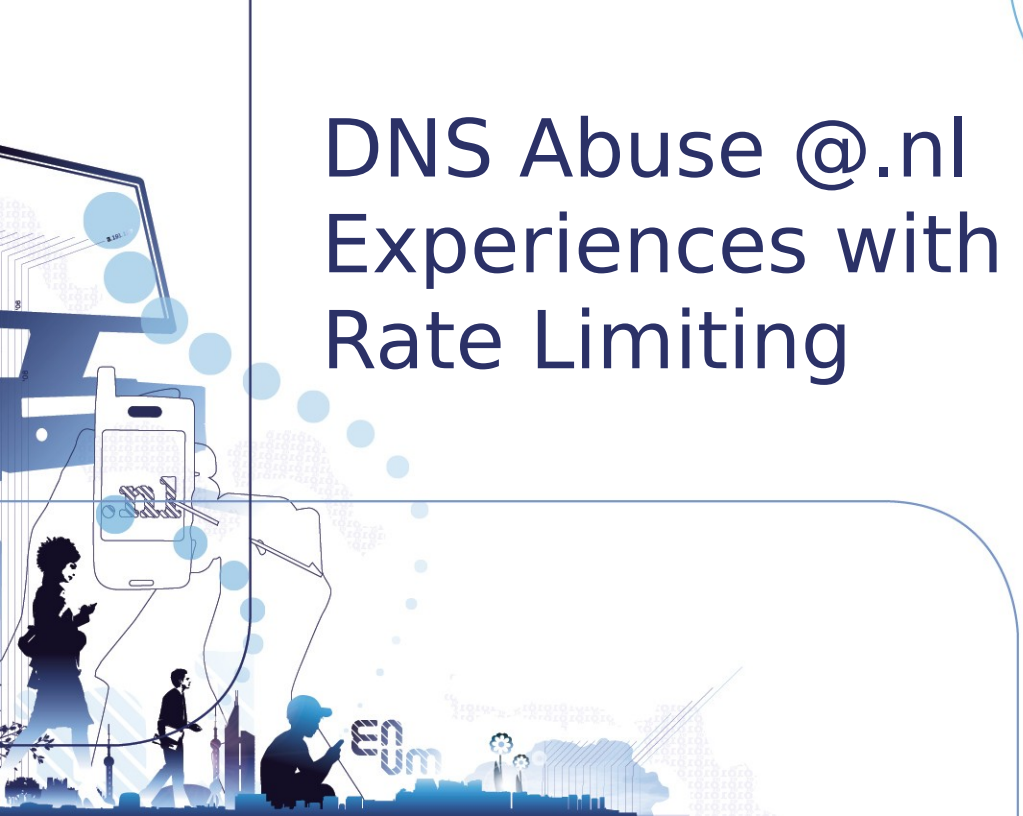
DNS Abuse @.nl Experiences with Rate Limiting



May 15, 2013

RIPE66 DNS-wg

Dublin

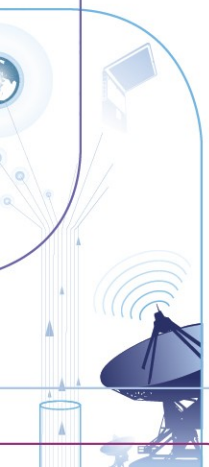
Stephan.Rutten@sidn.nl

SIDN

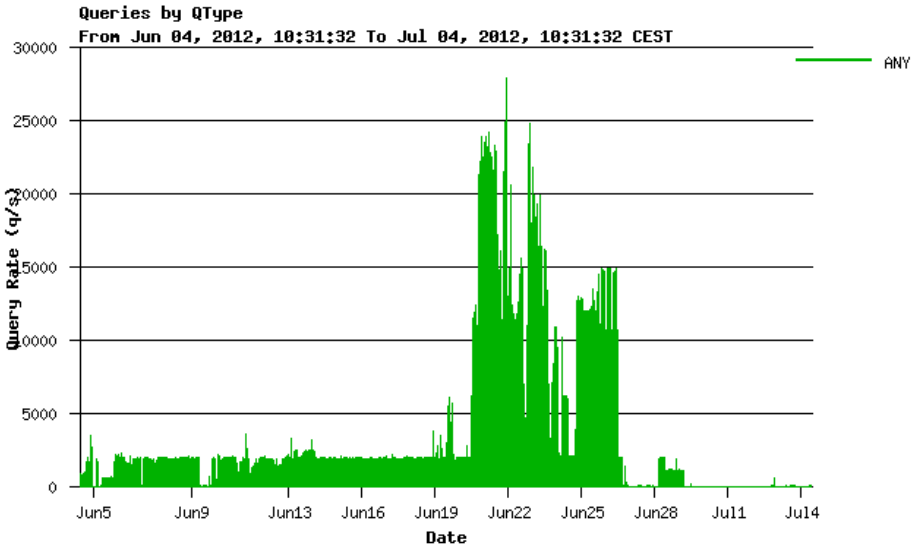
- Rise in abusive DNS traffic
- Mitigating the adverse effects
- What we are working on now

2012 ANY traffic grows

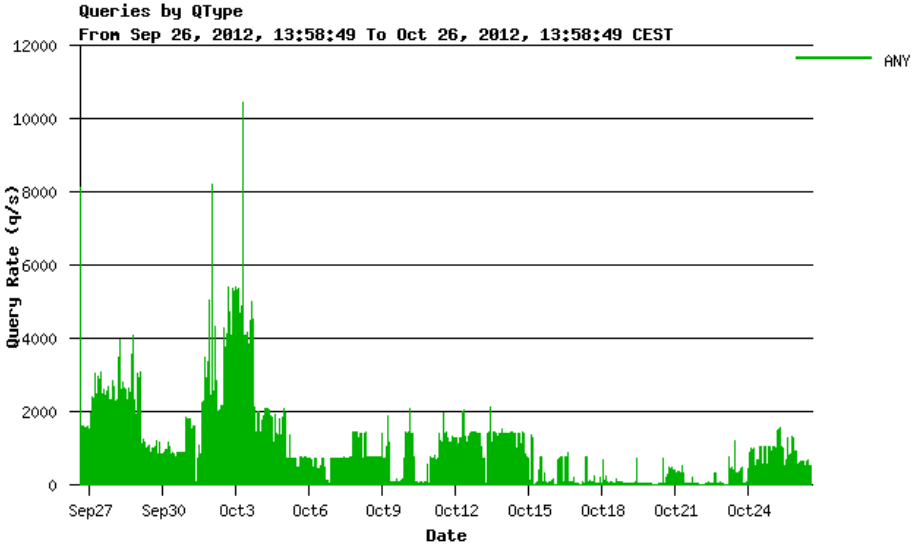
- Amplification attacks using ANY queries
- Traffic is amplified 100 times
- Could have been almost 200 if RD bit set



ANY traffic vs iptables u32 filtering

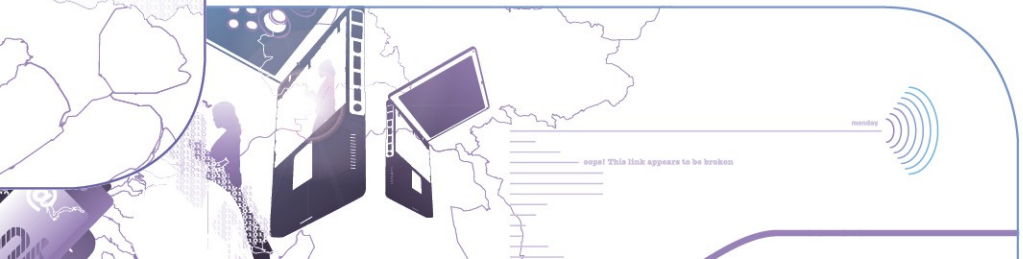


Incoming ANY traffic still abnormal



February 2013

- ANY traffic at our secondary name servers
- FreeBSD / OpenBSD – no U32
- So we built a new Linux cluster
- First implementation of RRLs in BIND
- RRLs on all DNS servers (BIND & NSD)



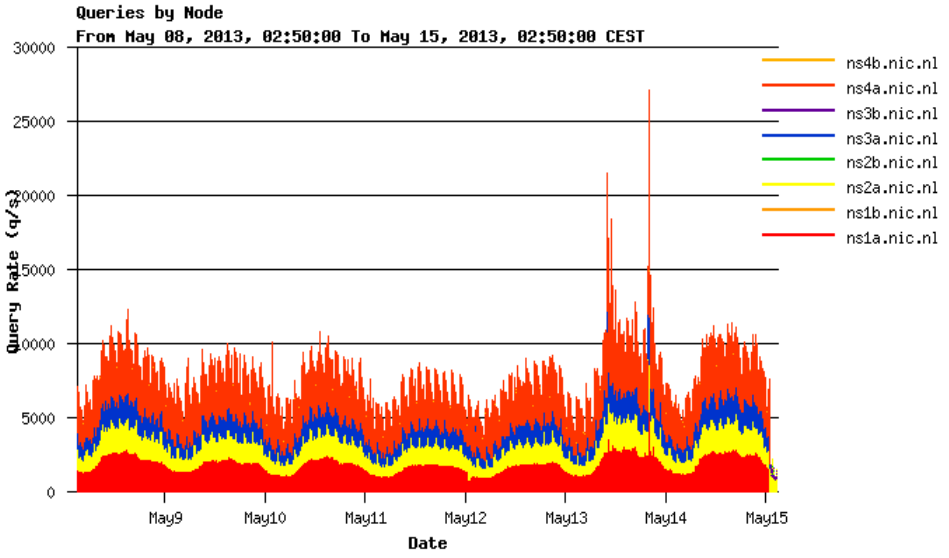
Now

- Rolling out anycast name servers
- Increasing monitoring and alerting
- 30+ checks per DNS server
- Ready for the next big one

Look, even more Nagios checks.

ns-ams-glob2.anycloud.nl	# Users		OK	2013-05-14 11:45:54	11d 22h 32m 41s	1/3	USERS OK - 0 users currently logged in
	/ Disk Usage		OK	2013-05-14 11:47:58	12d 21h 27m 43s	1/3	DISK OK - free space: / 1017 MB (72% inode=96%):
	/boot Disk Usage		OK	2013-05-14 11:43:44	9d 11h 51m 2s	1/3	DISK OK - free space: /boot 169 MB (78% inode=99%):
	/home Disk Usage		OK	2013-05-14 11:48:28	12d 21h 32m 19s	1/3	DISK OK - free space: /home 74698 MB (98% inode=99%):
	/sidn Disk Usage waakdienst		OK	2013-05-14 11:48:07	9d 11h 43m 11s	1/3	DISK OK - free space: /sidn 11860 MB (88% inode=99%):
	/tmp Disk Usage		OK	2013-05-14 11:47:55	12d 21h 27m 43s	1/3	DISK OK - free space: /tmp 1870 MB (99% inode=99%):
	/usr Disk Usage		OK	2013-05-14 11:47:30	12d 21h 27m 43s	1/3	DISK OK - free space: /usr 7147 MB (89% inode=86%):
	/var Disk Usage		OK	2013-05-14 11:43:44	9d 11h 51m 1s	1/3	DISK OK - free space: /var 18607 MB (97% inode=99%):
	Apt Package Status		WARNING	2013-05-14 11:30:48	0d 4h 37m 49s	3/3	APT WARNING: 6 packages available for upgrade (0 critical updates).
	Check Disk Checks		OK	2013-05-14 10:22:55	12d 21h 25m 58s	1/3	OK: All disks are checked.
	DNS SOA UPTODATE .NL		OK	2013-05-14 11:48:22	12d 1h 43m 17s	1/3	OK - Both serials are: 2013051405
	DSC ANY Queries per second		OK	2013-05-14 11:43:51	9d 11h 51m 1s	1/3	OK - 0 ANY queries per second
	DSC MX Queries per second		OK	2013-05-14 11:43:51	9d 11h 50m 53s	1/3	OK - 0 MX queries per second
	DSC TCP Queries per second		OK	2013-05-14 11:47:56	1d 0h 50m 44s	1/3	OK - 0 tcp queries per second
	DSC Total Queries per second		OK	2013-05-14 11:43:51	12d 21h 27m 43s	1/3	OK - 0 TOTAL queries per second
	HP ProLiant via NRPE		OK	2013-05-14 11:47:07	12d 20h 26m 41s	1/3	Compaq/HP Agent Check: overall system state OK
	IP6TABLES Check		OK	2013-05-14 11:46:10	12d 21h 29m 42s	1/3	OK INPUT 30 rules
	IPTABLES Check		OK	2013-05-14 11:46:15	12d 21h 35m 41s	1/3	OK INPUT 16 rules OK RATELIMITER 1 rules
	Ksplice Uptrack Status		OK	2013-05-14 10:27:13	11d 21h 21m 24s	1/3	ns-ams-glob2 (94.198.159.251) is OK
	Load Average		OK	2013-05-14 11:46:19	12d 21h 27m 43s	1/3	OK - load average: 0.05, 0.07, 0.05
	NTP Stratum		OK	2013-05-14 11:43:50	9d 11h 51m 1s	1/3	STRATUM OK. Level: 3 (Good) System Peer: 94.198.152.3
	Nameserver NIC Usage		OK	2013-05-14 11:48:22	12d 21h 32m 19s	1/3	RX Bytes: 379MB, TX Bytes: 380MB: RX Speed: 230Bps, TX Speed: 230Bps: OK bandwidth utilization
	Network Bonding		OK	2013-05-14 11:46:33	12d 21h 32m 53s	1/3	bond0 up: members = eth3 (up) eth1 (up) bond1 up: members = eth2 (up) eth0 (up)
	Network Interface Usage		OK	2013-05-14 11:48:13	12d 21h 27m 43s	1/3	RX Bytes: 379MB, TX Bytes: 380MB: RX Speed: 253Bps, TX Speed: 255Bps: OK bandwidth utilization
	Puppet Check		OK	2013-05-14 11:43:44	9d 11h 51m 1s	1/3	OK: puppetd running fine. Last succesful run was 504 seconds ago.
	Swap Memory Usage		OK	2013-05-14 11:44:07	12d 21h 27m 43s	1/3	SWAP OK - 100% free (11623 MB out of 11623 MB)
	Total Processes		OK	2013-05-14 11:43:46	9d 11h 51m 1s	1/3	PROCS OK: 250 processes
	Zombie Guard		OK	2013-05-14 11:46:48	12d 21h 27m 42s	1/3	PROCS OK: 1 process with STATE = Z

'Normal traffic'



Questions?