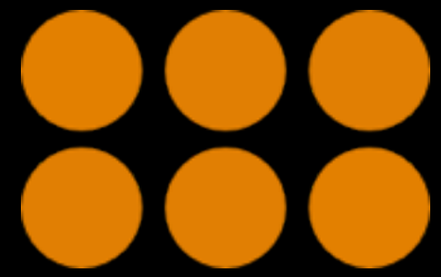
Lua Policy Engine

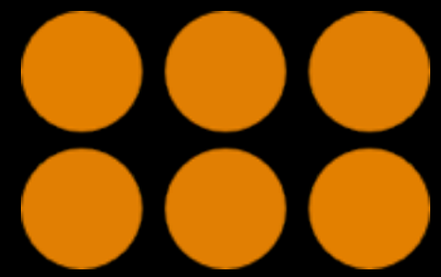
Peter van Dijk, PowerDNS

Context



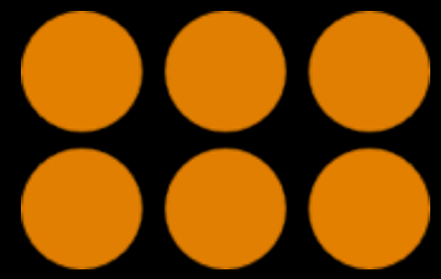
- DNS amplification
- Reflection
- RRL
- competing proposals (DNS Dampening)

Idea



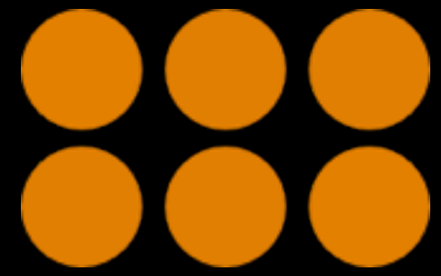
- Enough rope to hang yourself^W^Wsupport ‘redbarn’ RRL
- Handle caching
- Allow real time management

Convention



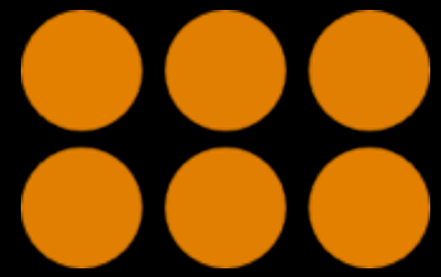
```
function police (req, resp, isTcp)
  if resp
  then
    qname, qtype = resp:getQuestion()
    -- magic happens here
    -- perhaps return pdns.TRUNCATE?
    -- or pdns.DROP?
  end
  return pdns.PASS
end
```

Methods



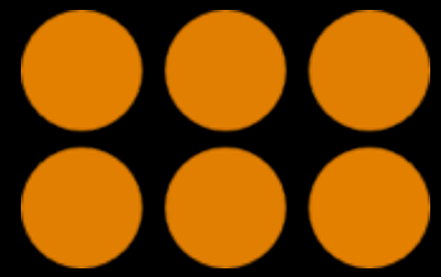
- `qname, qtype = resp:getQuestion()` -- string, number
- `remote = resp:getRemote()` -- string (remote IPv4/v6 address)
- `wild = resp:getWild()` -- string
- `zone = resp:getZone()` -- string
- `reqsize = req:getSize()` -- number (in bytes)
- `respsize = resp:getSize()` -- number (in bytes)
- `rcode = resp:getRcode()` -- number
- `an, ns, ar = resp:getRRCounts()` -- number, number, number

Truncate wildcards



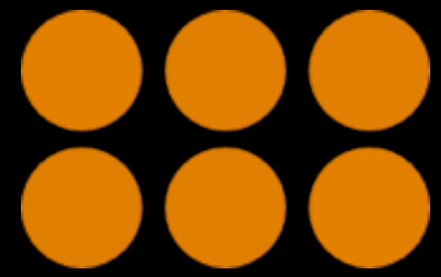
```
function police (req, resp, isTcp)
   if resp and resp:getWild():len() > 0
   then
      return pdns.TRUNCATE
   end
   return pdns.PASS
end
```

RRL example (1)



```
conf = {}
conf.rps = 5
conf.eps = 5
conf.logonly = false
conf.window = 5
conf.v4len = 24
conf.v6len = 56
conf.leakrate = 3
conf.tcrate = 2
```

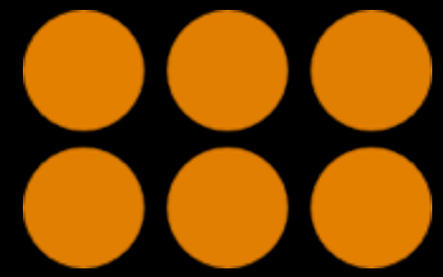
RRL example (2)



```
if wild:len() > 0 then
   imputedname = wild
elseif rcode == pdns.NXDOMAIN or errorstatus
then
   imputedname = zone
end


token = mask(remote)..”/"..
   imputedname..”/"..
   tostring(errorstatus)
```

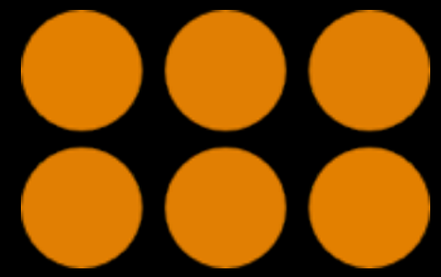
Inspect



```
$ pdns_control policy get example.com
qps for example.com is 58
```

```
function policycmd(cmd, arg)
  if cmd == "get" then
    local qps = getqps(arg)
    return "qps for "..arg.." is "..qps
  end
end
```

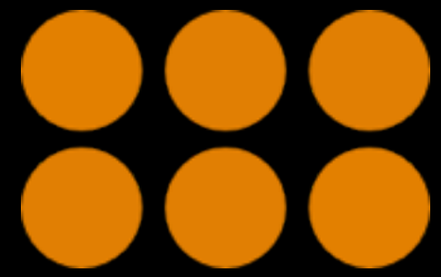
Modify



```
$ pdns_control policy block example.com
example.com now blocked
```

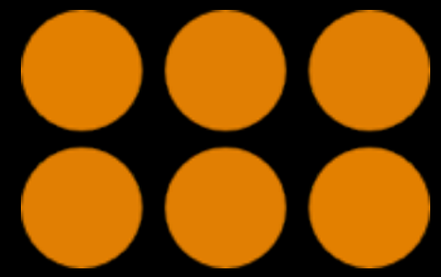
```
function policycmd(cmd, arg)
   if cmd == "block" then
      blocks[arg] = 1
      return arg.." now blocked"
   end
end
```

Measure



```
function metrics()
  return {foo=5, bar=10}
end
```

Thank you



http://tinyurl.com/pdnsripe69