


 lieter\_  
 PowerDNS

pieterlexis   
PowerDNS 

## dnsmist: two years later

---

Pieter Lexis  
PowerDNS Engineer

**POWERDNS**   
AN  COMPANY

The story of dnsmdist  
- or -  
“Do we need a DNS Delivery Controller”?

<http://dnsmdist.org/>

## dnsmist – A recap

“dnsmist is a highly DNS-, DoS- and abuse-aware loadbalancer. Its goal in life is to route traffic to the best server, delivering top performance to legitimate users while shunting or blocking abusive traffic.”

- “Query concentrator”
- A lot of statistics
- Live traffic inspection
- Filter traffic (from the kernel)
- Packet mangler
- Open Source (GPLv2) and vendor neutral

## dnsmist – A recap

- Send traffic to different backend server pools
- Actions can be applied based on many query or response attributes
- Actions included
  - Drop
  - Delay
  - Spoof an answer
  - Execute a Lua function
- Automatic time-limited blocking of clients

## Discussion: do we need this?

- A pure load balancer knows nothing of DNS and can be very fast ('lob packets')
- A nameserver is fully featured and can also do load balancing itself ('forwarders')
- Is there room or need for something in between?
- People tell us 'yes', but are they right?
  - Or will we end up 'making another nameserver in front of your nameserver'?

The answer

YES

The answer

YES

ABSO-F\*\*\*\*\*-LUTELY

# “I have seen things”

- Statistics for legacy nameserver platform
- Cache in front of a dying recursor cluster
- In front of an existing authoritative platform:
  - to prepare for migrations
  - to protect un-upgradeable platforms
- Send DNSSEC queries to DNSSEC resolvers
- Send abusive traffic to “abuse pool”
- Realtime inspection of traffic
- Restricting queries from legitimate users
- Large scale DoS: absorb & filter at million QPS rates



# New features since May 2015

- A per-pool cache
- JSON API with stats
- Remote logging via Protobuf over TCP
- More selectors
  - QNameLabelsCountRule()
  - QNameWirelengthRule()
  - Destination Address matching
  - RCodeRule()
- Response Actions

# Upcoming features

- Response TTL modification
- Cache-hit selector
- `SNMPTrapAction()`
- Statistics through SNMP
- Per-pool server selection policy
- DNStap support

# Questions/Comments?

Packages: <https://repo.powerdns.com>  
Documentation: <http://dnsmdist.org>  
Issue Tracker: <https://github.com/PowerDNS/pdns/issues>

**POWERDNS**   
AN  COMPANY