lieter_
PowerDNS

pieterlexis
PowerDNS

# dnsdist: Denial of Service Protection for DNS

**Pieter Lexis**
PowerDNS Engineer

POWERDNS
AN OX COMPANY

# Protecting DNS Servers From Denial of Service Attacks

## Common DNS protection steps

1. `tcpdump`
2. `grep`/`awk`
3. **cursing**
4. `iptables -A INPUT -i eth0 -p udp --port 53 -m string --hex-string "|07|example|03|com" -algo bm -j DROP`
5. Realising it is incomplete
6. GOTO 1

# Live traffic inspection i

```
> topQueries(5)
   1  <snip>.ru.                          2358 23.6%
   2  localhost.                          2281 22.8%
   3  time.apple.com.                      537  5.4%
   4  <snip>.de.                           144  1.4%
   5  time.euro.apple.com.                 109  1.1%
   6  Rest                                4571 45.7%

> topResponses(2, dnsdist.SERVFAIL)
   1  <snip>.in-addr.arpa.                  31 22.1%
   2  <snip>.de.                            15 10.7%
   3  Rest                                  94 67.1%
```

# Live traffic inspection ii

```
> grepq('ru', 2)
Time  Client              Server         ID    Name        Type Lat. TC RD AA Rcode
-0.2  192.168.1.92:33846                 4905  <snip>.ru.  ANY          RD    Question
-0.2  192.168.1.92:33846  127.0.0.1:5300 4905  <snip>.ru.  ANY  0.2     RD    Non-Existe
-0.2  192.168.1.92:33846                 4907  <snip>.ru.  ANY          RD    Question
-0.2  192.168.1.92:33846  127.0.0.1:5300 4907  <snip>.ru.  ANY  0.3     RD    Non-Existe

> grepq({'apple.com.', "100ms"}, 5)
Time    Client              Server         ID    Name           Type Lat.  TC RD AA Rcode
-127.6  192.168.1.92:43583 127.0.0.1:5300 44987 cl4.apple.com. A    247.2    RD    No Er
```

# Different Ways of Limiting Traffic i

```
1  -- Drop all queries for all questions under .example
2  addDomainBlock("example.")
```

# Different Ways of Limiting Traffic ii

```
-- Limit /24's on IPv4 and /64's on IPv6 to 5 QPS
addAction(MaxQPSIPRule(5, 24, 64), DropAction())
```

# Different Ways of Limiting Traffic iii

```
1  -- Create a NetMaskGroup for matching
2  nmg = newNMG()
3  nmg:addMask('192.0.2.0/27')
4  nmg:addMask('2001:db8:0:12::/48')
5
6  -- match QTYPE AAAA and QNAME containing powerdns
7  selector = AndRule{QTypeRule(dnsdist.AAAA),
     ↪  RegexRule('powerdns')}
8
9  -- Add the netmask group to the rule selector
10 selector = AndRule{selector, NetmaskGroupRule(nmg)}
11
12 -- Delay by 900 ms
13 addAction(selector, DelayAction(900))
```

# Automatically Block Traffic

```
function maintenance()
  -- Get the addresses that had more than 100
    ↪  NXDOMAINs in the last 10 seconds
  addresses = exceedNXDOMAINS(100, 10)
  -- Block the addresses for a minute
  addDynBlocks(addresses, "Exceeded NXDomain", 60)
end
```

# Traffic Matching and Actions

## Selectors

- Source Address
- Destination address
- QNAME
- QTYPE
- Flags
- OPCODE
- TCP query
- Number of entries in a packet section
- Number of labels in the name
- Regular Expression
- Combine selectors with And, Or and Not

## Actions

- Drop
- Route to Pool
- Truncate (TC=1)
- Return SERVFAIL, NOTIMP, REFUSED
- Return custom answer
- Delay response by n milliseconds
- Remove flags before passing to backend
- Add originating IP address in an EDNS option
- Log query to TCP/IP host via Protobuf
- Increase statistics counter
- Strip EDNS Client Subnet
- Send SNMP trap

Packages at

**https://repo.powerdns.com**

Documentation at

**http://dnsdist.org**

Help and Support at

**irc://chat.oftc.net/#powerdns**

# Other **dnsdist** Scenarios

- Statistics for legacy nameserver platform
- Realtime inspection of traffic
- Send DNSSEC queries to DNSSEC servers
- Send abusive traffic to “abuse pool”
- Fix up case sensitive backends / clients
- Use regular expressions to route queries
- Client DoS worries: limit each host QPS or per /64
- Large scale DoS: absorb & filter at million QPS rates