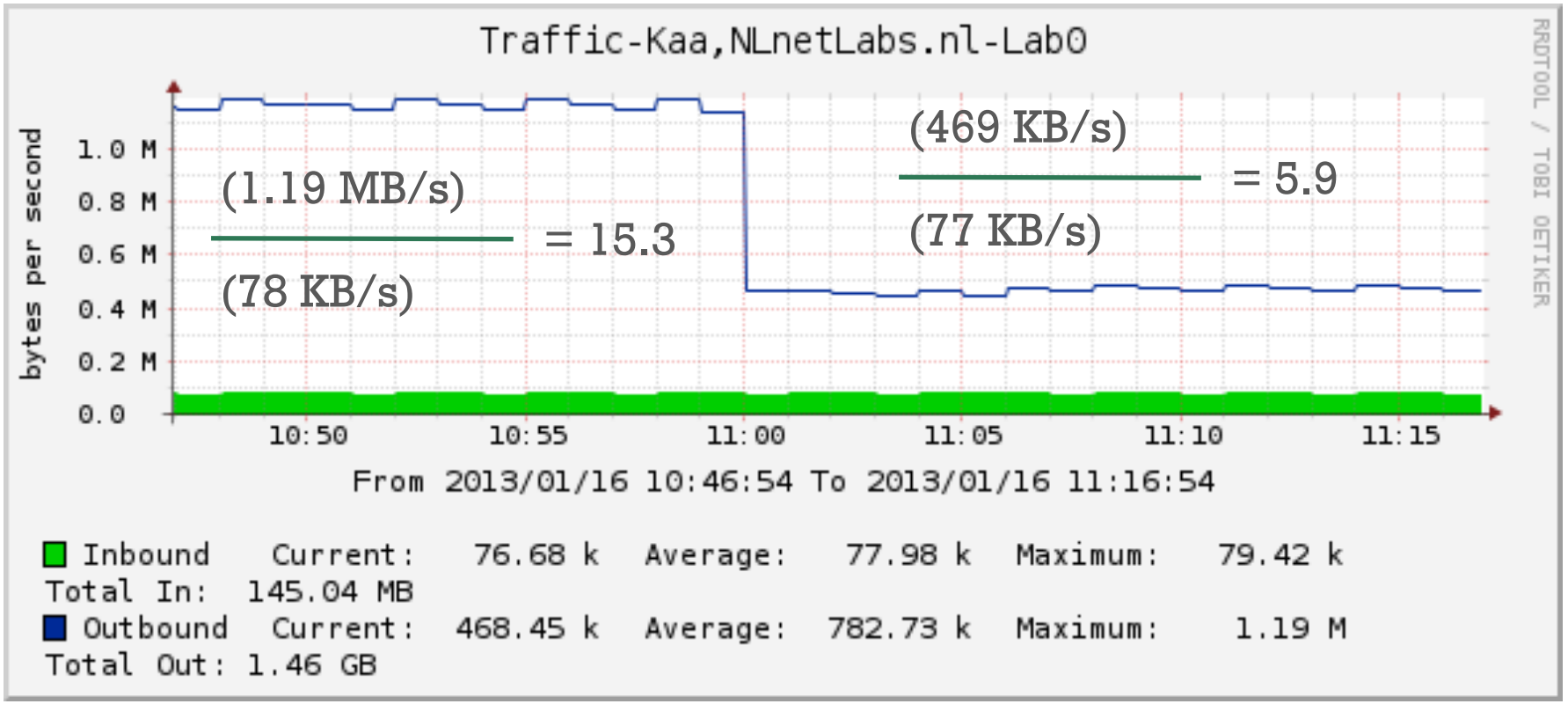
Measurements 2/5 – Varying query attack (25%)



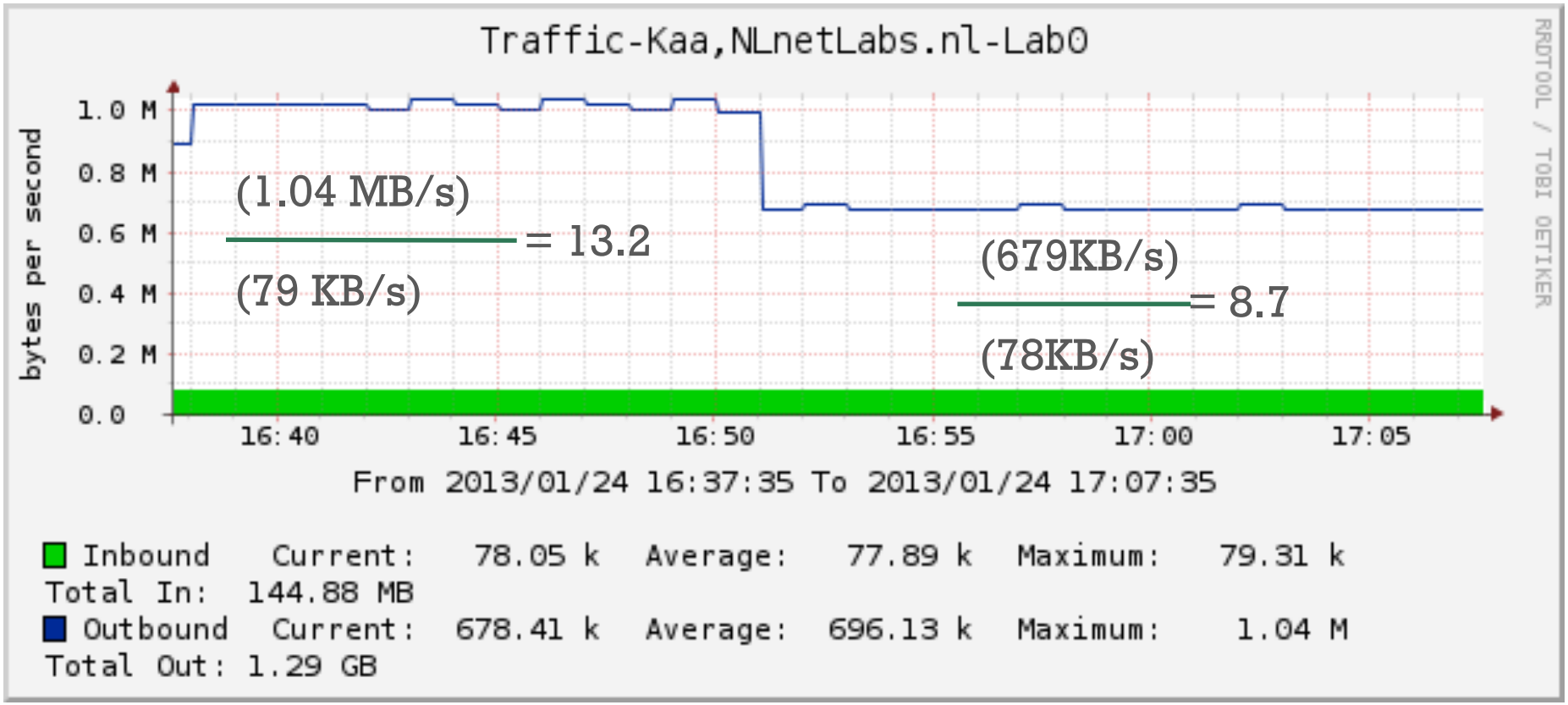
Measurements 3/5 – Varying query attack (50%)



Measurements 3/5 – Varying query attack (50%)



Measurements 4/5 – Varying query attack (75%)



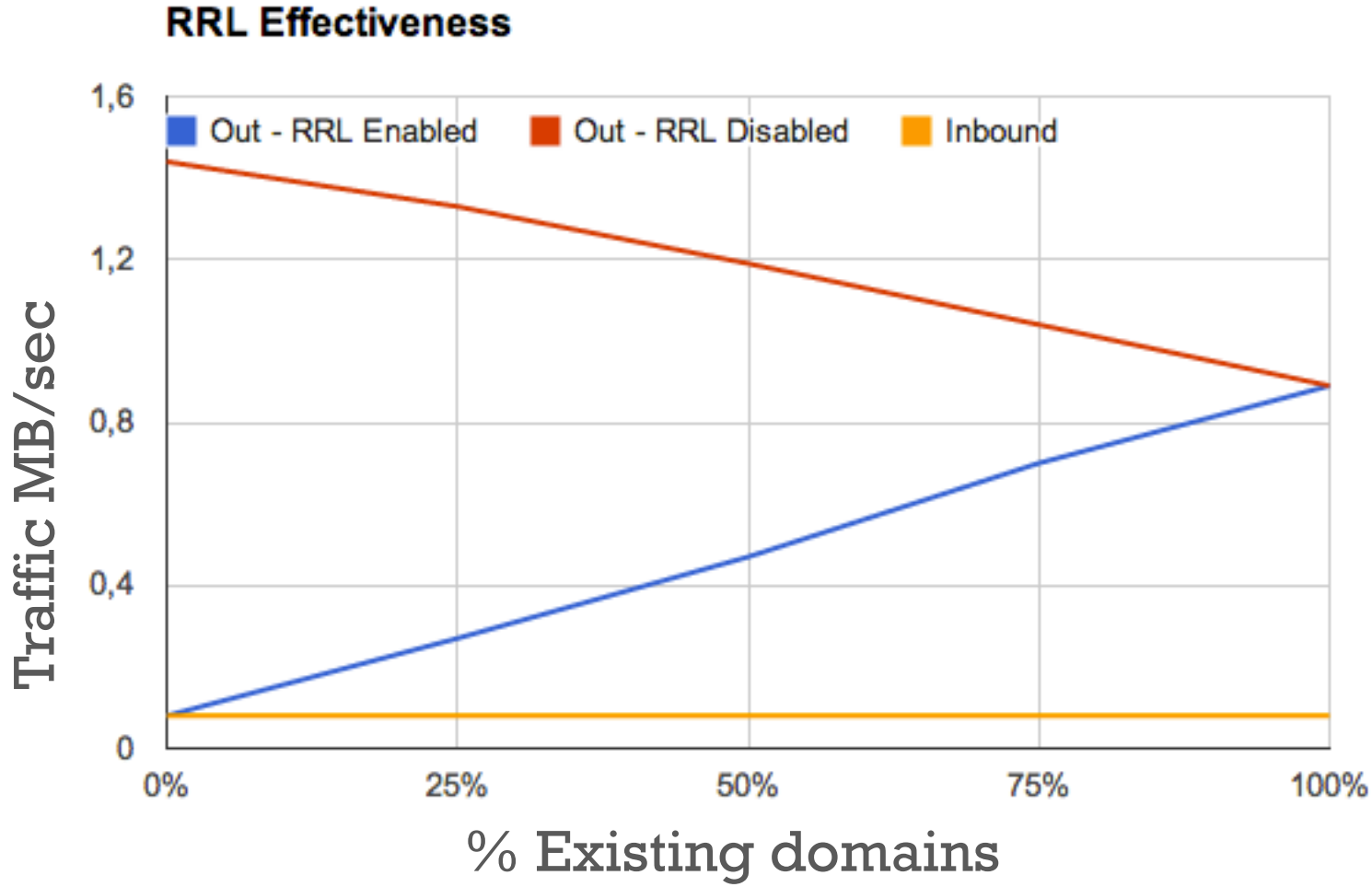
Measurements 4/5 – Varying query attack (75%)

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%

Measurements 5/5 – Varying query attack (100%)

RRL	In	Out	Amp. ratio
Disabled	80KB/s	891KB/s	1:11.14
Enabled	80KB/s	891KB/s	1:11.14

Results


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

DNS Dampening

- Successful against distributed attacks
- Counts requests instead of responses
- Penalty points for every request
- No mechanism like slip implemented
- Most parameters cannot be changed in configuration

Conclusion

- RRL effective:
  - Attacks repeating the same query.
- RRL ineffective:
  - Varying query attacks / Distributed attacks.
- DNS Dampening:
  - Effective against all tested attacks.
  - No mechanism to prevent false positives.
- Need to push BCP38

Q&A